Documentação do StorageGRID 11,9

StorageGRID 11.9

NetApp
November 08, 2024

Índice

Documentação do StorageGRID 11,9

Dispositivos StorageGRID

```
https://docs.netapp.com/us-en/storagegrid-
appliances/index.html["Documentação do StorageGRID Appliance"^]Acesse para
saber como instalar, configurar e manter dispositivos de armazenamento e
serviços StorageGRID.
```

Notas de lançamento

Obtenha informações específicas sobre problemas corrigidos e problemas conhecidos.

Faça login no site de suporte da NetApp para "Ver ou transferir um ficheiro PDF" conter as notas de versão do StorageGRID 11,9.

Comece a usar um sistema StorageGRID

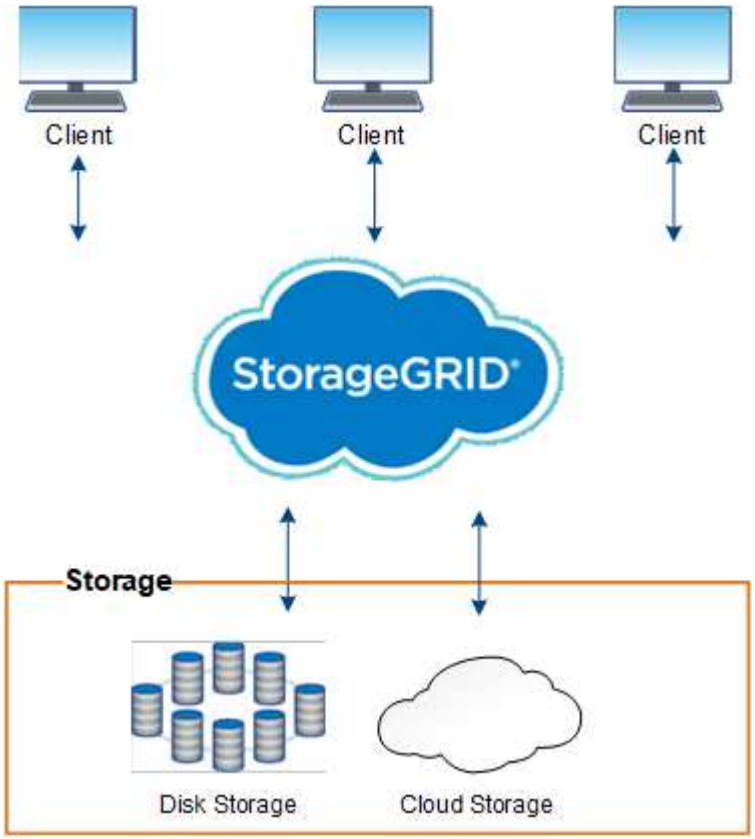
Saiba mais sobre o StorageGRID

O que é o StorageGRID?

O NetApp StorageGRID é um pacote de storage de objetos definido por software compatível com uma ampla variedade de casos de uso em ambientes multicloud públicos, privados e híbridos. A StorageGRID oferece suporte nativo à API Amazon S3 e oferece inovações líderes do setor, como gerenciamento automatizado do ciclo de vida, para armazenar, proteger e preservar dados não estruturados de maneira econômica por longos períodos.

O StorageGRID fornece storage seguro e durável para dados não estruturados em escala. As políticas integradas de gerenciamento de ciclo de vida orientadas por metadados otimizam a localização dos dados durante todo o ciclo de vida. O conteúdo fica no local certo, no momento certo e na camada de storage certa para reduzir os custos.

O StorageGRID é composto por nós heterogêneos, redundantes e distribuídos geograficamente, que podem ser integrados a aplicativos clientes existentes e de próxima geração.



O suporte para nós de arquivamento foi removido. Mover objetos de um nó de arquivo para um sistema de armazenamento de arquivamento externo por meio da API S3 foi substituído pelo "Pools de storage em nuvem da ILM", que oferece mais funcionalidade.

Benefícios do StorageGRID

As vantagens do sistema StorageGRID incluem o seguinte:

- Altamente escalável e fácil de usar um repositório de dados distribuído geograficamente para dados não estruturados.
- Protocolos padrão de storage de objetos:
  - Amazon Web Services Simple Storage Service (S3)
  - OpenStack Swift

  > O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

- Nuvem híbrida habilitada. O gerenciamento do ciclo de vida das informações (ILM) baseado em políticas armazena objetos em nuvens públicas, incluindo Amazon Web Services (AWS) e Microsoft Azure. Os serviços de plataforma StorageGRID permitem replicação de conteúdo, notificação de eventos e pesquisa de metadados de objetos armazenados em nuvens públicas.
- Proteção de dados flexível para garantir durabilidade e disponibilidade. Os dados podem ser protegidos usando replicação e codificação de apagamento em camadas. A verificação de dados em repouso e em trânsito garante a integridade para retenção a longo prazo.
- Gerenciamento dinâmico do ciclo de vida dos dados para ajudar a gerenciar custos de storage. Você pode criar regras de ILM que gerenciam o ciclo de vida dos dados no nível do objeto, personalizando a localidade, a durabilidade, o desempenho, o custo e o tempo de retenção dos dados.
- Alta disponibilidade de storage de dados e algumas funções de gerenciamento, com balanceamento de carga integrado para otimizar a carga de dados entre os recursos da StorageGRID.
- Suporte para várias contas de inquilinos de storage para segregar os objetos armazenados em seu sistema por diferentes entidades.
- Várias ferramentas para monitorar a integridade do seu sistema StorageGRID, incluindo um sistema de alerta abrangente, um painel gráfico e status detalhado para todos os nós e sites.
- Suporte para implantação baseada em software ou hardware. Você pode implantar o StorageGRID em qualquer uma das seguintes opções:
  - Máquinas virtuais em execução no VMware.
  - Motores de contentor em hosts Linux.
  - Aparelhos projetados pela StorageGRID.
    - Os dispositivos de storage fornecem storage de objetos.
    - Os dispositivos de serviços fornecem serviços de administração de grade e balanceamento de carga.
- Em conformidade com os requisitos de armazenamento relevantes destes regulamentos:
  - Securities and Exchange Commission (SEC) em 17 CFR 240,17a-4(f), que regula os membros de câmbio, corretores ou revendedores.
  - Regra 4511(c) da Financial Industry Regulatory Authority (FINRA), que defensa o formato e os requisitos de Mídia da regra 17a-4(f) da SEC.
  - Comissão de negociação de futuros de commodities (CFTC) na regra 17 CFR 1,31 (c)-(d), que regula a negociação de futuros de commodities.
- Operações de atualização e manutenção sem interrupções. Mantenha o acesso ao conteúdo durante os

procedimentos de atualização, expansão, desativação e manutenção.

- Gerenciamento de identidade federado. Integra-se com ative Directory, OpenLDAP ou Oracle Directory Service para autenticação de usuário. Suporta logon único (SSO) usando o padrão SAML 2,0 (Security Assertion Markup Language 2,0) para trocar dados de autenticação e autorização entre o StorageGRID e o AD FS (Serviços de Federação do ative Directory).

Nuvens híbridas com StorageGRID

Use o StorageGRID em uma configuração de nuvem híbrida implementando gerenciamento de dados voltado a políticas para armazenar objetos em pools de storage de nuvem, utilizando serviços de plataforma StorageGRID e disposição em camadas de dados do ONTAP para o StorageGRID com o NetApp FabricPool.

Pools de storage de nuvem

Os pools de armazenamento em nuvem permitem armazenar objetos fora do sistema StorageGRID. Por exemplo, você pode migrar objetos acessados com pouca frequência para storage de nuvem de baixo custo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou a categoria Acesso de arquivamento no storage de Blobs do Microsoft Azure. Ou, talvez você queira manter um backup em nuvem de objetos StorageGRID, que pode ser usado para recuperar dados perdidos devido a uma falha de volume de storage ou nó de storage.

O armazenamento de parceiros de terceiros também é suportado, incluindo armazenamento em disco e fita.

> O uso de pools de armazenamento em nuvem com FabricPool não é suportado devido à latência adicional para recuperar um objeto do destino de pool de armazenamento em nuvem.

Serviços de plataforma S3

Os serviços de plataforma S3 oferecem a capacidade de usar serviços remotos como endpoints para replicação de objetos, notificações de eventos ou integração de pesquisa. Os serviços de plataforma operam independentemente das regras ILM da grade e são habilitados para buckets individuais do S3. Os seguintes serviços são suportados:

- O serviço de replicação do CloudMirror espelha automaticamente objetos especificados em um bucket do S3 de destino, que pode estar no Amazon S3 ou em um segundo sistema StorageGRID.
- O serviço de notificação de eventos envia mensagens sobre ações especificadas para um endpoint externo que suporta o recebimento de eventos do Simple Notification Service (Amazon SNS).
- O serviço de integração de pesquisa envia metadados de objetos para um serviço Elasticsearch externo, permitindo que os metadados sejam pesquisados, visualizados e analisados usando ferramentas de terceiros.

Por exemplo, você pode usar a replicação do CloudMirror para espelhar Registros específicos de clientes no Amazon S3 e aproveitar os serviços da AWS para realizar análises nos seus dados.

Disposição de dados em camadas do ONTAP usando o FabricPool

Você pode reduzir os custos do storage do ONTAP categorizando os dados no StorageGRID usando o FabricPool. O FabricPool permite a disposição automatizada de dados em camadas de storage de objetos de baixo custo, seja no local ou fora dele.

Diferentemente das soluções de disposição manual em camadas, o FabricPool reduz o custo total de

propriedade automatizando a disposição em camadas de dados para reduzir o custo de storage. Ele oferece os benefícios da economia da nuvem ao dispor em camadas em nuvens públicas e privadas, incluindo o StorageGRID.

Informações relacionadas

- "O que é Cloud Storage Pool?"
- "Gerenciar serviços de plataforma"
- "Configurar o StorageGRID para FabricPool"

Topologia de rede e arquitetura StorageGRID

Um sistema StorageGRID consiste em vários tipos de nós de grade em um ou mais locais de data center.

Consulte "descrições dos tipos de nó de grade".

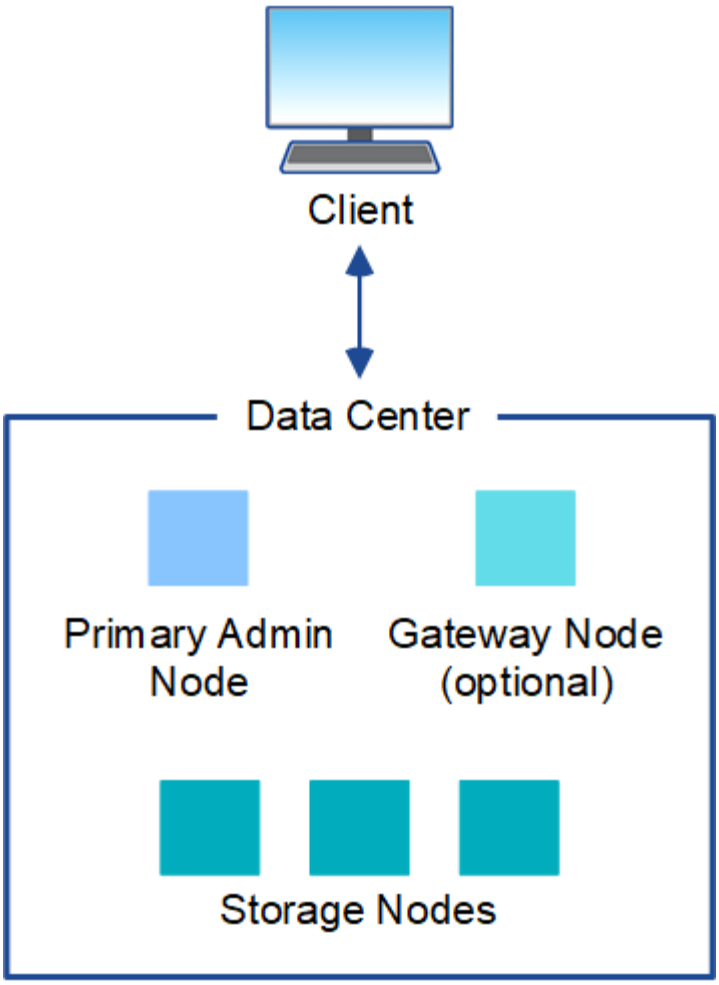
Para obter informações adicionais sobre topologia de rede, requisitos e comunicações em grade do StorageGRID, consulte o "Diretrizes de rede".

Topologias de implantação

O sistema StorageGRID pode ser implantado em um único local de data center ou em vários locais de data center.

Um único local

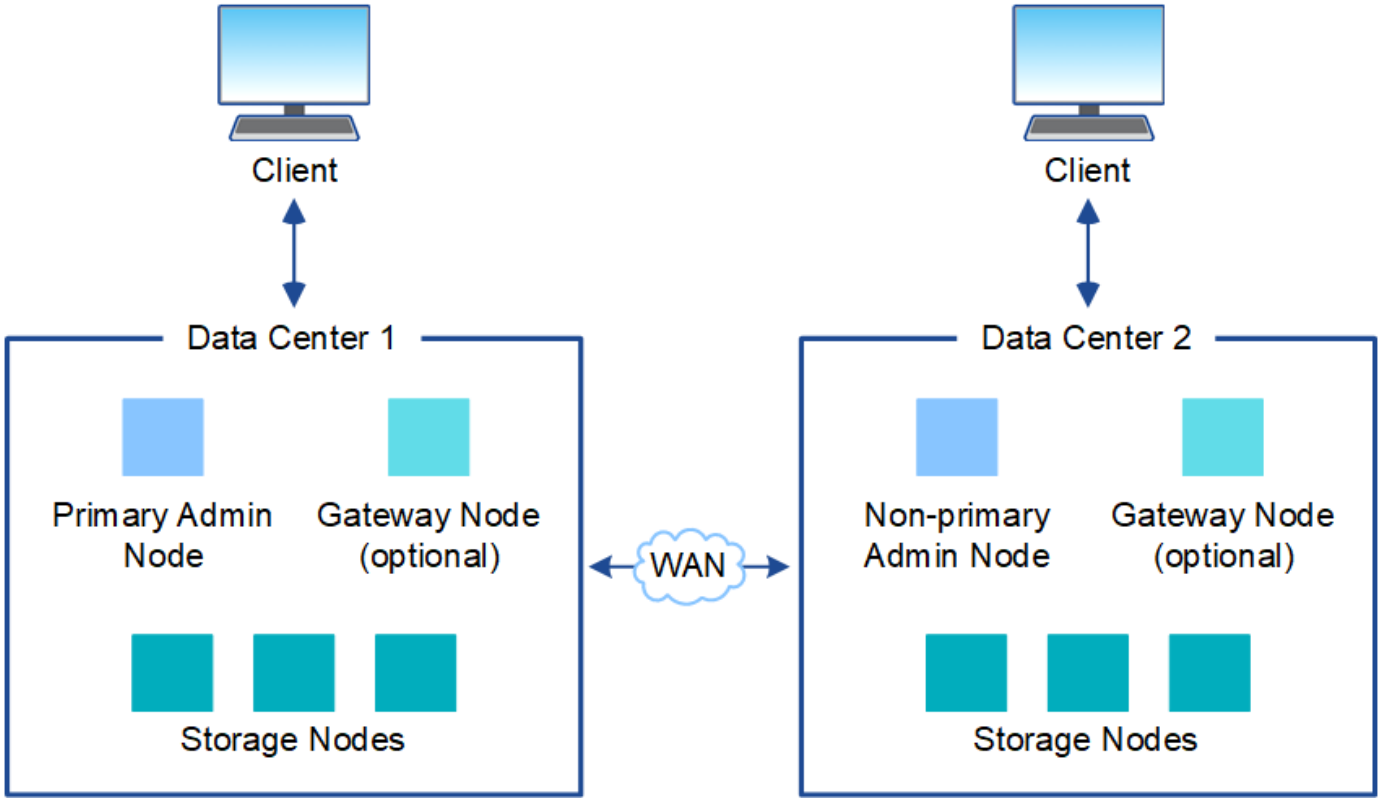
Em uma implantação com um único local, a infraestrutura e as operações do sistema StorageGRID são centralizadas.



Vários locais

Em uma implantação com vários sites, diferentes tipos e números de recursos do StorageGRID podem ser instalados em cada local. Por exemplo, pode ser necessário mais armazenamento em um data center do que em outro.

Diferentes locais são frequentemente localizados em locais geograficamente diferentes em diferentes domínios de falha, como uma linha de falha de Terremoto ou planície de inundação. O compartilhamento de dados e a recuperação de desastres são obtidos pela distribuição automatizada de dados para outros sites.



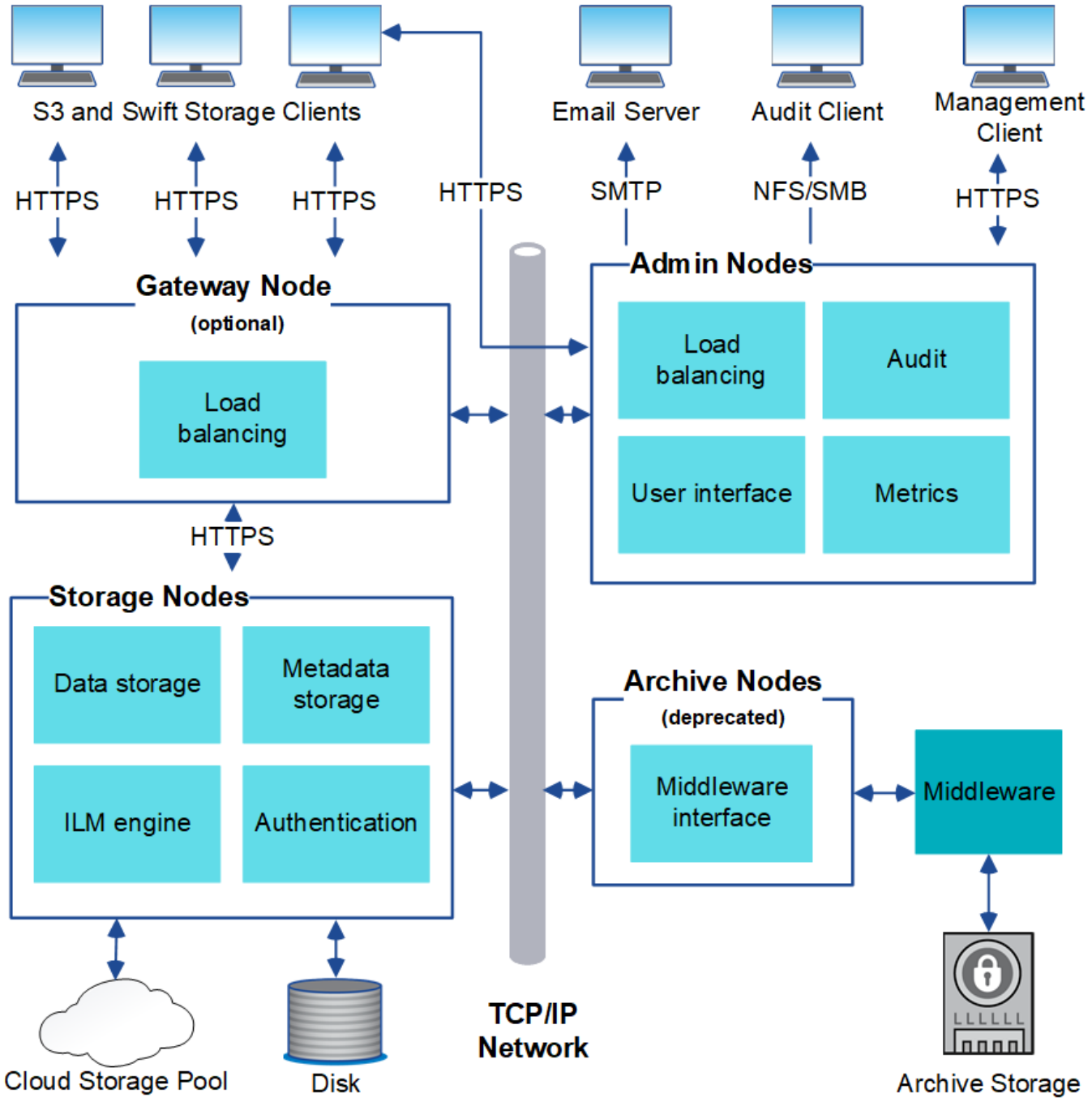
Vários locais lógicos também podem existir em um único data center para permitir o uso de replicação distribuída e codificação de apagamento para aumentar a disponibilidade e a resiliência.

Redundância de nó de grade

Em uma implantação de um único local ou de vários locais, você pode incluir opcionalmente mais de um nó de administrador ou nó de gateway para redundância. Por exemplo, você pode instalar mais de um nó de administrador em um único site ou em vários sites. No entanto, cada sistema StorageGRID só pode ter um nó de administração principal.

Arquitetura do sistema

Este diagrama mostra como os nós de grade são organizados dentro de um sistema StorageGRID.



Os clientes S3 armazenam e recuperam objetos no StorageGRID. Outros clientes são usados para enviar notificações por e-mail, acessar a interface de gerenciamento do StorageGRID e, opcionalmente, acessar o compartilhamento de auditoria.

Os clientes S3 podem se conetar a um nó de gateway ou a um nó de administrador para usar a interface de balanceamento de carga aos nós de storage. Como alternativa, os clientes S3 podem se conectar diretamente aos nós de storage usando HTTPS.

Os objetos podem ser armazenados no StorageGRID em nós de storage baseados em software ou hardware ou em pools de storage de nuvem, que consistem em buckets externos do S3 ou contêineres de storage Azure Blob.

Nós e serviços de grade

Nós e serviços de grade

O componente básico básico de um sistema StorageGRID é o nó de grade. Os nós contêm serviços, que são módulos de software que fornecem um conjunto de recursos para um nó de grade.

Tipos de nós de grade

O sistema StorageGRID usa quatro tipos de nós de grade:

Nós de administração

Fornecer serviços de gerenciamento, como configuração do sistema, monitoramento e logs. Quando você entra no Gerenciador de Grade, você está se conetando a um nó Admin. Cada grade deve ter um nó de administração principal e pode ter nós de administração não primários adicionais para redundância. Você pode se conetar a qualquer nó de administrador e cada nó de administrador exibe uma exibição semelhante do sistema StorageGRID. No entanto, os procedimentos de manutenção devem ser executados usando o nó de administração principal.

Os nós de administração também podem ser usados para equilibrar o tráfego de clientes S3.

Consulte "O que é um nó de administração?"

Nós de storage

Gerenciar e armazenar dados e metadados de objetos. Cada local do seu sistema StorageGRID precisa ter pelo menos três nós de storage.

Consulte "O que é um nó de storage?"

Nós de gateway (opcional)

Fornecer uma interface de balanceamento de carga que os aplicativos clientes podem usar para se conetar ao StorageGRID. Um balanceador de carga direciona os clientes de forma otimizada para um nó de storage ideal, de modo que a falha de nós ou até mesmo um local inteiro seja transparente.

Consulte "O que é um nó de gateway?"

Nós de hardware e software

Os nós do StorageGRID podem ser implantados como nós de dispositivos StorageGRID ou como nós baseados em software.

Nós de dispositivos StorageGRID

Os aparelhos de hardware StorageGRID são especialmente projetados para uso em um sistema StorageGRID. Alguns dispositivos podem ser usados como nós de storage. Outros dispositivos podem ser usados como nós de administrador ou nós de gateway. Você pode combinar nós de dispositivo com nós baseados em software ou implantar grades totalmente projetadas e totalmente compatíveis com dispositivos que não têm dependências de hipervisores externos, storage ou hardware de computação.

Consulte o seguinte para saber mais sobre os aparelhos disponíveis:

- "Documentação do StorageGRID Appliance"

- "NetApp Hardware Universe"

Nós baseados em software

Os nós de grade baseados em software podem ser implantados como máquinas virtuais VMware ou dentro dos mecanismos de contentor em um host Linux.

- Máquina virtual (VM) no VMware vSphere: "Instale o StorageGRID no VMware"Consulte .
- Dentro de um mecanismo de contentor no Red Hat Enterprise Linux: "Instale o StorageGRID no Red Hat Enterprise Linux"Consulte .
- Dentro de um motor de container no Ubuntu ou Debian: Veja "Instale o StorageGRID no Ubuntu ou Debian".

Utilize o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)" para determinar as versões suportadas.

Durante a instalação inicial de um novo nó de storage baseado em software, você pode especificar que ele só será usado "armazenar metadados"no .

Serviços da StorageGRID

A seguir está uma lista completa de serviços do StorageGRID.

Serviço	Descrição	Localização
Serviço de conta Forwarder	Fornece uma interface para o serviço Load Balancer para consultar o Serviço de conta em hosts remotos e fornece notificações de alterações de configuração do Load Balancer Endpoint no serviço Load Balancer.	Serviço de balanceamento de carga em nós de administração e nós de gateway
ADC (controlador de domínio administrativo)	Mantém informações de topologia, fornece serviços de autenticação e responde a consultas dos serviços LDR e CMN.	Pelo menos três nós de storage que contêm o serviço ADC em cada local
AMS (sistema de Gestão de Auditoria)	Monitora e Registra todos os eventos e transações do sistema auditados em um arquivo de log de texto.	Nós de administração
Cassandra Reaper	Executa reparos automáticos de metadados de objetos.	Nós de storage
Serviço de chunk	Gerencia dados codificados por apagamento e fragmentos de paridade.	Nós de storage
CMN (nó de gerenciamento de configuração)	Gerencia configurações e tarefas de grade em todo o sistema. Cada grade tem um serviço CMN.	Nó de administração principal
DDS (armazenamento de dados distribuídos)	Interfaces com o banco de dados Cassandra para gerenciar metadados de objetos.	Nós de storage

Serviço	Descrição	Localização
DMV (transferência de dados)	Move dados para pontos de extremidade da nuvem.	Nós de storage
IP dinâmico (dynip)	Monitora a grade para alterações dinâmicas de IP e atualiza configurações locais.	Todos os nós
Grafana	Usado para visualização de métricas no Gerenciador de Grade.	Nós de administração
Alta disponibilidade	Gerencia IPs virtuais de alta disponibilidade em nós configurados na página grupos de alta disponibilidade. Este serviço também é conhecido como o serviço keepalived.	Nós de administrador e gateway
Identidade (idnt)	Federa identidades de usuários do LDAP e do ative Directory.	Nós de storage que usam o serviço ADC
Árbitro lambda	Gerencia S3 Selecione SelectObjectContent Requests.	Todos os nós
Balanceador de carga (nginx-gw)	Fornece balanceamento de carga de tráfego S3 de clientes para nós de storage. O serviço Load Balancer pode ser configurado através da página de configuração Load Balancer Endpoints. Este serviço também é conhecido como o serviço nginx-gw.	Nós de administrador e gateway
LDR (router de distribuição local)	Gerencia o armazenamento e a transferência de conteúdo dentro da grade.	Nós de storage
MISCd Information Service Control Daemon	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
nginx	Atua como um mecanismo de autenticação e comunicação segura para vários serviços de grade (como Prometheus e Dynamic IP) para poder falar com serviços em outros nós através de APIs HTTPS.	Todos os nós
nginx-gw	Alimenta o serviço Load Balancer.	Nós de administrador e gateway

Serviço	Descrição	Localização
NMS (sistema de gerenciamento de rede)	Alimenta as opções de monitoramento, relatórios e configuração que são exibidas pelo Gerenciador de Grade.	Nós de administração
Persistência	Gerencia arquivos no disco raiz que precisam persistir ao longo de uma reinicialização.	Todos os nós
Prometheus	Coleta métricas de séries temporais de serviços em todos os nós.	Nós de administração
RSM (máquina de estado replicado)	Garante que as solicitações de serviço da plataforma sejam enviadas para seus respetivos endpoints.	Nós de storage que usam o serviço ADC
SSM (Monitor de status do servidor)	Monitora as condições de hardware e os relatórios para o serviço NMS.	Uma instância está presente em cada nó de grade
Trace Collector	Executa a coleta de rastreamento para coletar informações para uso pelo suporte técnico. O serviço de coletor de rastreamento usa software Jaeger de código aberto.	Nós de administração

O que é um nó de administração?

Os nós de administração fornecem serviços de gerenciamento, como configuração, monitoramento e log do sistema. Os nós de administração também podem ser usados para equilibrar o tráfego de clientes S3. Cada grade deve ter um nó de administração principal e pode ter qualquer número de nós de administração não primários para redundância.

Diferenças entre nós de administração primários e não primários

Quando você entra no Gerenciador de Grade ou no Gerenciador de Tenant, você está se conetando a um nó Admin. Você pode se conetar a qualquer nó de administrador e cada nó de administrador exibe uma exibição semelhante do sistema StorageGRID. No entanto, o nó de administração principal fornece mais funcionalidade do que os nós de administração não primários. Por exemplo, a maioria dos procedimentos de manutenção deve ser realizada a partir dos nós de administração primários.

A tabela resume os recursos dos nós de administração primários e não primários.

Recursos	Nó de administração principal	Nó de administração não primário
Inclui o AMS serviço	Sim	Sim
Inclui o CMN serviço	Sim	Não

Recursos	Nó de administração principal	Nó de administração não primário
Inclui o NMS serviço	Sim	Sim
Inclui o Prometheus serviço	Sim	Sim
Inclui o SSM serviço	Sim	Sim
Inclui os Balanceador de carga serviços eAlta disponibilidade	Sim	Sim
Suporta o Interface do Programa de aplicação de Gestão (mgmt-api)	Sim	Sim
Pode ser usado para todas as tarefas de manutenção relacionadas à rede, por exemplo, alteração de endereço IP e atualização de servidores NTP	Sim	Não
Pode executar o rebalanceamento de EC após a expansão do nó de storage	Sim	Não
Pode ser usado para o procedimento de restauração de volume	Sim	Sim
Pode coletar arquivos de log e dados do sistema de um ou mais nós	Sim	Não
Envia notificações de alerta, pacotes AutoSupport e traps SNMP e informa	Sim. Atua como o remetente preferido.	Sim. Atua como um remetente em espera.

nó Admin do remetente preferido

Se sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal é o remetente preferido para notificações de alerta, pacotes AutoSupport e traps SNMP e informa.

Em operações normais do sistema, apenas o remetente preferido envia notificações. No entanto, todos os outros nós de administração monitoram o remetente preferido. Se um problema for detetado, outros nós de administração agem como *remetentes de reserva*.

Várias notificações podem ser enviadas nesses casos:

- Se os nós de administração ficarem "isaterizados" uns dos outros, tanto o remetente preferido como os remetentes de reserva tentarão enviar notificações, e várias cópias de notificações podem ser recebidas.
- Se o remetente em espera detetar problemas com o remetente preferido e começar a enviar notificações, o remetente preferido pode recuperar sua capacidade de enviar notificações. Se isso ocorrer, notificações duplicadas podem ser enviadas. O remetente em espera deixará de enviar notificações quando não detetar mais erros no remetente preferido.

Quando você testa pacotes do AutoSupport, todos os nós de administração enviam o teste. Ao testar notificações de alerta, você deve entrar em cada nó de administração para verificar a conetividade.

Serviços primários para nós de administração

A tabela a seguir mostra os serviços primários para nós de administração; no entanto, essa tabela não lista todos os serviços de nó.

Serviço	Função de chave
sistema de Gestão de Auditoria (AMS)	Monitoriza a atividade e os eventos do sistema.
nó de gerenciamento de configuração (CMN)	Gerencia a configuração em todo o sistema.
alta disponibilidade	Gerencia endereços IP virtuais de alta disponibilidade para grupos de nós de administração e nós de gateway. **Nota:** este serviço também é encontrado em nós de Gateway.
balanceador de carga	Fornece balanceamento de carga de tráfego S3 de clientes para nós de storage. **Nota:** este serviço também é encontrado em nós de Gateway.
Interface de Programa de aplicação de Gestão (mgmt-api)	Processa solicitações da API de gerenciamento de grade e da API de gerenciamento do locatário.
sistema de Gestão de rede (NMS)	Fornece funcionalidade para o Gerenciador de Grade.
prometheus	Coleta e armazena métricas de séries temporais dos serviços em todos os nós.
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

O que é um nó de storage?

Os nós de storage gerenciam e armazenam dados e metadados de objetos. Os nós de storage incluem os serviços e processos necessários para armazenar, mover, verificar e recuperar dados de objetos e metadados em disco.

Cada local do seu sistema StorageGRID precisa ter pelo menos três nós de storage.

Tipos de nós de storage

Durante a instalação, você pode selecionar o tipo de nó de armazenamento que deseja instalar. Esses tipos estão disponíveis para nós de storage baseados em software e para nós de storage baseados no dispositivo que oferecem suporte ao recurso:

- Nó de storage combinado de dados e metadados
- Nó de storage somente de metadados
- Nó de storage somente de dados

Você pode selecionar o tipo de nó de armazenamento nestas situações:

- Ao instalar inicialmente um nó de storage
- Quando você adiciona um nó de storage durante a expansão do sistema StorageGRID

> Não é possível alterar o tipo depois que a instalação do nó de armazenamento estiver concluída.

Nó de storage de dados e metadados (combinado)

Por padrão, todos os novos nós de storage armazenarão dados de objetos e metadados. Esse tipo de nó de armazenamento é chamado de nó de armazenamento *combinado*.

Nó de storage somente de metadados

Usar um nó de armazenamento exclusivo para metadados pode fazer sentido se sua grade armazenar um número muito grande de objetos pequenos. A instalação da capacidade de metadados dedicada fornece um melhor equilíbrio entre o espaço necessário para um grande número de pequenos objetos e o espaço necessário para os metadados desses objetos. Além disso, os nós de storage somente de metadados hospedados em dispositivos de alta performance podem aumentar a performance.

Ao instalar nós somente metadados, a grade também deve conter um número mínimo de nós para o storage de dados:

- Para uma grade de um único local, configure pelo menos dois nós de storage combinados ou somente de dados.
- Para uma grade de vários locais, configure pelo menos um nó de armazenamento combinado ou somente de dados *por local*.

> Embora os nós de storage somente metadados contenham o Serviço LDR e possam processar solicitações de clientes do S3, a performance do StorageGRID pode não aumentar.

Nó de storage somente de dados

O uso de um nó de storage exclusivo para dados pode fazer sentido se seus nós de storage tiverem características de desempenho diferentes. Por exemplo, para aumentar potencialmente a performance, você pode ter nós de storage de disco giratório somente de dados e alta capacidade acompanhados por nós de storage de alta performance somente de metadados.

Ao instalar nós somente dados, a grade deve conter o seguinte:

- Um mínimo de dois nós de storage combinados ou somente de dados *por grade*
- Pelo menos um nó de storage combinado ou somente de dados *por local*
- Um mínimo de três nós de storage combinados ou somente de metadados *por local*

Serviços primários para nós de storage

A tabela a seguir mostra os serviços primários para nós de storage; no entanto, essa tabela não lista todos os serviços de nós.

> Alguns serviços, como o serviço ADC e o serviço RSM, normalmente existem apenas em três nós de storage em cada local.

Serviço	Função de chave
Conta (acct)	Gerencia contas de locatários.
Controlador de domínio administrativo (ADC)	Mantém a topologia e a configuração em toda a grade. **Nota**: Os nós de storage somente de dados não hospedam o serviço ADC. **Detalhes** O serviço controlador de domínio administrativo (ADC) autentica os nós de grade e suas conexões entre si. O serviço ADC é hospedado em um mínimo de três nós de storage em um local. O serviço ADC mantém informações de topologia, incluindo a localização e disponibilidade dos serviços. Quando um nó de grade requer informações de outro nó de grade ou uma ação a ser executada por outro nó de grade, ele entra em Contato com um serviço ADC para encontrar o melhor nó de grade para processar sua solicitação. Além disso, o serviço ADC retém uma cópia dos pacotes de configuração da implantação do StorageGRID, permitindo que qualquer nó de grade recupere informações de configuração atuais. Para facilitar operações distribuídas e desembarcadas, cada serviço ADC sincroniza certificados, pacotes de configuração e informações sobre serviços e topologia com os outros serviços ADC no sistema StorageGRID. Em geral, todos os nós de grade mantêm uma conexão com pelo menos um serviço ADC. Isso garante que os nós de grade estejam sempre acessando as informações mais recentes. Quando os nós de grade se conetam, eles armazenam em cache certificados de outros nós de grade, permitindo que os sistemas continuem funcionando com nós de grade conhecidos, mesmo quando um serviço ADC não está disponível. Novos nós de grade só podem estabelecer conexões usando um serviço ADC. A conexão de cada nó de grade permite que o serviço ADC colete informações de topologia. Essas informações de nó de grade incluem a carga da CPU, o espaço disponível em disco (se ele tiver armazenamento), os serviços suportados e o ID do site do nó de grade. Outros serviços pedem ao serviço ADC informações de topologia por meio de consultas de topologia. O serviço ADC responde a cada consulta com as informações mais recentes recebidas do sistema StorageGRID.

Serviço	Função de chave
Cassandra	Armazena e protege metadados de objetos. **Nota**: Os nós de storage somente de dados não hospedam o serviço Cassandra.
Cassandra Reaper	Executa reparos automáticos de metadados de objetos. **Nota**: Os nós de storage somente de dados não hospedam o serviço Cassandra Reaper.
Chunk	Gerencia dados codificados por apagamento e fragmentos de paridade.
Transferência de dados (dmv)	Move dados para Cloud Storage Pools.
Armazenamento de dados distribuídos (DDS)	Monitora o armazenamento de metadados de objetos. **Detalhes** Cada nó de armazenamento inclui o serviço armazenamento de dados distribuído (DDS). Esse serviço faz interface com o banco de dados Cassandra para executar tarefas em segundo plano nos metadados de objetos armazenados no sistema StorageGRID. O serviço DDS rastreia o número total de objetos ingeridos no sistema StorageGRID, bem como o número total de objetos ingeridos através de cada uma das interfaces suportadas do sistema (S3).
Identidade (idnt)	Federa identidades de usuários do LDAP e do ative Directory.

Serviço	Função de chave
Router de distribuição local (LDR)	Processa solicitações de protocolo de storage de objetos e gerencia dados de objetos em disco.

Serviço	Função de chave
Máquina de estado replicado (RSM)	Garante que as solicitações de serviços da plataforma S3 sejam enviadas para seus respetivos endpoints.
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

ardúo do sistema StorageGRID, manipulando cargas de transferência de dados e funções de tráfego de dados.

O serviço LDR lida com as seguintes tarefas:

- Consultas
- Atividade de gerenciamento do ciclo de vida das informações (ILM)
- Exclusão de objeto
- Storage de objetos
- Transferências de dados de objeto de outro serviço LDR (Storage Node)
- Gerenciamento de storage de dados
- Interface de protocolo S3

O serviço LDR também mapeia cada objeto S3 para seu UUID exclusivo.

Armazenamentos de objetos

O armazenamento de dados subjacente de um serviço LDR é dividido em um número fixo de armazenamentos de objetos (também conhecidos como volumes de armazenamento). Cada armazenamento de objetos é um ponto de montagem separado.

Os armazenamentos de objetos em um nó de armazenamento são identificados por um número hexadecimal de 0000 a 002F, que é conhecido como ID de volume. O espaço é reservado no primeiro armazenamento de objetos (volume 0) para metadados de objetos em um banco de dados Cassandra; qualquer espaço restante nesse volume é usado para dados de objeto. Todos os outros armazenamentos de objetos são usados exclusivamente para dados de objetos, o que inclui

não é configurável e executada automaticamente. Para obter detalhes, "Gerenciar o storage de metadados de objetos"consulte .

O que é um nó de gateway?

Os nós de gateway fornecem uma interface dedicada de balanceamento de carga que os aplicativos clientes S3 podem usar para se conetar ao StorageGRID. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo a carga de trabalho em vários nós de storage. Os nós de gateway são opcionais.

O serviço de balanceador de carga é incluído em todos os nós de administração e todos os nós de gateway. Ele executa o encerramento do TLS (Transport Layer Security) das solicitações do cliente, inspeciona as solicitações e estabelece novas conexões seguras aos nós de storage. O serviço Load Balancer direciona os clientes de forma otimizada para um nó de storage ideal, de modo que a falha de nós ou até mesmo um local inteiro seja transparente.

Você configura um ou mais pontos de extremidade do balanceador de carga para definir a porta e o protocolo de rede (HTTPS ou HTTP) que as solicitações de clientes de entrada e saída usarão para acessar os serviços do Load Balancer nos nós Gateway e Admin. O ponto de extremidade do balanceador de carga também define o tipo de cliente (S3), o modo de encadernação e, opcionalmente, uma lista de locatários permitidos ou bloqueados. "Considerações para balanceamento de carga" Consulte .

Conforme necessário, você pode agrupar as interfaces de rede de vários nós de gateway e nós de administrador em um grupo de alta disponibilidade (HA). Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho do aplicativo cliente. "Gerenciar grupos de alta disponibilidade (HA)"Consulte .

Serviços primários para nós de gateway

A tabela a seguir mostra os serviços primários para nós de Gateway, no entanto, essa tabela não lista todos os serviços de nós.

Serviço	Função de chave
Alta disponibilidade	Gerencia endereços IP virtuais de alta disponibilidade para grupos de nós de administração e nós de gateway. **Observação:** este serviço também é encontrado em nós de administração.
Balanceador de carga	Fornece balanceamento de carga de camada 7 do tráfego S3 de clientes para nós de storage. Este é o mecanismo de balanceamento de carga recomendado. **Observação:** este serviço também é encontrado em nós de administração.

Serviço	Função de chave
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

O que é um nó de arquivo?

O suporte para nós de arquivamento foi removido.

Para obter informações sobre nós de arquivo, "O que é um nó de arquivo (StorageGRID 11,8 doc site)"consulte .

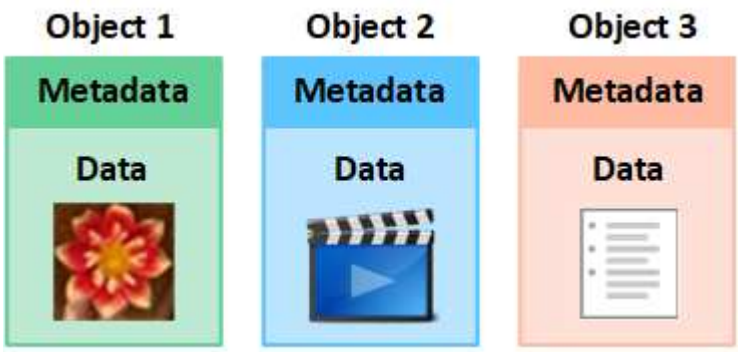
Como o StorageGRID gerencia dados

O que é um objeto

Com o armazenamento de objetos, a unidade de armazenamento é um objeto, em vez de um arquivo ou um bloco. Ao contrário da hierarquia semelhante a uma árvore de um sistema de arquivos ou armazenamento em bloco, o armazenamento de objetos organiza os dados em um layout plano e não estruturado.

O armazenamento de objetos separa a localização física dos dados do método usado para armazenar e recuperar esses dados.

Cada objeto em um sistema de storage baseado em objeto tem duas partes: Dados de objeto e metadados de objeto.



O que são dados de objeto?

Os dados do objeto podem ser qualquer coisa; por exemplo, uma fotografia, um filme ou um Registro médico.

O que é metadados de objetos?

Metadados de objetos são qualquer informação que descreva um objeto. O StorageGRID usa metadados de objetos para rastrear os locais de todos os objetos na grade e gerenciar o ciclo de vida de cada objeto ao longo do tempo.

Os metadados de objeto incluem informações como as seguintes:

- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket do S3 ou do contentor Swift, 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.

- O local de storage atual de cada cópia de objeto ou fragmento codificado de apagamento.
- Quaisquer metadados de usuário associados ao objeto.

Os metadados de objetos são personalizáveis e expansíveis, tornando-os flexíveis para uso dos aplicativos.

Para obter informações detalhadas sobre como e onde o StorageGRID armazena metadados de objetos, vá para "Gerenciar o storage de metadados de objetos".

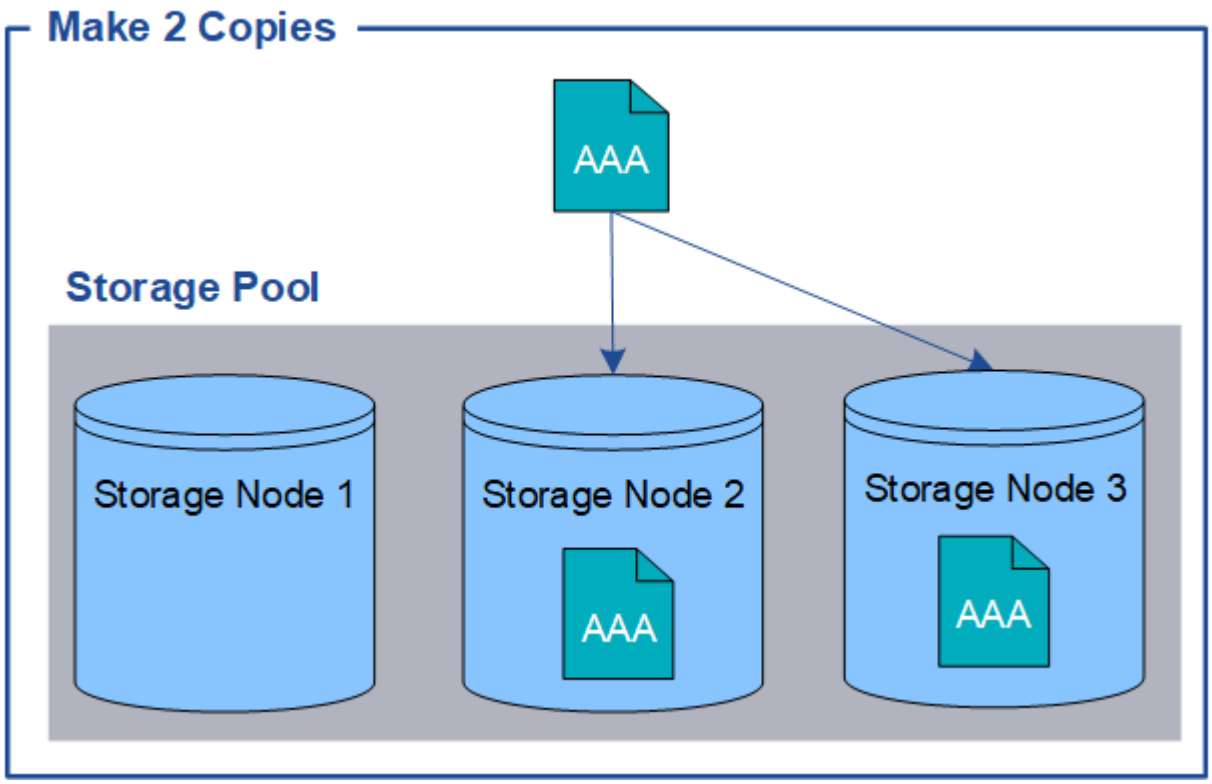
Como os dados do objeto são protegidos?

O sistema StorageGRID fornece dois mecanismos para proteger os dados de objetos contra perda: Replicação e codificação de apagamento.

Replicação

Quando o StorageGRID faz a correspondência de objetos a uma regra de gerenciamento do ciclo de vida das informações (ILM) configurada para criar cópias replicadas, o sistema cria cópias exatas de dados de objetos e os armazena em nós de storage ou pools de storage de nuvem. As regras do ILM determinam o número de cópias feitas, onde essas cópias são armazenadas e por quanto tempo elas são mantidas pelo sistema. Se uma cópia for perdida, por exemplo, como resultado da perda de um nó de armazenamento, o objeto ainda estará disponível se uma cópia dele existir em outro lugar do sistema StorageGRID.

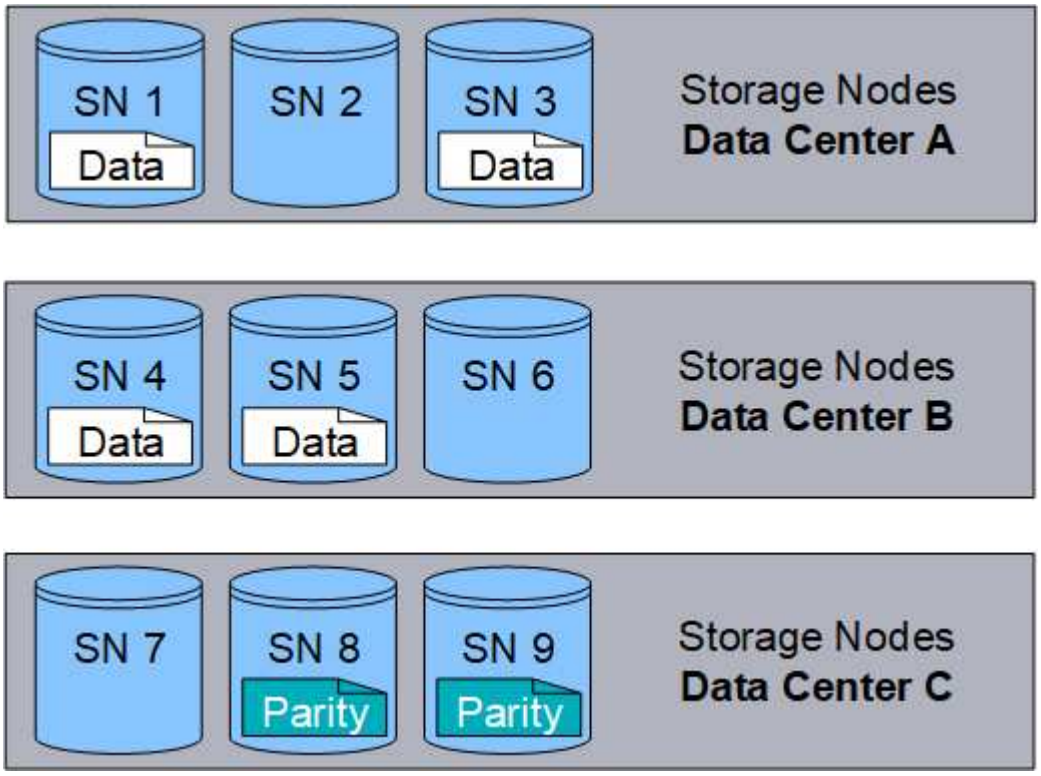
No exemplo a seguir, a regra fazer 2 cópias especifica que duas cópias replicadas de cada objeto serão colocadas em um pool de storage que contém três nós de storage.



Codificação de apagamento

Quando o StorageGRID faz a correspondência de objetos a uma regra ILM configurada para criar cópias codificadas por apagamento, ele corta dados de objetos em fragmentos de dados, calcula fragmentos de paridade adicionais e armazena cada fragmento em um nó de storage diferente. Quando um objeto é acessado, ele é remontado usando os fragmentos armazenados. Se um dado ou um fragmento de paridade ficar corrompido ou perdido, o algoritmo de codificação de apagamento pode recriar esse fragmento usando um subconjunto dos dados restantes e fragmentos de paridade. As regras do ILM e os perfis de codificação de apagamento determinam o esquema de codificação de apagamento usado.

O exemplo a seguir ilustra o uso da codificação de apagamento nos dados de um objeto. Neste exemplo, a regra ILM usa um esquema de codificação de apagamento 4-2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados do objeto. Cada um dos seis fragmentos é armazenado em um nó de storage diferente em três data centers para fornecer proteção de dados para falhas de nós ou perda do local.



Informações relacionadas

- "Gerenciar objetos com ILM"
- "Use o gerenciamento do ciclo de vida das informações"

A vida de um objeto

A vida de um objeto consiste em vários estágios. Cada etapa representa as operações que ocorrem com o objeto.

A vida útil de um objeto inclui as operações de ingestão, gerenciamento de cópias, recuperação e exclusão.

- **Ingest**: O processo de um aplicativo cliente S3 salvando um objeto em HTTP para o sistema StorageGRID. Nesta fase, o sistema StorageGRID começa a gerenciar o objeto.
- **Gerenciamento de cópias**: O processo de gerenciamento de cópias replicadas e codificadas de

apagamento no StorageGRID, conforme descrito pelas regras do ILM nas políticas ativas do ILM. Durante a etapa de gerenciamento de cópias, o StorageGRID protege os dados de objetos contra perda, criando e mantendo o número e o tipo especificados de cópias de objetos em nós de storage ou em um pool de storage de nuvem.

- **Retrieve**: O processo de um aplicativo cliente acessando um objeto armazenado pelo sistema StorageGRID. O cliente lê o objeto, que é recuperado de um nó de storage ou pool de armazenamento em nuvem.
- **Delete**: O processo de remoção de todas as cópias de objetos da grade. Os objetos podem ser excluídos como resultado do aplicativo cliente enviando uma solicitação de exclusão para o sistema StorageGRID ou como resultado de um processo automático que o StorageGRID executa quando a vida útil do objeto expira.

Informações relacionadas

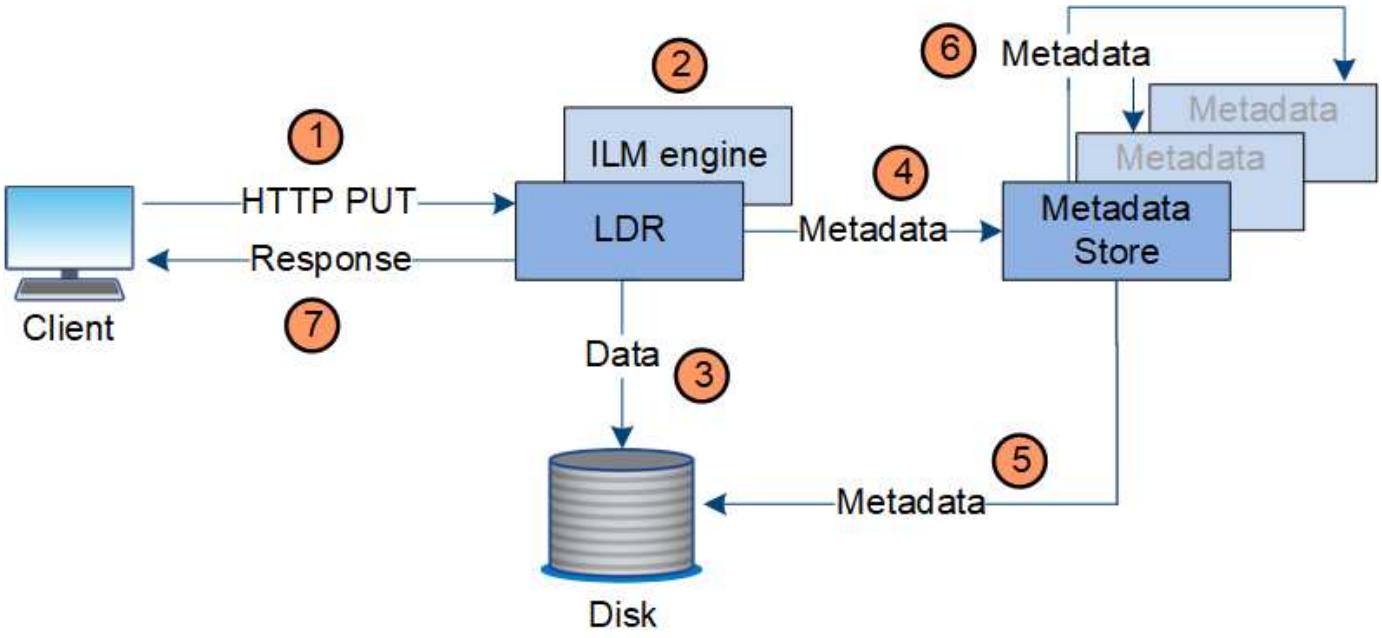
- "Gerenciar objetos com ILM"
- "Use o gerenciamento do ciclo de vida das informações"

Ingira o fluxo de dados

Uma operação de ingestão ou salvamento consiste em um fluxo de dados definido entre o cliente e o sistema StorageGRID.

Fluxo de dados

Quando um cliente ingere um objeto ao sistema StorageGRID, o serviço LDR em nós de armazenamento processa a solicitação e armazena os metadados e dados no disco.



1. O aplicativo cliente cria o objeto e o envia para o sistema StorageGRID por meio de uma solicitação HTTP PUT.
2. O objeto é avaliado em relação à política ILM do sistema.
3. O serviço LDR salva os dados do objeto como uma cópia replicada ou como uma cópia codificada por apagamento. (O diagrama mostra uma versão simplificada de armazenar uma cópia replicada no disco.)
4. O serviço LDR envia os metadados do objeto para o armazenamento de metadados.
5. O armazenamento de metadados salva os metadados do objeto no disco.
6. O armazenamento de metadados propaga cópias de metadados de objetos para outros nós de storage. Essas cópias também são salvas no disco.
7. O serviço LDR retorna uma resposta HTTP 200 OK ao cliente para reconhecer que o objeto foi ingerido.

Gerenciamento de cópias

Os dados de objeto são gerenciados pelas políticas ativas do ILM e pelas regras associadas do ILM. As regras de ILM fazem cópias replicadas ou codificadas por apagamento para proteger os dados de objetos contra perda.

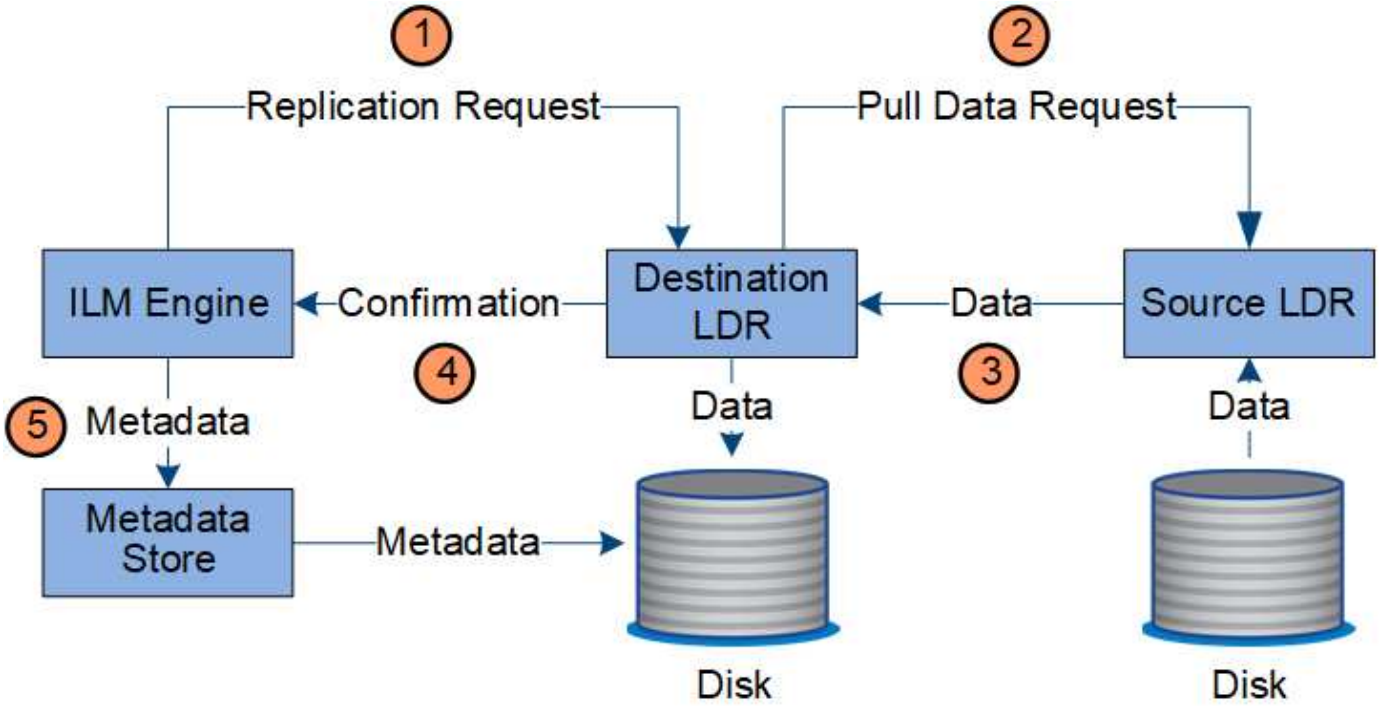
Diferentes tipos ou locais de cópias de objetos podem ser necessários em momentos diferentes na vida do objeto. As regras do ILM são periodicamente avaliadas para garantir que os objetos sejam colocados conforme necessário.

Os dados do objeto são geridos pelo serviço LDR.

Proteção de conteúdo: Replicação

Se as instruções de posicionamento de conteúdo de uma regra ILM exigirem cópias replicadas de dados de objetos, as cópias serão feitas e armazenadas no disco pelos nós de storage que compõem o pool de storage configurado.

O mecanismo ILM no serviço LDR controla a replicação e garante que o número correto de cópias seja armazenado nos locais corretos e durante o período de tempo correto.

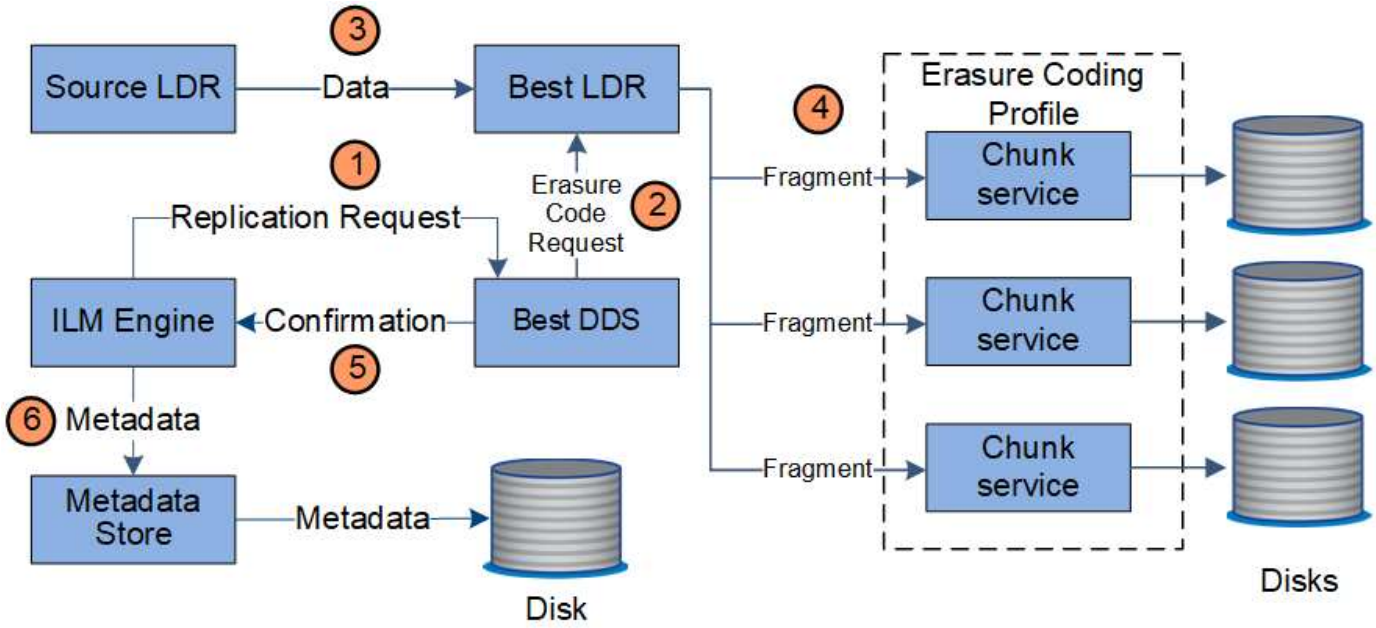


1. O mecanismo ILM consulta o serviço ADC para determinar o melhor serviço LDR de destino dentro do pool de armazenamento especificado pela regra ILM. Em seguida, envia um comando para iniciar a replicação ao serviço LDR.
2. O serviço LDR de destino consulta o serviço ADC para obter a melhor localização de origem. Em seguida, envia uma solicitação de replicação para o serviço LDR de origem.
3. O serviço LDR de origem envia uma cópia para o serviço LDR de destino.
4. O serviço LDR de destino notifica o mecanismo ILM de que os dados do objeto foram armazenados.
5. O mecanismo ILM atualiza o armazenamento de metadados com metadados de localização de objetos.

Proteção de conteúdo: Codificação de apagamento

Se uma regra de ILM incluir instruções para fazer cópias codificadas para apagamento de dados de objetos, o esquema de codificação de apagamento aplicável quebra os dados de objetos em dados e fragmentos de paridade e distribui esses fragmentos entre os nós de storage configurados no perfil de codificação de apagamento.

O mecanismo ILM, que é um componente do serviço LDR, controla a codificação de apagamento e garante que o perfil de codificação de apagamento seja aplicado aos dados do objeto.

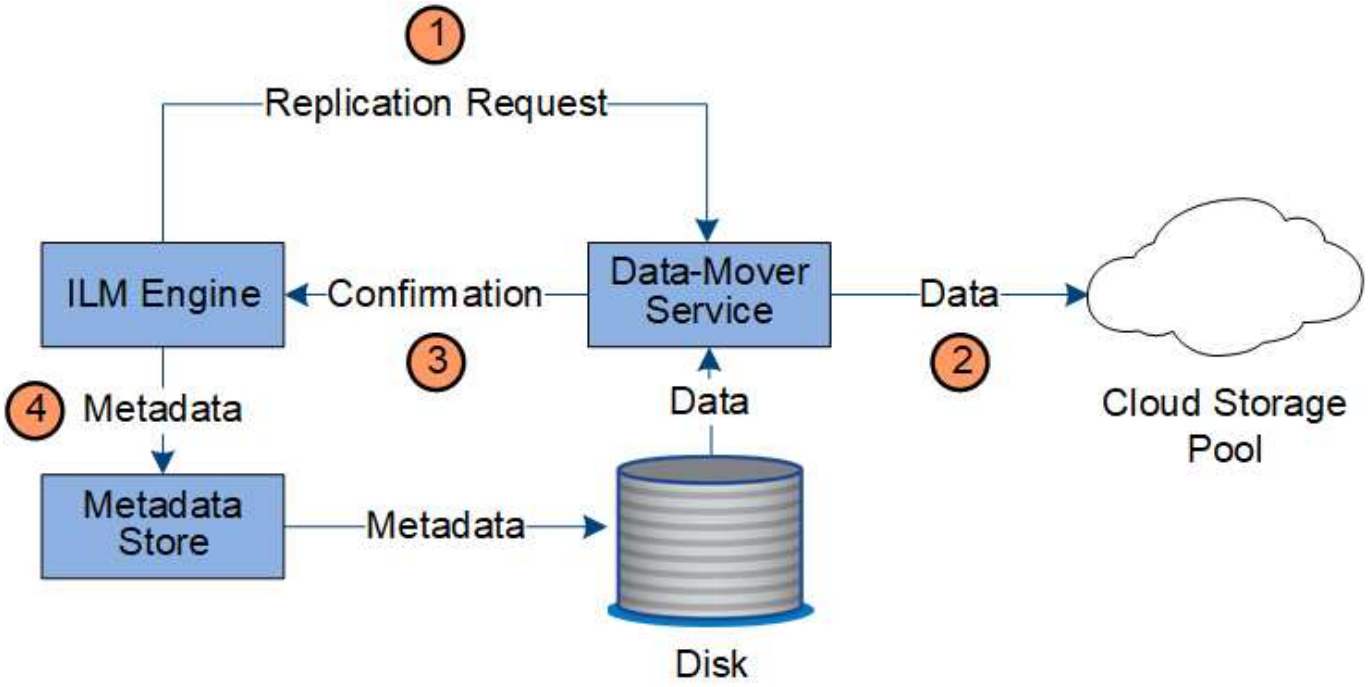


1. O mecanismo ILM consulta o serviço ADC para determinar qual serviço DDS pode executar melhor a operação de codificação de apagamento. Quando determinado, o motor ILM envia uma solicitação de "iniciar" para esse serviço.
2. O serviço DDS instrui um LDR a apagar os dados do objeto.
3. O serviço LDR de origem envia uma cópia para o serviço LDR selecionado para codificação de apagamento.
4. Depois de criar o número apropriado de paridade e fragmentos de dados, o serviço LDR distribui esses fragmentos pelos nós de armazenamento (serviços Chunk) que compõem o pool de armazenamento do perfil de codificação de apagamento.
5. O serviço LDR notifica o mecanismo ILM, confirmando que os dados do objeto são distribuídos com sucesso.
6. O mecanismo ILM atualiza o armazenamento de metadados com metadados de localização de objetos.

Proteção de conteúdo: Cloud Storage Pool

Se as instruções de posicionamento de conteúdo de uma regra ILM exigirem que uma cópia replicada dos dados de objetos seja armazenada em um Cloud Storage Pool, os dados de objetos serão duplicados para o bucket externo do S3 ou para o contêiner de storage Azure Blob especificado para o Cloud Storage Pool.

O mecanismo ILM, que é um componente do serviço LDR, e o serviço Data Mover controlam o movimento de objetos para o Cloud Storage Pool.



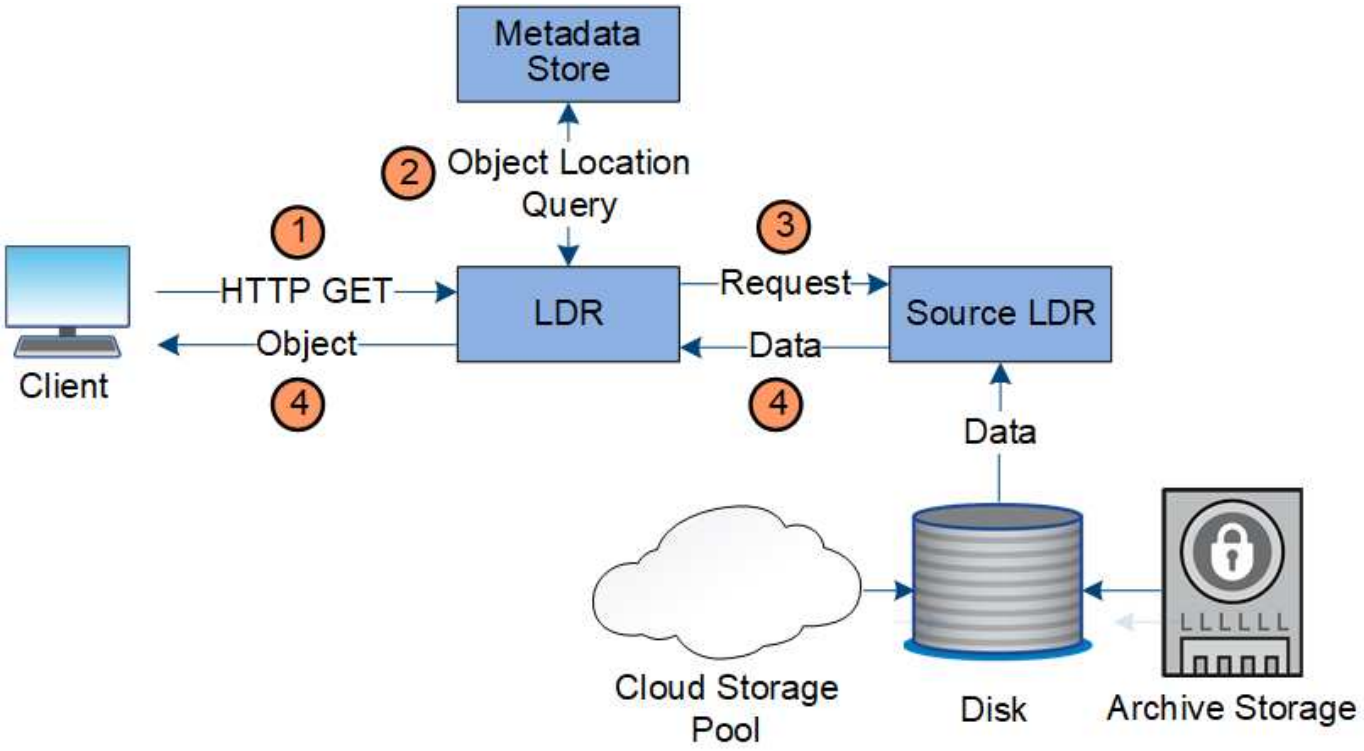
1. O mecanismo ILM seleciona um serviço Data Mover para replicação no Cloud Storage Pool.
2. O serviço Data Mover envia os dados do objeto para o Cloud Storage Pool.
3. O serviço Data Mover notifica o mecanismo ILM de que os dados do objeto foram armazenados.
4. O mecanismo ILM atualiza o armazenamento de metadados com metadados de localização de objetos.

Recuperar fluxo de dados

Uma operação de recuperação consiste em um fluxo de dados definido entre o sistema StorageGRID e o cliente. O sistema usa atributos para rastrear a recuperação do objeto de um nó de armazenamento ou, se necessário, um pool de armazenamento em nuvem.

O serviço LDR do nó de armazenamento consulta o armazenamento de metadados para a localização dos dados do objeto e recupera-os do serviço LDR de origem. Preferencialmente, a recuperação é de um nó de armazenamento. Se o objeto não estiver disponível em um nó de armazenamento, a solicitação de recuperação será direcionada para um pool de armazenamento em nuvem.

Se a única cópia de objeto estiver no armazenamento do AWS Glacier ou no nível do Azure Archive, o aplicativo cliente deverá emitir uma solicitação de S3 RestoreObject para restaurar uma cópia recuperável para o Cloud Storage Pool.



1. O serviço LDR recebe um pedido de recuperação da aplicação cliente.
2. O serviço LDR consulta o armazenamento de metadados para a localização de dados do objeto e metadados.
3. O serviço LDR encaminha o pedido de recuperação para o serviço LDR de origem.
4. O serviço LDR de origem retorna os dados do objeto do serviço LDR consultado e o sistema retorna o objeto para o aplicativo cliente.

Eliminar fluxo de dados

Todas as cópias de objetos são removidas do sistema StorageGRID quando um cliente executa uma operação de exclusão ou quando a vida útil do objeto expira, acionando sua remoção automática. Há um fluxo de dados definido para exclusão de objeto.

Hierarquia de exclusão

O StorageGRID fornece vários métodos para controlar quando objetos são retidos ou excluídos. Os objetos podem ser excluídos por solicitação do cliente ou automaticamente. O StorageGRID sempre prioriza quaisquer configurações de bloqueio de objetos S3 sobre solicitações de exclusão do cliente, que são priorizadas sobre o ciclo de vida do bucket S3 e instruções de posicionamento do ILM.

- **S3 Object Lock**: Se a configuração global S3 Object Lock estiver ativada para a grade, os clientes S3 podem criar buckets com o S3 Object Lock ativado e, em seguida, usar a API REST S3 para especificar as configurações de retenção legal e de retenção para cada versão de objeto adicionada a esse bucket.
  - Uma versão de objeto que está sob uma retenção legal não pode ser excluída por nenhum método.
  - Antes que a data de retenção de uma versão de objeto seja alcançada, essa versão não pode ser excluída por nenhum método.
  - Objetos em buckets com o bloqueio de objetos S3 ativado são retidos pelo ILM "Forever". No entanto, após a data de retenção ser alcançada, uma versão de objeto pode ser excluída por uma solicitação

de cliente ou pela expiração do ciclo de vida do bucket.

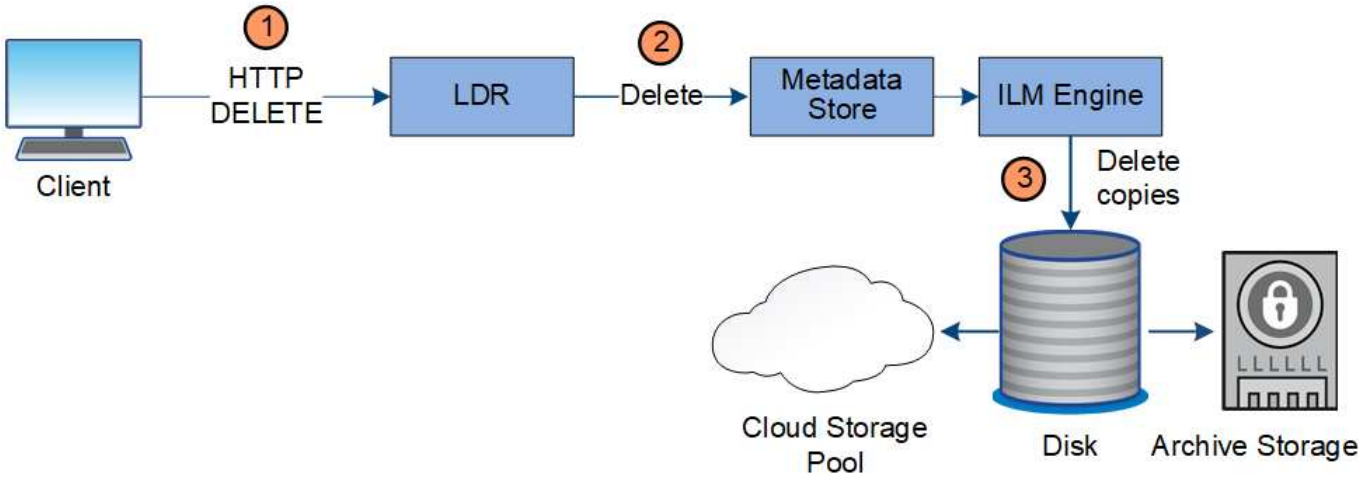
  - Se os clientes S3 aplicarem uma data retida-até-data padrão ao intervalo, eles não precisarão especificar uma data retida-até para cada objeto.

- **Solicitação de exclusão de cliente**: Um cliente S3 pode emitir uma solicitação de exclusão de objeto. Quando um cliente exclui um objeto, todas as cópias do objeto são removidas do sistema StorageGRID.
- **Excluir objetos no bucket**: Os usuários do Gerenciador de locatários podem usar essa opção para remover permanentemente todas as cópias dos objetos e versões de objetos em buckets selecionados do sistema StorageGRID.
- **Ciclo de vida do bucket do S3**: Os clientes do S3 podem adicionar uma configuração do ciclo de vida aos buckets que especifica uma ação de expiração. Se existir um ciclo de vida de bucket, o StorageGRID excluirá automaticamente todas as cópias de um objeto quando a data ou o número de dias especificados na ação de expiração forem atendidos, a menos que o cliente exclua o objeto primeiro.
- **Instruções de colocação de ILM**: Supondo que o bucket não tenha o bloqueio de objeto S3 ativado e que não haja ciclo de vida de bucket, o StorageGRID exclui automaticamente um objeto quando o último período de tempo na regra ILM termina e não há mais colocações especificadas para o objeto.

> Quando um ciclo de vida do bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política do ILM para objetos que correspondem ao filtro do ciclo de vida. Como resultado, um objeto pode ser retido na grade mesmo depois que quaisquer instruções ILM para colocar o objeto tenham expirado.

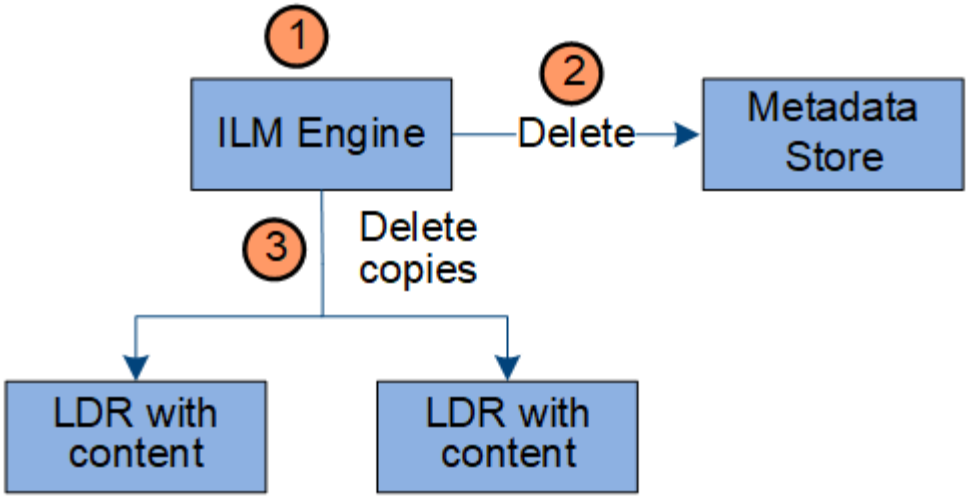
Consulte "Como os objetos são excluídos" para obter mais informações.

Fluxo de dados para exclusões do cliente



1. O serviço LDR recebe uma solicitação de exclusão do aplicativo cliente.
2. O serviço LDR atualiza o armazenamento de metadados para que o objeto pareça excluído às solicitações do cliente e instrui o mecanismo ILM a remover todas as cópias dos dados do objeto.
3. O objeto é removido do sistema. O armazenamento de metadados é atualizado para remover metadados de objetos.

Fluxo de dados para exclusões de ILM



1. O mecanismo ILM determina que o objeto precisa ser excluído.
2. O mecanismo ILM notifica o armazenamento de metadados. O armazenamento de metadados atualiza os metadados de objetos para que o objeto pareça excluído para solicitações de cliente.
3. O mecanismo ILM remove todas as cópias do objeto. O armazenamento de metadados é atualizado para remover metadados de objetos.

Gerenciamento do ciclo de vida das informações

Use o gerenciamento do ciclo de vida das informações (ILM) para controlar o posicionamento, a duração e o comportamento de ingestão de todos os objetos no sistema StorageGRID. As regras do ILM determinam como o StorageGRID armazena objetos ao longo do tempo. Você configura uma ou mais regras ILM e as adiciona a uma política ILM.

Uma grade tem apenas uma política ativa de cada vez. Uma política pode conter várias regras.

As regras do ILM definem:

- Quais objetos devem ser armazenados. Uma regra pode ser aplicada a todos os objetos ou você pode especificar filtros para identificar quais objetos uma regra se aplica. Por exemplo, uma regra só pode se aplicar a objetos associados a determinadas contas de locatário, buckets específicos do S3 ou contentores Swift ou valores específicos de metadados.
- O tipo de armazenamento e a localização. Os objetos podem ser armazenados em nós de storage ou em Cloud Storage Pools.
- O tipo de cópias de objeto feitas. As cópias podem ser replicadas ou codificadas para apagamento.
- Para cópias replicadas, o número de cópias feitas.
- Para cópias codificadas para apagamento, o esquema de codificação de apagamento usado.
- As alterações ao longo do tempo para o local de armazenamento de um objeto e tipo de cópias.
- Como os dados do objeto são protegidos à medida que os objetos são ingeridos na grade (colocação síncrona ou commit duplo).

Observe que os metadados de objetos não são gerenciados pelas regras do ILM. Em vez disso, os metadados de objetos são armazenados em um banco de dados Cassandra no que é conhecido como armazenamento de metadados. Três cópias dos metadados de objetos são mantidas automaticamente em

cada local para proteger os dados da perda.

Exemplo de regra ILM

Como exemplo, uma regra ILM pode especificar o seguinte:

- Aplicar apenas aos objetos pertencentes ao Locatário A..
- Faça duas cópias replicadas desses objetos e armazene cada cópia em um local diferente.
- Guarde as duas cópias "para sempre", o que significa que o StorageGRID não as eliminará automaticamente. Em vez disso, o StorageGRID manterá esses objetos até que sejam excluídos por uma solicitação de exclusão de cliente ou pela expiração de um ciclo de vida de bucket.
- Use a opção equilibrada para comportamento de ingestão: A instrução de colocação de dois locais é aplicada assim que o locatário A salva um objeto no StorageGRID, a menos que não seja possível fazer imediatamente ambas as cópias necessárias.

  Por exemplo, se o local 2 estiver inacessível quando o locatário A salva um objeto, o StorageGRID fará duas cópias provisórias nos nós de storage no local 1. Assim que o Site 2 estiver disponível, a StorageGRID fará a cópia necessária nesse site.

Como uma política ILM avalia objetos

As políticas de ILM ativas para o seu sistema StorageGRID controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos.

Quando os clientes salvam objetos no StorageGRID, os objetos são avaliados em relação ao conjunto ordenado de regras ILM na política ativa, da seguinte forma:

1. Se os filtros da primeira regra na política corresponderem a um objeto, o objeto será ingerido de acordo com o comportamento de ingestão dessa regra e armazenado de acordo com as instruções de colocação dessa regra.
2. Se os filtros da primeira regra não corresponderem ao objeto, o objeto será avaliado em relação a cada regra subsequente na política até que uma correspondência seja feita.
3. Se nenhuma regra corresponder a um objeto, as instruções de comportamento de ingestão e posicionamento da regra padrão na política serão aplicadas. A regra padrão é a última regra de uma política e não pode usar nenhum filtro. Ele deve se aplicar a todos os locatários, todos os buckets e todas as versões de objetos.

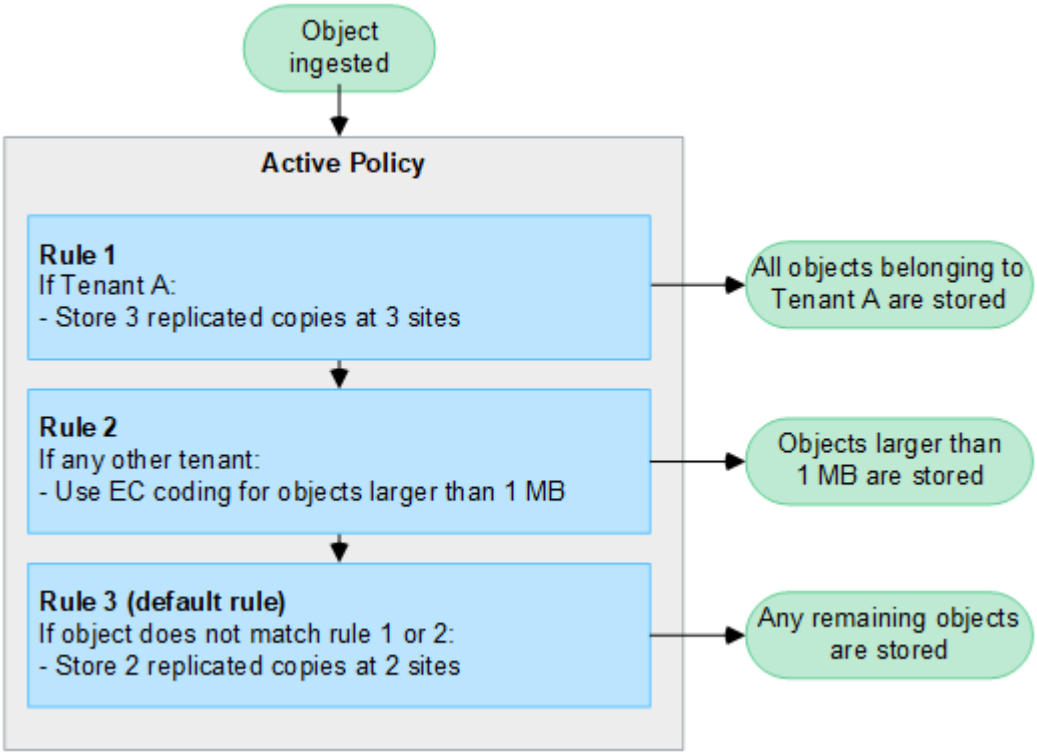
Exemplo de política ILM

Como exemplo, uma política ILM pode conter três regras ILM que especificam o seguinte:

- **Regra 1: Cópias replicadas para o locatário A**
  - Corresponder todos os objetos pertencentes ao locatário A..
  - Armazene esses objetos como três cópias replicadas em três locais.
  - Objetos pertencentes a outros inquilinos não são correspondidos pela regra 1, portanto, eles são avaliados em relação à regra 2.
- **Regra 2: Codificação de apagamento para objetos com mais de 1 MB**
  - Combine todos os objetos de outros inquilinos, mas somente se eles forem maiores que 1 MB. Esses objetos maiores são armazenados usando codificação de apagamento 6-3 em três locais.

- Não corresponde a objetos de 1 MB ou menores, portanto, esses objetos são avaliados em relação à regra 3.

- **Regra 3: 2 cópias 2 data centers** (padrão)
  - É a última regra e padrão na política. Não utiliza filtros.
  - Faça duas cópias replicadas de todos os objetos não correspondidos pela regra 1 ou regra 2 (objetos não pertencentes ao locatário A que tenham 1 MB ou menos).



Informações relacionadas

- "Gerenciar objetos com ILM"

Explore o StorageGRID

Explore o Gerenciador de Grade

O Gerenciador de Grade é a interface gráfica baseada em navegador que permite configurar, gerenciar e monitorar seu sistema StorageGRID.

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

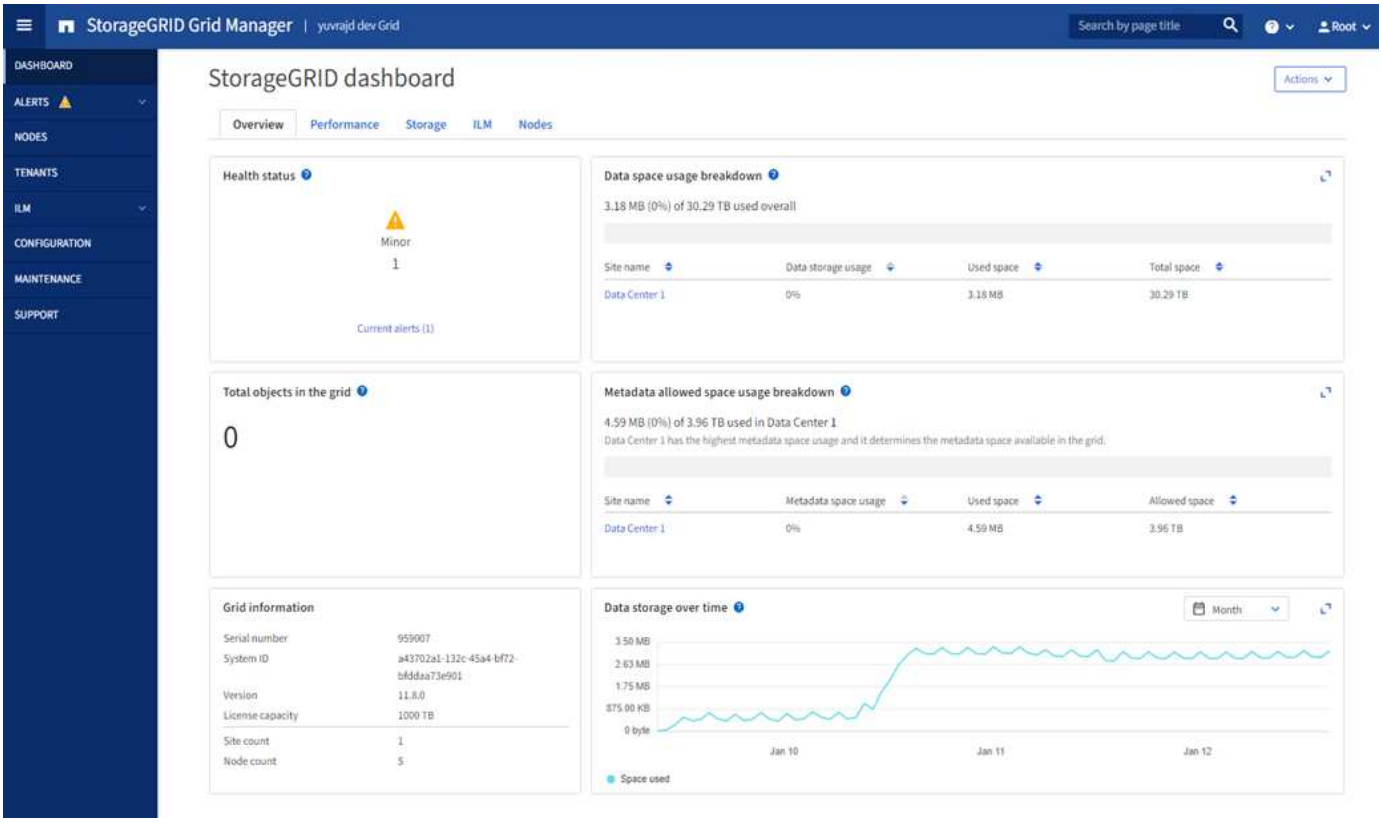
Quando você entra no Gerenciador de Grade, você está se conetando a um nó Admin. Cada sistema StorageGRID inclui um nó de administração principal e qualquer número de nós de administração não primários. Você pode se conetar a qualquer nó de administrador e cada nó de administrador exibe uma exibição semelhante do sistema StorageGRID.

Você pode acessar o Gerenciador de Grade usando um "navegador da web suportado".

Painel do Grid Manager

Ao iniciar sessão pela primeira vez no Gestor de grelha, pode utilizar o painel para "monitorar as atividades do sistema" o visualizar rapidamente.

O dashboard contém informações sobre a integridade e a performance do sistema, o uso do storage, os processos de ILM, as operações S3 e os nós na grade. "configure o painel de instrumentos"Pode selecionar a partir de uma coleção de cartões que contêm as informações de que necessita para monitorizar eficazmente o seu sistema.



Para obter uma explicação das informações apresentadas em cada cartão, selecione o ícone de ajuda para esse cartão.

Campo de pesquisa

O campo **Search** na barra de cabeçalho permite que você navegue rapidamente para uma página específica dentro do Gerenciador de Grade. Por exemplo, você pode inserir **km** para acessar a página servidor de gerenciamento de chaves (KMS).

Você pode usar **Search** para encontrar entradas na barra lateral do Gerenciador de Grade e nos menus Configuração, Manutenção e suporte. Você também pode pesquisar por nome itens como nós de grade e contas de locatário.

Menu Ajuda

O menu de ajuda fornece acesso a:

- O "FabricPool"assistente e"Configuração S3"
- O centro de documentação do StorageGRID para a versão atual
- "Documentação do API"

- Informações sobre qual versão do StorageGRID está instalada atualmente

Menu de alertas

O menu Alertas fornece uma interface fácil de usar para detetar, avaliar e resolver problemas que possam ocorrer durante a operação do StorageGRID.

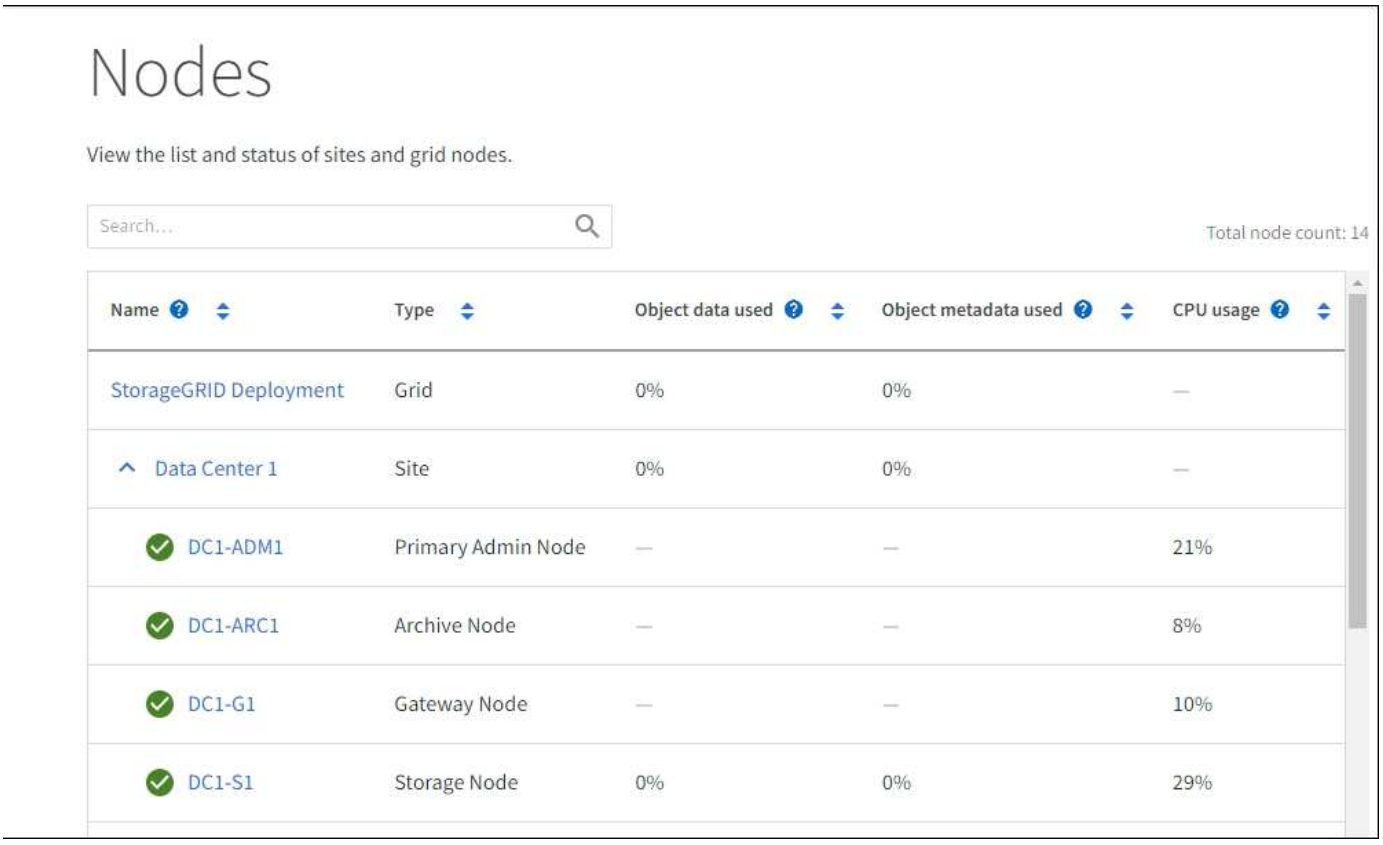
No menu Alertas, você pode fazer o seguinte para"gerenciar alertas":

- Reveja os alertas atuais
- Reveja os alertas resolvidos
- Configure silêncios para suprimir notificações de alerta
- Defina regras de alerta para condições que acionam alertas
- Configure o servidor de e-mail para receber notificações de alerta

Página de nós

O "Página de nós" exibe informações sobre toda a grade, cada local na grade e cada nó em um local.

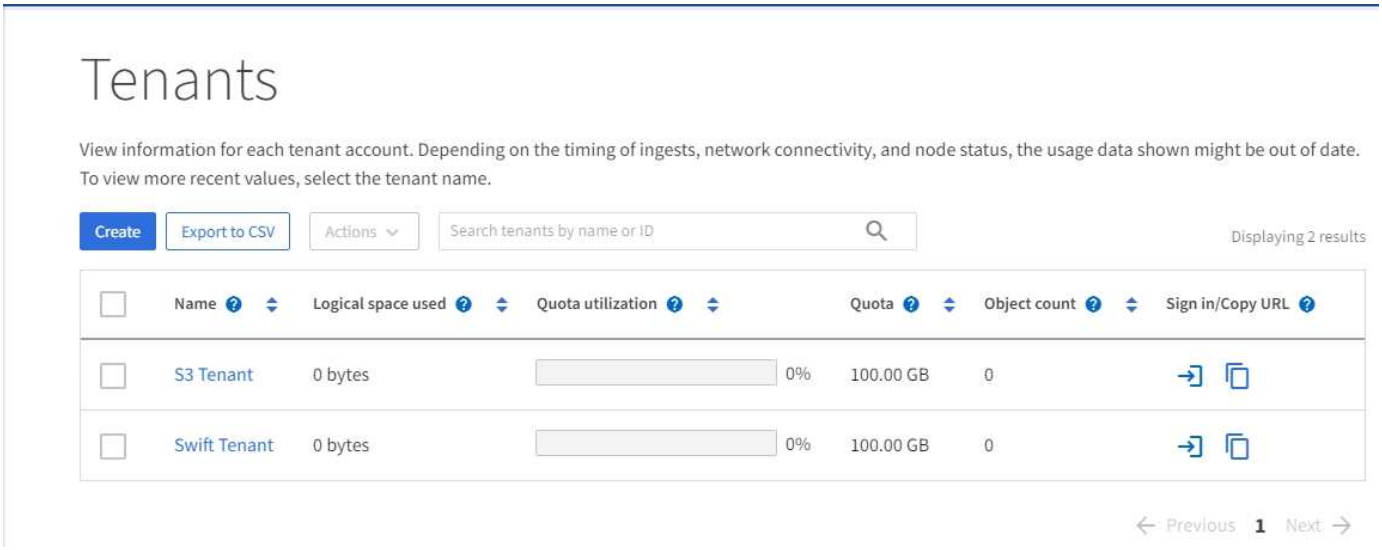
A home page dos nós exibe métricas combinadas para toda a grade. Para exibir informações de um site ou nó específico, selecione o site ou nó.



Página de inquilinos

O "Página de inquilinos" permite-lhe "crie e monitore as contas de locatários de storage"utilizar o seu sistema StorageGRID. Você deve criar pelo menos uma conta de locatário para especificar quem pode armazenar e recuperar objetos e qual funcionalidade está disponível para eles.

A página locatários também fornece detalhes de uso para cada locatário, incluindo a quantidade de storage usada e o número de objetos. Se você definir uma cota quando criou o locatário, poderá ver quanto dessa cota foi usada.



Menu ILM

O "Menu ILM" permite que "Configurar as regras e políticas de gerenciamento do ciclo de vida das informações (ILM)"você governe a durabilidade e a disponibilidade dos dados. Você também pode inserir um identificador de objeto para exibir os metadados desse objeto.

No menu ILM, você pode visualizar e gerenciar ILM:

- Regras
- Políticas
- Etiquetas de política
- Pools de armazenamento
- Classes de armazenamento
- Regiões
- Pesquisa de metadados de objetos

Menu de configuração

O menu Configuração permite especificar as definições de rede, as definições de segurança, as definições do sistema, as opções de monitorização e as opções de controlo de acesso.

Tarefas de rede

As tarefas de rede incluem:

- "Gerenciamento de grupos de alta disponibilidade"
- "Gerenciamento de pontos de extremidade do balanceador de carga"
- "Configurando nomes de domínio de endpoint S3"
- "Gerir políticas de classificação de tráfego"

- "Configurando interfaces VLAN"

Tarefas de segurança

As tarefas de segurança incluem:

- "Gerenciamento de certificados de segurança"
- "Gerenciamento de controles internos de firewall"
- "Configurando servidores de gerenciamento de chaves"
- Configurar as definições de segurança, incluindo "Política TLS e SSH", "opções de segurança de rede e objetos"e "definições de segurança da interface".
- Configurar as definições de a "proxy de storage" ou A. "proxy de administrador"

Tarefas do sistema

As tarefas do sistema incluem:

- Uso "federação de grade" para clonar informações da conta de locatário e replicar dados de objeto entre dois sistemas StorageGRID.
- Opcionalmente, ativando a "Comprimir objetos armazenados" opção.
- "Gerenciando o bloqueio de objetos S3"
- Noções básicas sobre opções de armazenamento, "segmentação de objetos"como e "marcas de água do volume de armazenamento".
- "Gerenciar perfis de codificação de apagamento".

Tarefas de monitorização

As tarefas de monitoramento incluem:

- "Configurando mensagens de auditoria e destinos de log"
- "Utilizar a monitorização SNMP"

Tarefas de controle de acesso

As tarefas de controle de acesso incluem:

- "Gerenciando grupos de administradores"
- "Gerenciamento de usuários administrativos"
- Alterar "frase-passe do aprovisionamento"ou "senhas do console do nó"
- "Usando a federação de identidade"
- "Configurando SSO"

Menu de manutenção

O menu Manutenção permite executar tarefas de manutenção, manutenção do sistema e manutenção da rede.

Tarefas

As tarefas de manutenção incluem:

- "Operações de desativação" para remover locais e nós de grade não utilizados
- "Operações de expansão" para adicionar novos nós de grade e locais
- "Procedimentos de recuperação do nó de grade" para substituir um nó com falha e restaurar dados
- "Mudar o nome dos procedimentos" para alterar os nomes de exibição de sua grade, sites e nós
- "Operações de verificação de existência de objeto" verificar a existência (embora não a correção) de dados de objeto
- Executando um "reinício contínuo" para reiniciar vários nós de grade
- "Operações de restauração de volume"

Sistema

As tarefas de manutenção do sistema que você pode executar incluem:

- "Visualizar informações de licença do StorageGRID" ou "atualizando informações de licença"
- Gerando e baixando o. "Pacote de recuperação"
- Executar atualizações de software do StorageGRID, incluindo atualizações de software, hotfixes e atualizações do software SANtricity os em dispositivos selecionados
  - "Procedimento de atualização"
  - "Procedimento de correção"
  - "Atualize o SANtricity os em controladores de storage SG6000 usando o Gerenciador de Grade"
  - "Atualize o SANtricity os em controladores de storage SG5700 usando o Gerenciador de Grade"

Rede

As tarefas de manutenção de rede que você pode executar incluem:

- "Configurando servidores DNS"
- "Atualizando sub-redes de rede de Grade"
- "Gerenciamento de servidores NTP"

Menu de suporte

O menu suporte fornece opções que ajudam o suporte técnico a analisar e solucionar problemas do seu sistema.

Ferramentas

Na seção Ferramentas do menu suporte, você pode:

- "Configurar o AutoSupport"
- "Execute o diagnóstico" no estado atual da grelha
- "Acesse a árvore de topologia de grade" para exibir informações detalhadas sobre nós de grade, serviços e atributos

- "Colete arquivos de log e dados do sistema"
- "Analise as métricas de suporte"

> As ferramentas disponíveis na opção **Metrics** destinam-se a ser utilizadas pelo suporte técnico. Alguns recursos e itens de menu dentro dessas ferramentas são intencionalmente não funcionais.

Alarmes (legado)

As informações sobre alarmes legados foram removidas desta versão da documentação. Consulte a "Gerenciar alertas e alarmes (documentação do StorageGRID 11,8)".

Outros

Na outra seção do menu suporte, você pode:

- Gerenciar "custo da ligação"
- "Sistema de gerenciamento de rede (NMS)"Ver entradas
- Gerenciar "marcas de água de armazenamento"

Explore o Gestor do Locatário

"Gerente do locatário"A é a interface gráfica baseada em navegador que os usuários locatários acessam para configurar, gerenciar e monitorar suas contas de storage.

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

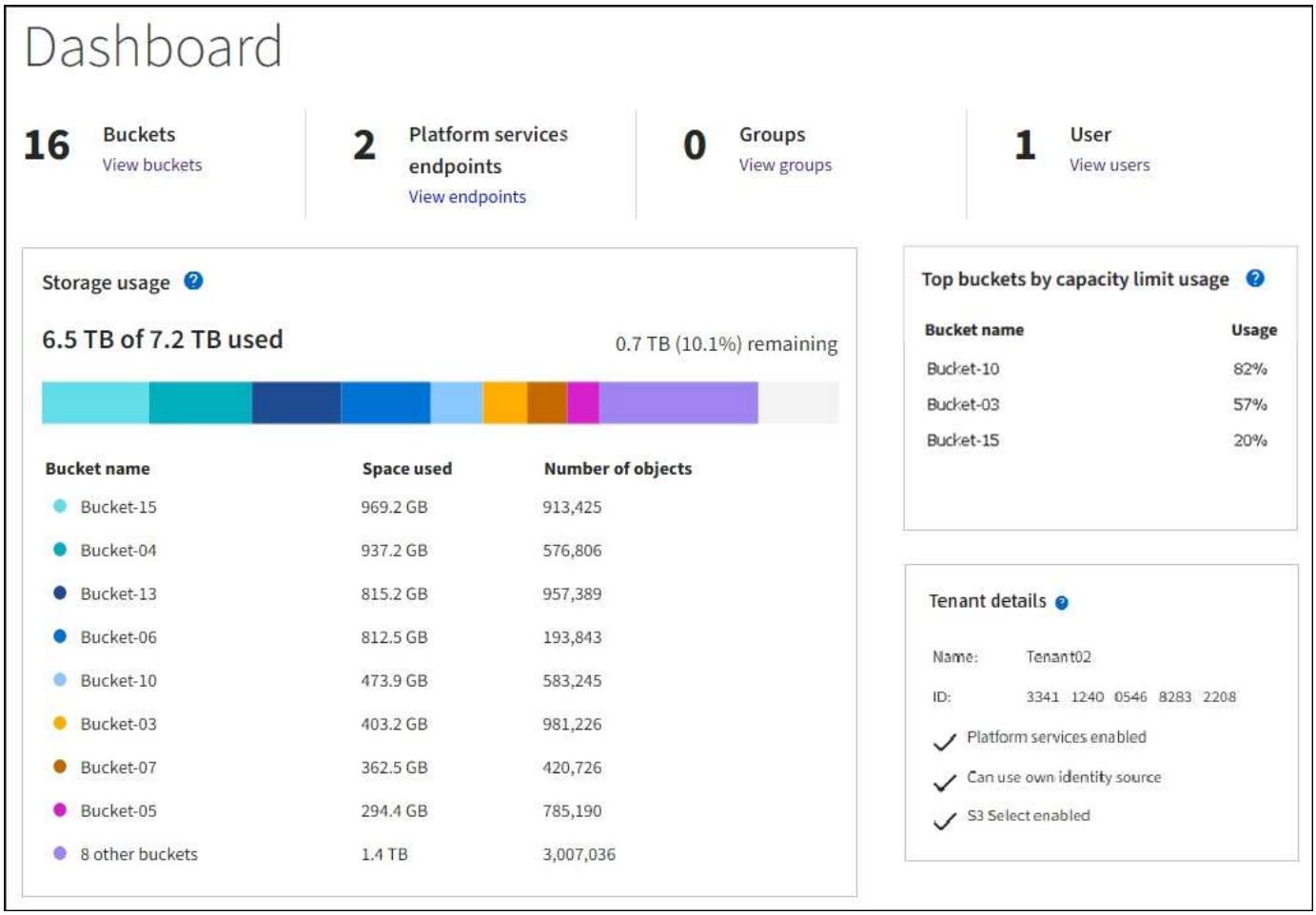
Quando os usuários do locatário entram no Gerenciador do locatário, eles estão se conetando a um nó de administrador.

Painel do Gerenciador do locatário

Depois que um administrador de grade criar uma conta de locatário usando o Gerenciador de Grade ou a API de Gerenciamento de Grade, os usuários do locatário podem fazer login no Gerenciador do locatário.

O painel do Tenant Manager permite que os usuários do locatário monitorem rapidamente o uso do armazenamento. O painel uso do armazenamento contém uma lista dos maiores buckets (S3) ou contentores (Swift) para o locatário. O valor espaço usado é a quantidade total de dados de objeto no intervalo ou recipiente. O gráfico de barras representa os tamanhos relativos desses baldes ou contentores.

O valor mostrado acima do gráfico de barras é uma soma do espaço usado para todos os buckets ou contentores do locatário. Se o número máximo de gigabytes, terabytes ou petabytes disponíveis para o locatário foi especificado quando a conta foi criada, a quantidade de cota usada e restante também será mostrada.



Menu de armazenamento (S3)

O menu armazenamento é fornecido apenas para contas de inquilino do S3. Esse menu permite que os usuários do S3 gerenciem chaves de acesso; criem, gerenciem e excluam buckets; gerenciem endpoints de serviços de plataforma; e visualizem todas as conexões de federação de grade que tenham permissão para usar.

As minhas chaves de acesso

Os usuários do S3 locatário podem gerenciar chaves de acesso da seguinte forma:

- Os usuários que têm a permissão Gerenciar suas próprias credenciais do S3 podem criar ou remover suas próprias chaves de acesso do S3.
- Os usuários que têm a permissão de acesso root podem gerenciar as chaves de acesso para a conta raiz do S3, sua própria conta e todos os outros usuários. As chaves de acesso root também fornecem acesso total aos buckets e objetos do locatário, a menos que explicitamente desabilitados por uma política de bucket.

> O gerenciamento das chaves de acesso para outros usuários ocorre no menu Gerenciamento de acesso.

Baldes

S3 os usuários locatários com as permissões apropriadas podem executar as seguintes tarefas para seus

buckets:

- Crie buckets
- Ativar bloqueio de objeto S3 para um novo bucket (pressupõe que o bloqueio de objeto S3 está ativado para o sistema StorageGRID)
- Atualizar valores de consistência
- Ative e desative as atualizações da última hora de acesso
- Ativar ou suspender o controle de versão de objetos
- Atualização S3 retenção padrão bloqueio Objeto
- Configurar o compartilhamento de recursos entre origens (CORS)
- Exclua todos os objetos em um bucket
- Exclua buckets vazios
- Utilize o "S3 Console" para gerir objetos de balde

Se um administrador de grade tiver habilitado o uso de serviços de plataforma para a conta de locatário, um usuário de locatário S3 com as permissões apropriadas também poderá executar estas tarefas:

- Configure as notificações de eventos do S3, que podem ser enviadas para um serviço de destino compatível com o Amazon Simple Notification Service.
- Configure a replicação do CloudMirror, que permite que o locatário replique automaticamente objetos para um bucket externo do S3.
- Configure a integração de pesquisa, que envia metadados de objetos para um índice de pesquisa de destino sempre que um objeto é criado, excluído ou seus metadados ou tags são atualizados.

Endpoints de serviços de plataforma

Se um administrador de grade tiver habilitado o uso de serviços de plataforma para a conta de locatário, um usuário de locatário S3 com a permissão Gerenciar endpoints poderá configurar um endpoint de destino para cada serviço de plataforma.

Conexões de federação de grade

Se um administrador de grade tiver habilitado o uso de uma conexão de federação de grade para a conta de locatário, um usuário de locatário S3 que tenha permissão de acesso root poderá exibir o nome da conexão, acessar a página de detalhes do bucket para cada bucket que tem replicação entre grades ativada e exibir o erro mais recente a ocorrer quando os dados do bucket estavam sendo replicados para a outra grade na conexão. "Exibir conexões de federação de grade"Consulte .

Menu Gerenciamento de Acesso

O menu Gerenciamento de acesso permite que os locatários do StorageGRID importem grupos de usuários de uma origem de identidade federada e atribuam permissões de gerenciamento. Os locatários também podem gerenciar grupos de locatários locais e usuários, a menos que o logon único (SSO) esteja em vigor para todo o sistema StorageGRID.

Diretrizes de rede

Diretrizes de rede

Use essas diretrizes para conhecer a arquitetura e as topologias de rede do StorageGRID e conhecer os requisitos de configuração e provisionamento de rede.

Sobre estas instruções

Essas diretrizes fornecem informações que você pode usar para criar a infraestrutura de rede do StorageGRID antes de implantar e configurar os nós do StorageGRID. Use essas diretrizes para ajudar a garantir que a comunicação possa ocorrer entre todos os nós da grade e entre a grade e clientes e serviços externos.

Clientes externos e serviços externos precisam se conetar a redes StorageGRID para executar funções como as seguintes:

- Armazenar e recuperar dados de objeto
- Receber notificações por e-mail
- Acesse a interface de gerenciamento do StorageGRID (Gerenciador de grade e Gerenciador de locatário)
- Acessar o compartilhamento de auditoria (opcional)
- Fornecer serviços como:
  - Protocolo de tempo de rede (NTP)
  - Sistema de nomes de domínio (DNS)
  - Servidor de gerenciamento de chaves (KMS)

A rede StorageGRID deve ser configurada adequadamente para lidar com o tráfego dessas funções e muito mais.

Antes de começar

A configuração da rede para um sistema StorageGRID requer um alto nível de experiência com comutação Ethernet, rede TCP/IP, sub-redes, roteamento de rede e firewalls.

Antes de configurar a rede, familiarize-se com a arquitetura StorageGRID conforme descrito em "Saiba mais sobre o StorageGRID".

Depois de determinar quais redes StorageGRID você deseja usar e como essas redes serão configuradas, você poderá instalar e configurar os nós StorageGRID seguindo as instruções apropriadas.

Instale os nós do dispositivo

- "Instale o hardware do dispositivo"

Instalar nós baseados em software

- "Instale o StorageGRID no Red Hat Enterprise Linux"
- "Instale o StorageGRID no Ubuntu ou Debian"
- "Instale o StorageGRID no VMware"

Configurar e administrar o software StorageGRID

- "Administrar o StorageGRID"
- "Notas de lançamento"

Tipos de rede StorageGRID

Os nós de grade em um sistema StorageGRID processam *grid traffic*, *admin traffic* e *client traffic*. Você deve configurar a rede adequadamente para gerenciar esses três tipos de tráfego e fornecer controle e segurança.

Tipos de tráfego

Tipo de trânsito	Descrição	Tipo de rede
Tráfego de grade	O tráfego StorageGRID interno que viaja entre todos os nós na grade. Todos os nós de grade devem ser capazes de se comunicar com todos os outros nós de grade por essa rede.	Rede de rede (necessária)
Tráfego de administração	O tráfego utilizado para a administração e manutenção do sistema.	Admin Network (opcional), Rede VLAN (opcional)
Tráfego do cliente	O tráfego que viaja entre aplicativos clientes externos e a grade, incluindo todas as solicitações de armazenamento de objetos de clientes S3.	Rede do cliente (opcional), Rede VLAN (opcional)

Você pode configurar a rede das seguintes maneiras:

- Apenas rede de grelha
- Redes Grid e Admin
- Rede e redes de clientes
- Redes Grid, Admin e Client

A rede de Grade é obrigatória e pode gerenciar todo o tráfego de grade. As redes Admin e Client podem ser incluídas no momento da instalação ou adicionadas posteriormente para se adaptarem às alterações nos requisitos. Embora a rede de administração e a rede de cliente sejam opcionais, quando você usa essas redes para lidar com o tráfego administrativo e de cliente, a rede de grade pode ser isolada e segura.

As portas internas só são acessíveis através da rede de Grade. As portas externas são acessíveis a partir de todos os tipos de rede. Essa flexibilidade oferece várias opções para projetar uma implantação do StorageGRID e configurar o IP externo e a filtragem de portas em switches e firewalls. "comunicações internas do nó da grade"Consulte e "comunicações externas".

Interfaces de rede

Os nós de StorageGRID são conetados a cada rede usando as seguintes interfaces específicas:

Rede	Nome da interface
Rede de rede (necessária)	eth0
Admin Network (opcional)	eth1

Rede	Nome da interface
Rede cliente (opcional)	eth2

Para obter detalhes sobre o mapeamento de portas virtuais ou físicas para interfaces de rede de nós, consulte as instruções de instalação:

Nós baseados em software

- "Instale o StorageGRID no Red Hat Enterprise Linux"
- "Instale o StorageGRID no Ubuntu ou Debian"
- "Instale o StorageGRID no VMware"

Nós do dispositivo

- "SG6160 dispositivo de armazenamento"
- "SGF6112 dispositivo de armazenamento"
- "SG6000 dispositivo de armazenamento"
- "SG5800 dispositivo de armazenamento"
- "SG5700 dispositivo de armazenamento"
- "Aparelhos de serviços SG110 e SG1100"
- "Aparelhos de serviços SG100 e SG1000"

Informações de rede para cada nó

Você deve configurar o seguinte para cada rede ativa em um nó:

- Endereço IP
- Máscara de sub-rede
- Endereço IP do gateway

Você só pode configurar uma combinação de endereço IP/máscara/gateway para cada uma das três redes em cada nó de grade. Se você não quiser configurar um gateway para uma rede, use o endereço IP como endereço de gateway.

Grupos de alta disponibilidade

Os grupos de alta disponibilidade (HA) fornecem a capacidade de adicionar endereços IP virtuais (VIP) à interface Grid ou Client Network. Para obter mais informações, "Gerenciar grupos de alta disponibilidade"consulte .

Rede de rede

A rede de Grade é necessária. É usado para todo o tráfego interno do StorageGRID. A rede de Grade fornece conetividade entre todos os nós da grade, em todos os sites e sub-redes. Todos os nós na rede de Grade devem ser capazes de se comunicar com todos os outros nós. A rede de Grade pode consistir em várias sub-redes. As redes que contêm serviços de grade críticos, como NTP, também podem ser adicionadas como sub-redes de grade.

O StorageGRID não oferece suporte à conversão de endereços de rede (NAT) entre nós.

A rede de grade pode ser usada para todo o tráfego de administração e todo o tráfego de cliente, mesmo que a rede de administração e a rede de cliente estejam configuradas. O gateway de rede de grade é o gateway padrão do nó, a menos que o nó tenha a rede de cliente configurada.

> Ao configurar a rede de Grade, você deve garantir que a rede esteja protegida de clientes não confiáveis, como aqueles na Internet aberta.

Observe os seguintes requisitos e detalhes para o gateway de rede de grade:

- O gateway de rede de grade deve ser configurado se houver várias sub-redes de grade.
- O gateway Grid Network é o gateway padrão do nó até que a configuração da grade esteja concluída.
- As rotas estáticas são geradas automaticamente para todos os nós para todas as sub-redes configuradas na lista global de sub-redes de rede de Grade.
- Se for adicionada uma rede de cliente, o gateway predefinido muda do gateway de rede de grelha para o gateway de rede de cliente quando a configuração da grelha estiver concluída.

Rede de administração

A rede de administração é opcional. Quando configurado, ele pode ser usado para administração do sistema e tráfego de manutenção. A rede Admin é normalmente uma rede privada e não precisa ser roteável entre nós.

Você pode escolher quais nós de grade devem ter a rede Admin ativada neles.

Quando você usa a rede de administração, o tráfego administrativo e de manutenção não precisa viajar pela rede de grade. Os usos típicos da rede de administração incluem o seguinte:

- Acesso às interfaces de usuário do Grid Manager e do Tenant Manager.
- Acesso a serviços críticos, como servidores NTP, servidores DNS, servidores de gerenciamento de chaves externas (KMS) e servidores LDAP (Lightweight Directory Access Protocol).
- Acesso a logs de auditoria em nós de administração.
- Acesso ao Secure Shell Protocol (SSH) para manutenção e suporte.

A rede Admin nunca é utilizada para o tráfego interno da grelha. Um gateway de rede Admin é fornecido e permite que a rede Admin se comunique com várias sub-redes externas. No entanto, o gateway Admin Network nunca é usado como o gateway padrão do nó.

Observe os seguintes requisitos e detalhes para o gateway de rede de administração:

- O gateway de rede Admin é necessário se as conexões forem feitas fora da sub-rede da rede Admin ou se várias sub-redes da rede Admin estiverem configuradas.
- As rotas estáticas são criadas para cada sub-rede configurada na Lista de sub-rede Admin da rede do nó.

Rede de clientes

A rede do cliente é opcional. Quando configurado, ele é usado para fornecer acesso a serviços de grade para aplicativos clientes, como S3. Se você planeja tornar os dados do StorageGRID acessíveis a um recurso externo (por exemplo, um pool de armazenamento em nuvem ou o serviço de replicação do StorageGRID CloudMirror), o recurso externo também poderá usar a rede do cliente. Os nós de grade podem se comunicar com qualquer sub-rede acessível através do gateway rede cliente.

Você pode escolher quais nós de grade devem ter a rede do cliente ativada neles. Todos os nós não precisam

estar na mesma rede de clientes, e os nós nunca se comunicam uns com os outros pela rede de clientes. A rede do cliente não se torna operacional até que a instalação da grade esteja concluída.

Para maior segurança, você pode especificar que a interface de rede do cliente de um nó não seja confiável para que a rede do cliente seja mais restritiva de quais conexões são permitidas. Se a interface de rede do cliente de um nó não for confiável, a interface aceita conexões de saída, como as usadas pela replicação do CloudMirror, mas aceita somente conexões de entrada em portas que foram explicitamente configuradas como endpoints do balanceador de carga. "Gerenciar controles de firewall"Consulte e "Configurar pontos de extremidade do balanceador de carga".

Quando você usa uma rede de cliente, o tráfego de cliente não precisa viajar pela rede de grade. O tráfego de rede de grade pode ser separado em uma rede segura e não roteável. Os seguintes tipos de nó são frequentemente configurados com uma rede de cliente:

- Nós de gateway, porque esses nós fornecem acesso ao serviço do StorageGRID Load Balancer e ao acesso do cliente S3 à grade.
- Nós de storage, porque esses nós fornecem acesso ao protocolo S3, aos Cloud Storage Pools e ao serviço de replicação do CloudMirror.
- Nós de administração, para garantir que os usuários do locatário possam se conetar ao Gerenciador do locatário sem precisar usar a rede de administração.

Observe o seguinte para o gateway de rede do cliente:

- O gateway de rede do cliente é necessário se a rede do cliente estiver configurada.
- O gateway de rede do cliente torna-se a rota padrão para o nó de grade quando a configuração de grade estiver concluída.

Redes VLAN opcionais

Como necessário, você pode usar opcionalmente redes LAN virtual (VLAN) para tráfego de clientes e para alguns tipos de tráfego de administração. O tráfego de grade, no entanto, não pode usar uma interface VLAN. O tráfego StorageGRID interno entre nós deve sempre usar a rede de Grade no eth0.

Para suportar o uso de VLANs, você deve configurar uma ou mais interfaces em um nó como interfaces de tronco no switch. Você pode configurar a interface de rede de grade (eth0) ou a interface de rede de cliente (eth2) para ser um tronco, ou você pode adicionar interfaces de tronco ao nó.

Se eth0 estiver configurado como um tronco, o tráfego da rede de Grade flui sobre a interface nativa do tronco, conforme configurado no switch. Da mesma forma, se eth2 estiver configurado como um tronco e a rede do cliente também estiver configurada no mesmo nó, a rede do cliente usará a VLAN nativa da porta do tronco conforme configurada no switch.

Somente o tráfego de administração de entrada, como usado para o tráfego SSH, Grid Manager ou Tenant Manager, é suportado em redes VLAN. O tráfego de saída, como usado para NTP, DNS, LDAP, KMS e pools de armazenamento em nuvem, não é suportado em redes VLAN.

> As interfaces VLAN podem ser adicionadas apenas aos nós de administração e aos nós de gateway. Não é possível usar uma interface VLAN para acesso de cliente ou administrador a nós de storage.

"Configurar interfaces VLAN"Consulte para obter instruções e diretrizes.

As interfaces VLAN são usadas apenas em grupos de HA e são atribuídos endereços VIP no nó ativo.

"Gerenciar grupos de alta disponibilidade"Consulte para obter instruções e diretrizes.

Exemplos de topologia de rede

Topologia de rede de grade

A topologia de rede mais simples é criada configurando apenas a rede de Grade.

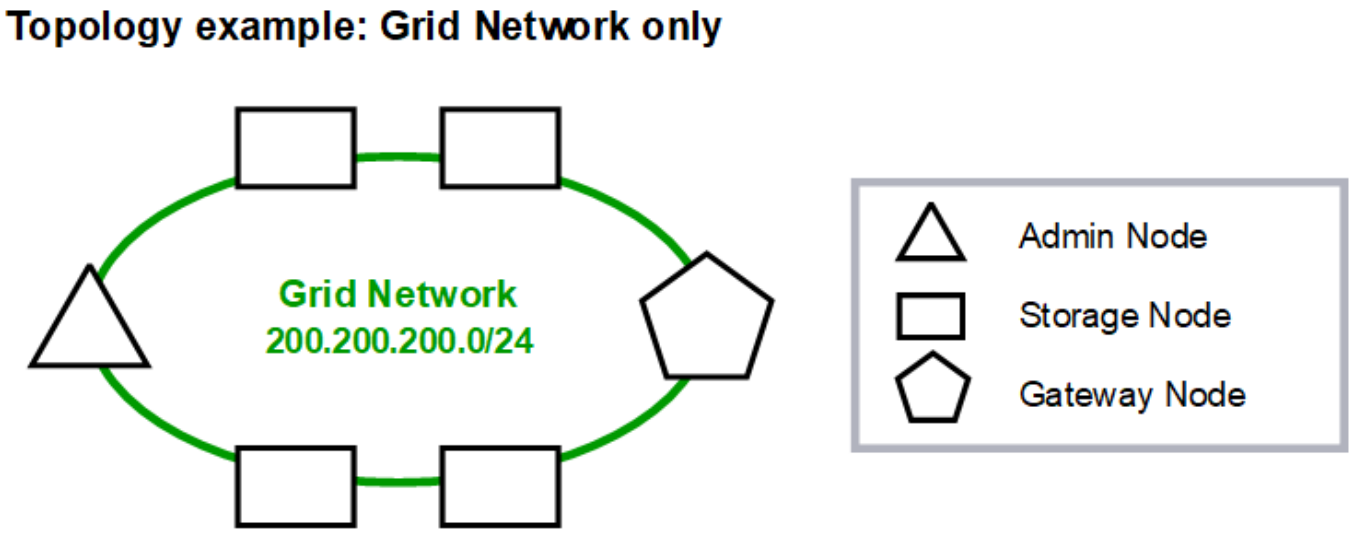
Ao configurar a rede de Grade, você estabelece o endereço IP do host, a máscara de sub-rede e o endereço IP do gateway para a interface eth0 para cada nó de grade.

Durante a configuração, você deve adicionar todas as sub-redes de rede de Grade à Lista de sub-redes de rede de Grade (GNSL). Essa lista inclui todas as sub-redes para todos os sites e também pode incluir sub-redes externas que fornecem acesso a serviços críticos, como NTP, DNS ou LDAP.

Na instalação, a interface rede de Grade aplica rotas estáticas para todas as sub-redes no GNSL e define a rota padrão do nó para o gateway rede de Grade se uma estiver configurada. O GNSL não é necessário se não houver rede de cliente e o gateway de rede de grade for a rota padrão do nó. As rotas de host para todos os outros nós na grade também são geradas.

Neste exemplo, todo o tráfego compartilha a mesma rede, incluindo o tráfego relacionado a solicitações de clientes S3 e funções administrativas e de manutenção.

Essa topologia é apropriada para implantações de um único local que não estão disponíveis externamente, implantações de prova de conceito ou teste ou quando um balanceador de carga de terceiros atua como limite de acesso do cliente. Quando possível, a rede de Grade deve ser usada exclusivamente para tráfego interno. Tanto a rede Admin quanto a rede Client têm restrições adicionais de firewall que bloqueiam o tráfego externo para serviços internos. O uso da rede de Grade para tráfego de cliente externo é suportado, mas esse uso oferece menos camadas de proteção.



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24	→	eth0	Link	Interface IP/mask

Topologia de rede de administração

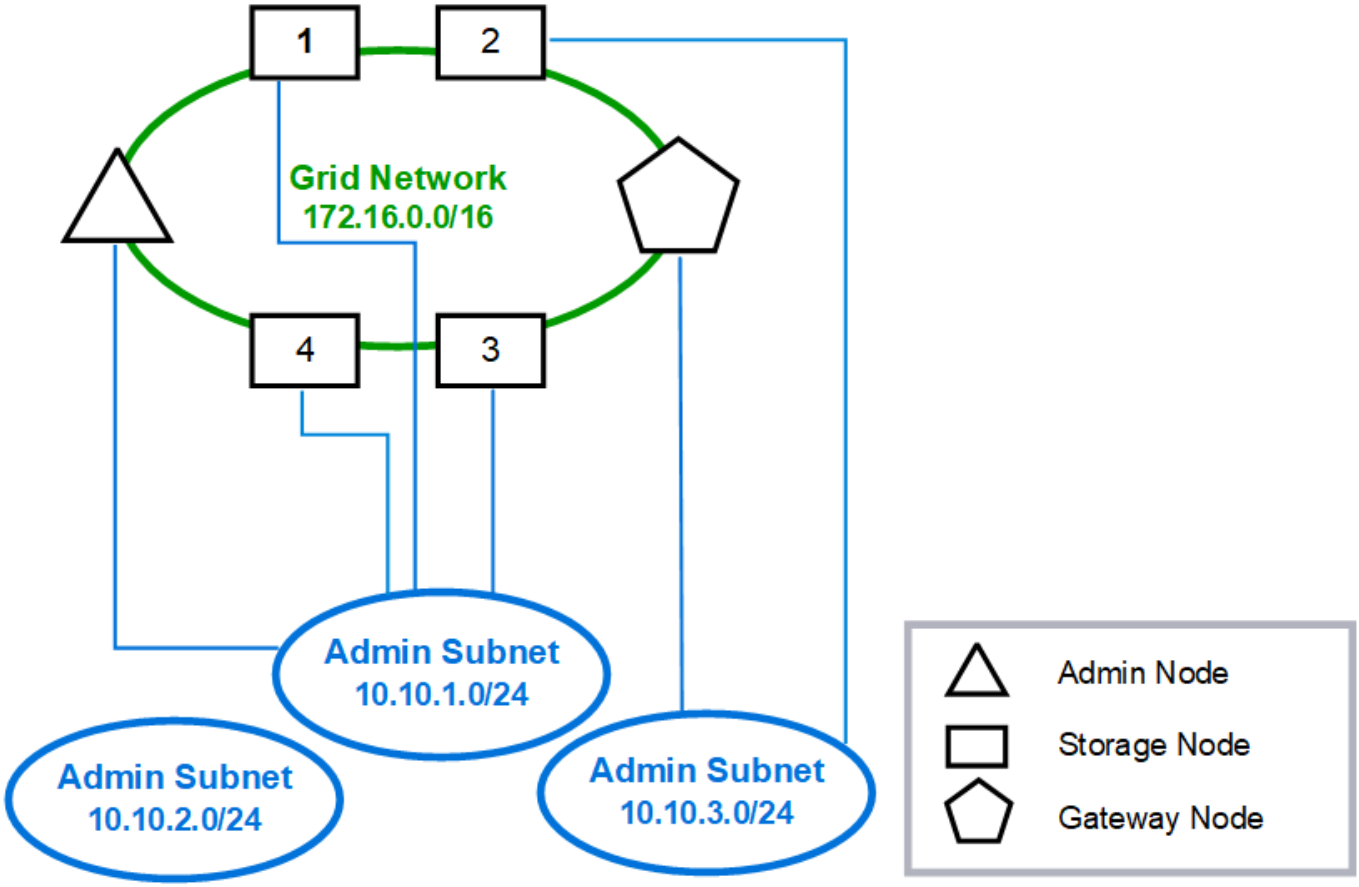
Ter uma rede de administração é opcional. Uma maneira de usar uma rede Admin e uma rede de Grade é configurar uma rede de Grade roteável e uma rede Admin limitada para cada nó.

Ao configurar a rede Admin, você estabelece o endereço IP do host, a máscara de sub-rede e o endereço IP do gateway para a interface eth1 para cada nó de grade.

A rede Admin pode ser exclusiva para cada nó e pode consistir em várias sub-redes. Cada nó pode ser configurado com uma Lista de sub-rede externa Admin (AESL). O AESL lista as sub-redes acessíveis pela rede Admin para cada nó. O AESL também deve incluir as sub-redes de quaisquer serviços que a grade acessará pela rede Admin, como NTP, DNS, KMS e LDAP. As rotas estáticas são aplicadas para cada sub-rede no AESL.

Neste exemplo, a rede de Grade é usada para tráfego relacionado a solicitações de clientes S3 e gerenciamento de objetos. Enquanto a rede de administração é usada para funções administrativas.

Topology example: Grid and Admin Networks



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**IP/mask**	**Gateway**	**IP/mask**	**Gateway**
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

Topologia de rede do cliente

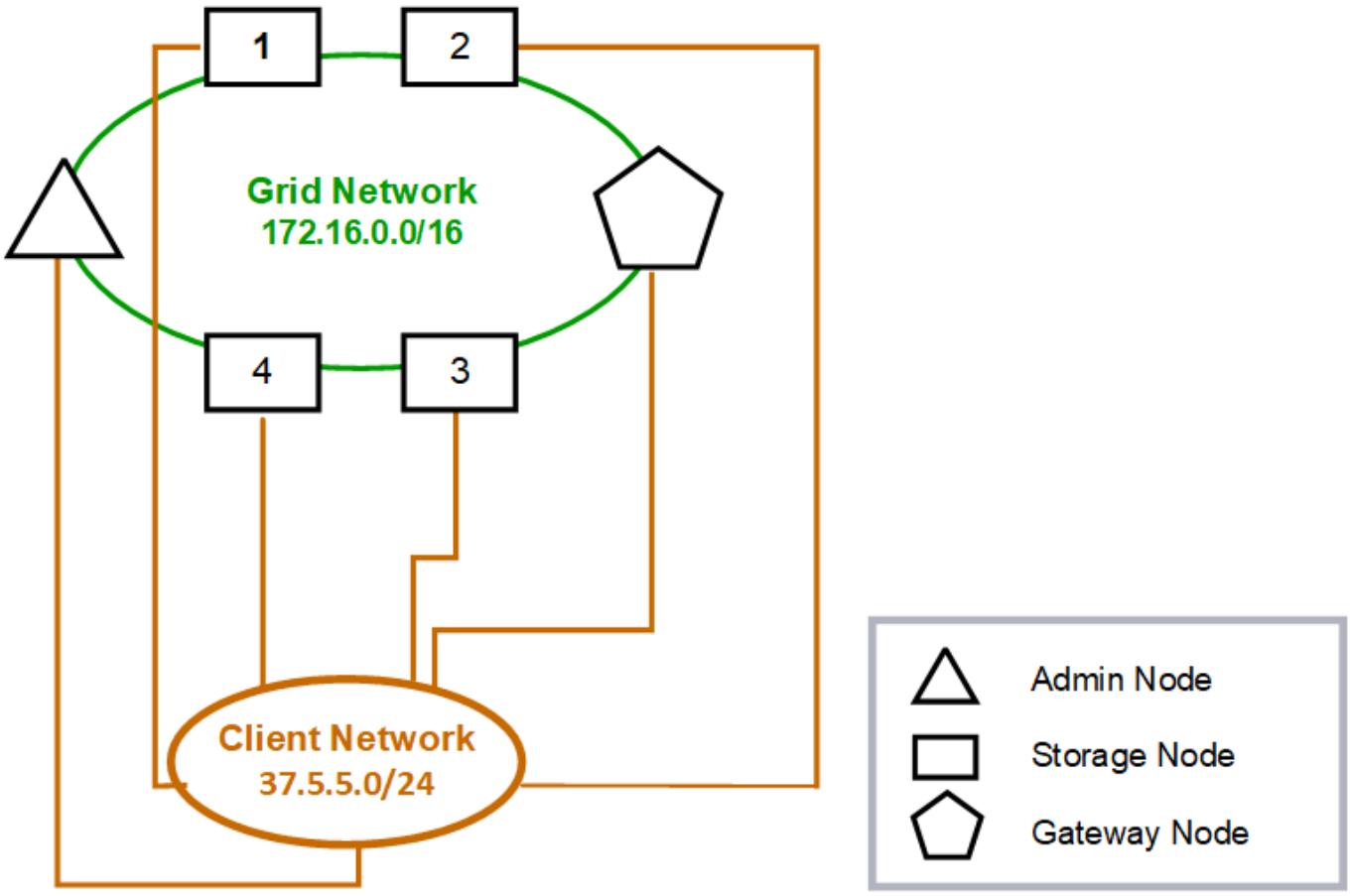
Ter uma rede de clientes é opcional. O uso de uma rede de cliente permite que o tráfego de rede do cliente (por exemplo, S3) seja separado do tráfego interno da grade, o que permite que a rede de grade seja mais segura. O tráfego administrativo pode ser Tratado pelo Cliente ou rede de Grade quando a rede Admin não estiver configurada.

Ao configurar a rede do cliente, você estabelece o endereço IP do host, a máscara de sub-rede e o endereço IP do gateway para a interface eth2 para o nó configurado. A rede Cliente de cada nó pode ser independente da rede Cliente em qualquer outro nó.

Se você configurar uma rede de cliente para um nó durante a instalação, o gateway padrão do nó mudará do gateway de rede de grade para o gateway de rede de cliente quando a instalação estiver concluída. Se uma rede de cliente for adicionada mais tarde, o gateway padrão do nó será alternado da mesma forma.

Neste exemplo, a rede de clientes é usada para solicitações de clientes S3 e para funções administrativas, enquanto a rede de Grade é dedicada a operações internas de gerenciamento de objetos.

Topology example: Grid and Client Networks



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→	eth0	Link	Interface IP/mask
	37.5.5.0/24	→	eth2	Link	Interface IP/mask

Informações relacionadas

"Alterar a configuração da rede do nó"

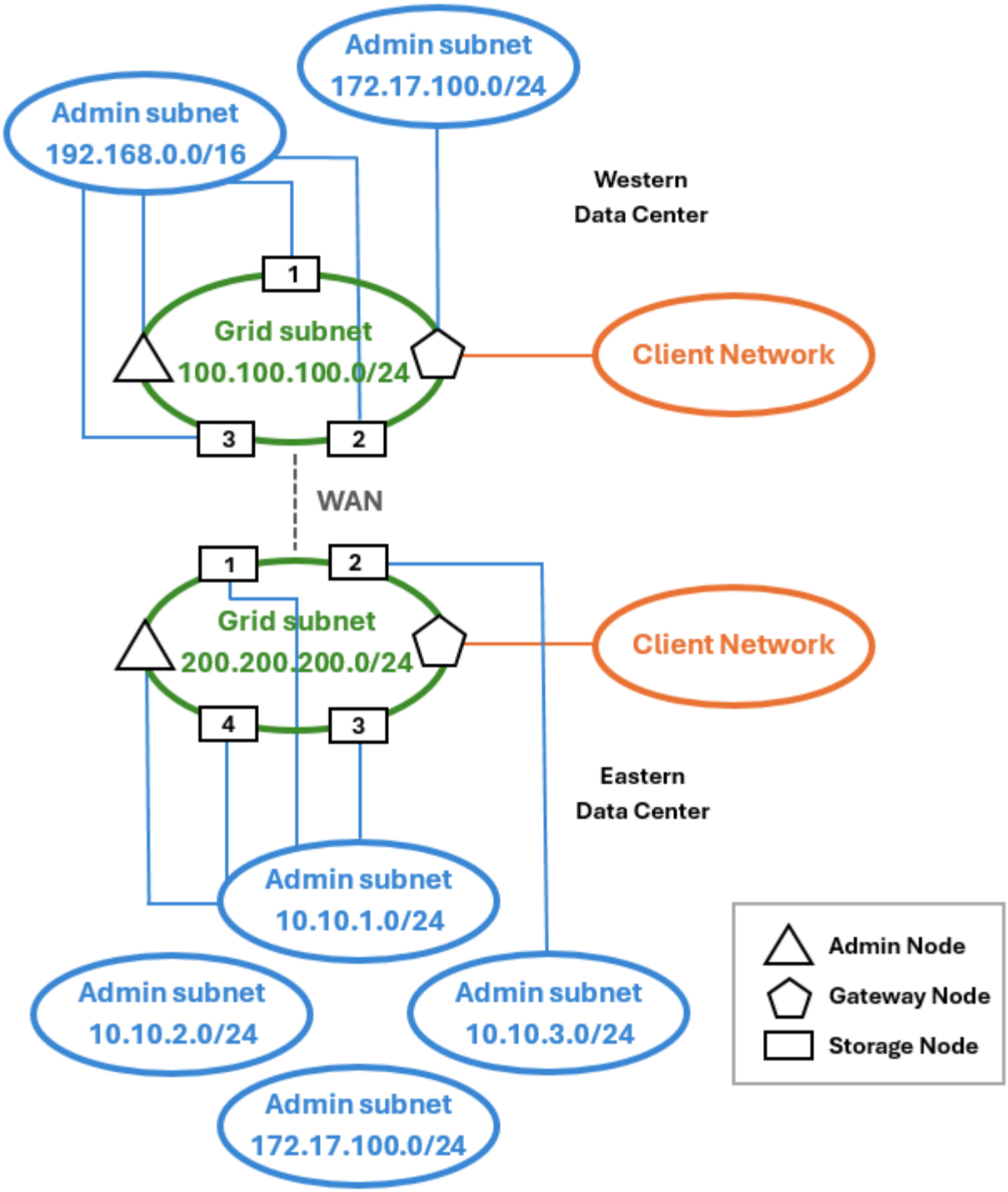
Topologia para todas as três redes

Você pode configurar todas as três redes em uma topologia de rede que consiste em uma rede de grade privada, redes de administração específicas de sites limitados e redes de clientes abertas. O uso de endpoints do balanceador de carga e redes de clientes não confiáveis pode fornecer segurança adicional, se necessário.

Neste exemplo:

- A rede de Grade é usada para o tráfego de rede relacionado a operações internas de gerenciamento de objetos.
- A rede de administração é utilizada para o tráfego relacionado com funções administrativas.
- A rede do cliente é usada para tráfego relacionado a solicitações do cliente S3.

Exemplo de topologia: Redes Grid, Admin e Client



Requisitos de rede

Você deve verificar se a infraestrutura e a configuração de rede atuais podem suportar o design de rede StorageGRID planejado.

Requisitos gerais de rede

Todas as implantações do StorageGRID devem ser capazes de suportar as seguintes conexões.

Essas conexões podem ocorrer através das redes Grid, Admin ou Client, ou as combinações dessas redes, conforme ilustrado nos exemplos de topologia de rede.

- * Conexões de gerenciamento*: Conexões de entrada de um administrador para o nó, geralmente através de SSH. Acesso do navegador da Web ao Gerenciador de Grade, ao Gerenciador do Locatário e ao Instalador de dispositivos StorageGRID.
- * Conexões de servidor NTP*: Conexão UDP de saída que recebe uma resposta UDP de entrada.

  Pelo menos um servidor NTP deve estar acessível pelo nó de administração principal.
- * Conexões de servidor DNS*: Conexão UDP de saída que recebe uma resposta UDP de entrada.
- * Conexões de servidor LDAP/ative Directory*: Conexão TCP de saída do serviço identidade nos nós de armazenamento.
- **AutoSupport**: Conexão TCP de saída dos nós de administração para um `support.netapp.com` proxy configurado pelo cliente ou para um proxy configurado pelo cliente.
- **Servidor de gerenciamento de chaves externo**: Conexão TCP de saída de cada nó de dispositivo com criptografia de nó ativada.
- Conexões TCP de entrada de clientes S3.
- Solicitações de saída de serviços da plataforma StorageGRID, como a replicação do CloudMirror ou de pools de storage de nuvem.

Se o StorageGRID não conseguir contactar qualquer um dos servidores NTP ou DNS aprovisionados utilizando as regras de encaminhamento predefinidas, tentará automaticamente contactar todas as redes (grelha, administrador e cliente), desde que os endereços IP dos servidores DNS e NTP sejam especificados. Se os servidores NTP ou DNS puderem ser alcançados em qualquer rede, o StorageGRID criará automaticamente regras de roteamento adicionais para garantir que a rede seja usada para todas as tentativas futuras de se conetar a ela.

Embora você possa usar essas rotas de host descobertas automaticamente, em geral, você deve configurar manualmente as rotas DNS e NTP para garantir a conetividade no caso de falha de descoberta automática.

Se você não estiver pronto para configurar as redes Admin e Client opcionais durante a implantação, você poderá configurar essas redes quando aprovar nós de grade durante as etapas de configuração. Além disso, pode configurar estas redes após a instalação, utilizando a ferramenta alterar IP ("Configurar endereços IP"consulte).

Apenas as conexões de cliente S3 e SSH, Grid Manager e Tenant Manager administrativas são suportadas por interfaces VLAN. As conexões de saída, como servidores NTP, DNS, LDAP, AutoSupport e KMS, devem passar diretamente pelas interfaces de rede Cliente, Administrador ou Grade. Se a interface for configurada como um tronco para suportar interfaces VLAN, esse tráfego fluirá sobre a VLAN nativa da interface, conforme configurado no switch.

Redes de Área ampla (WANs) para vários sites

Ao configurar um sistema StorageGRID com vários locais, a conexão WAN entre locais deve ter uma largura de banda mínima de 25 Mbit/segundo em cada direção antes de contabilizar o tráfego do cliente. A replicação de dados ou codificação de apagamento entre sites, nó ou expansão de site, recuperação de nós e outras operações ou configurações exigirão largura de banda adicional.

Os requisitos mínimos reais de largura de banda WAN dependem da atividade do cliente e do esquema de proteção ILM. Para obter assistência para estimar os requisitos mínimos de largura de banda da WAN, entre

em Contato com o consultor de Serviços profissionais da NetApp.

Conexões para nós de administração e nós de gateway

Os nós de administração devem sempre ser protegidos de clientes não confiáveis, como aqueles na Internet aberta. Você deve garantir que nenhum cliente não confiável possa acessar qualquer nó Admin na rede de Grade, na rede Admin ou na rede Cliente.

Os nós de administração e os nós de gateway que você pretende adicionar aos grupos de alta disponibilidade devem ser configurados com um endereço IP estático. Para obter mais informações, "Gerenciar grupos de alta disponibilidade"consulte .

Usando a tradução de endereços de rede (NAT)

Não use a tradução de endereço de rede (NAT) na rede de Grade entre nós de grade ou entre sites 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. No entanto, conforme necessário, você pode usar NAT entre clientes externos e nós de grade, como fornecer um endereço IP público para um nó de gateway. O uso de NAT para fazer a ponte de um segmento de rede pública é suportado apenas quando você emprega 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.

Requisitos específicos da rede

Siga os requisitos para cada tipo de rede StorageGRID.

Gateways de rede e roteadores

- Se definido, o gateway para uma determinada rede deve estar dentro da sub-rede da rede específica.
- Se você configurar uma interface usando endereçamento estático, você deve especificar um endereço de gateway diferente de 0,0.0,0.
- Se você não tiver um gateway, a prática recomendada é definir o endereço de gateway para ser o endereço IP da interface de rede.

Sub-redes

> Cada rede deve estar conetada à sua própria sub-rede que não se sobreponha a nenhuma outra rede no nó.

As seguintes restrições são impostas pelo Gerenciador de Grade durante a implantação. Eles são fornecidos aqui para ajudar no Planejamento de rede pré-implantação.

- A máscara de sub-rede para qualquer endereço IP de rede não pode ser 255.255.255.254 ou 255.255.255.255 (/31 ou /32 em notação CIDR).
- A sub-rede definida por um endereço IP de interface de rede e uma máscara de sub-rede (CIDR) não pode sobrepor a sub-rede de qualquer outra interface configurada no mesmo nó.
- A sub-rede da rede de Grade para cada nó deve ser incluída no GNSL.
- A sub-rede Admin Network não pode sobrepor a sub-rede Grid Network, a sub-rede Client Network ou qualquer sub-rede no GNSL.
- As sub-redes no AESL não podem se sobrepor com nenhuma sub-rede no GNSL.

- A sub-rede da rede do cliente não pode sobrepor a sub-rede da rede da grade, a sub-rede da rede do administrador, qualquer sub-rede no GNSL ou qualquer sub-rede no AESL.

Rede de rede

- No momento da implantação, cada nó de grade deve ser conetado à rede de Grade e deve ser capaz de se comunicar com o nó Admin principal usando a configuração de rede especificada ao implantar o nó.
- Durante as operações normais da grade, cada nó da grade deve ser capaz de se comunicar com todos os outros nós da grade pela rede da grade.

> A rede de Grade deve ser roteável diretamente entre cada nó. A conversão de endereços de rede (NAT) entre nós não é suportada.

- Se a rede de Grade consistir em várias sub-redes, adicione-as à Lista de sub-redes de rede de Grade (GNSL). As rotas estáticas são criadas em todos os nós para cada sub-rede no GNSL.
- Se a interface de rede de Grade estiver configurada como um tronco para suportar interfaces VLAN, a VLAN nativa do tronco deve ser a VLAN usada para o tráfego de rede de Grade. Todos os nós de grade devem estar acessíveis através da VLAN nativa do tronco.

Rede de administração

A rede de administração é opcional. Se você planeja configurar uma rede de administração, siga estes requisitos e diretrizes.

Os usos típicos da rede de administração incluem conexões de gerenciamento, AutoSupport, KMS e conexões com servidores críticos, como NTP, DNS e LDAP, se essas conexões não forem fornecidas pela rede de grade ou rede de cliente.

> A rede Admin e AESL podem ser exclusivas para cada nó, desde que os serviços de rede e clientes desejados sejam acessíveis.

> Você deve definir pelo menos uma sub-rede na rede Admin para habilitar conexões de entrada de sub-redes externas. As rotas estáticas são geradas automaticamente em cada nó para cada sub-rede no AESL.

Rede de clientes

A rede do cliente é opcional. Se você planeja configurar uma rede de cliente, observe as seguintes considerações.

- A rede de clientes foi projetada para suportar o tráfego de clientes S3. Se configurado, o gateway de rede do cliente se torna o gateway padrão do nó.
- Se você usar uma rede cliente, você pode ajudar a proteger o StorageGRID contra ataques hostis aceitando tráfego de cliente de entrada apenas em pontos de extremidade do balanceador de carga configurados explicitamente. "Configurar pontos de extremidade do balanceador de carga"Consulte .
- Se a interface de rede do cliente estiver configurada como um tronco para suportar interfaces VLAN, considere se a configuração da interface de rede do cliente (eth2) é necessária. Se configurado, o tráfego de rede do cliente fluirá sobre a VLAN nativa do tronco, conforme configurado no switch.

Informações relacionadas

"Alterar a configuração da rede do nó"

Considerações de rede específicas da implantação

Implantações Linux

Para eficiência, confiabilidade e segurança, o sistema StorageGRID é executado no Linux como uma coleção de motores de contentor. A configuração de rede relacionada ao motor do contentor não é necessária num sistema StorageGRID.

Use um dispositivo não-bond, como um par VLAN ou Ethernet virtual (vete), para a interface de rede do contentor. Especifique este dispositivo como a interface de rede no arquivo de configuração do nó.

> Não use dispositivos bond ou bridge diretamente como a interface de rede do contentor. Fazer isso pode impedir a inicialização do nó por causa de um problema de kernel com o uso de macvlan com dispositivos de ligação e ponte no namespace do contentor.

Consulte as instruções de instalação para "Red Hat Enterprise Linux" ou "Ubuntu ou Debian" implantações.

Configuração de rede de host para implantações do mecanismo de contêiner

Antes de iniciar a implantação do StorageGRID em uma plataforma de mecanismo de contentor, determine quais redes (Grade, Administrador, Cliente) cada nó usará. Você deve garantir que a interface de rede de cada nó esteja configurada na interface de host física ou virtual correta e que cada rede tenha largura de banda suficiente.

Hosts físicos

Se você estiver usando hosts físicos para oferecer suporte a nós de grade:

- Certifique-se de que todos os hosts usem a mesma interface de host para cada interface de nó. Essa estratégia simplifica a configuração de host e permite a migração futura de nós.
- Obtenha um endereço IP para o próprio host físico.

> Uma interface física no host pode ser usada pelo próprio host e por um ou mais nós executados no host. Todos os endereços IP atribuídos ao host ou nós que usam essa interface devem ser exclusivos. O host e o nó não podem compartilhar endereços IP.

- Abra as portas necessárias para o host.
- Se você pretende usar interfaces de VLAN no StorageGRID, o host deve ter uma ou mais interfaces de tronco que forneçam acesso às VLANs desejadas. Essas interfaces podem ser passadas para o contentor de nós como eth0, eth2 ou como interfaces adicionais. Para adicionar interfaces de tronco ou acesso, consulte o seguinte:
  - **RHEL (antes de instalar o nó)**: "Criar arquivos de configuração de nó"
  - * Ubuntu ou Debian (antes de instalar o nó)*: "Criar arquivos de configuração de nó"
  - **RHEL, Ubuntu ou Debian (após instalar o nó)**: "Linux: Adicione interfaces de tronco ou acesso a um nó"

Recomendações mínimas de largura de banda

A tabela a seguir fornece as recomendações mínimas de largura de banda da LAN para cada tipo de nó StorageGRID e cada tipo de rede. Você precisa provisionar cada host físico ou virtual com largura de banda suficiente para atender aos requisitos mínimos de largura de banda agregada para o número total e tipo de

nós de StorageGRID que você planeja executar nesse host.

Tipo de nó	Tipo de rede		
	Grelha	Administrador	Cliente
	• Largura de banda mínima da LAN*	Administrador	10 Gbps
1 Gbps	1 Gbps	Gateway	10 Gbps
1 Gbps	10 Gbps	Armazenamento	10 Gbps
1 Gbps	10 Gbps	Arquivar	10 Gbps

Esta tabela não inclui largura de banda SAN, que é necessária para acesso ao armazenamento compartilhado. Se você estiver usando storage compartilhado acessado por Ethernet (iSCSI ou FCoE), você deverá provisionar interfaces físicas separadas em cada host para fornecer largura de banda suficiente para SAN. Para evitar a introdução de um gargalo, a largura de banda da SAN para um determinado host deve corresponder aproximadamente à largura de banda da rede do nó de storage agregado para todos os nós de storage executados nesse host.

Use a tabela para determinar o número mínimo de interfaces de rede a provisionar em cada host, com base no número e no tipo de nós de StorageGRID que você planeja executar nesse host.

Por exemplo, para executar um nó de administrador, um nó de gateway e um nó de storage em um único host:

- Conetar as redes de Grade e Admin no nó Admin (requer 10 mais de 1 11 Gbps)
- Conetar as redes Grid e Client no Gateway Node (requer 10 e 10, ou 20 Gbps)
- Ligar a rede de grelha no nó de armazenamento (requer 10 Gbps)

Nesse cenário, você deve fornecer um mínimo de 11 41 Gbps e 20 Gbps ou 10 Gbps de largura de banda de rede, que pode ser atendida por duas interfaces de 40 Gbps ou cinco interfaces de 10 Gbps, potencialmente agregadas em troncos e, em seguida, compartilhadas pelas três ou mais VLANs que transportam as sub-redes Grid, Admin e Client locais para o data center físico que contém o host.

Para obter algumas maneiras recomendadas de configurar recursos físicos e de rede nos hosts do cluster StorageGRID para se preparar para a implantação do StorageGRID, consulte o seguinte:

- "Configurar a rede host (Red Hat Enterprise Linux)"
- "Configurar a rede host (Ubuntu ou Debian)"

Rede e portas para serviços de plataforma e Cloud Storage Pools

Se você planeja usar os serviços da plataforma StorageGRID ou os pools de armazenamento em nuvem, configure redes de grade e firewalls para garantir que os pontos de extremidade de destino possam ser alcançados.

Rede para serviços de plataforma

Conforme descrito no "Gerenciar serviços de plataforma para locatários" e "Gerenciar serviços de plataforma"no , os serviços de plataforma incluem serviços externos que fornecem integração de pesquisa, notificação de eventos e replicação do CloudMirror.

Os serviços de plataforma exigem acesso de nós de storage que hospedam o serviço StorageGRID ADC aos pontos de extremidade de serviço externos. Exemplos para fornecer acesso incluem:

- Nos nós de armazenamento com serviços ADC, configure redes de administração exclusivas com entradas AESL que roteam para os endpoints de destino.
- Confie na rota padrão fornecida por uma rede de clientes. Se utilizar a rota predefinida, pode utilizar o "Recurso rede cliente não confiável" para restringir as ligações de entrada.

Rede para pools de armazenamento em nuvem

Os Cloud Storage Pools também exigem acesso dos nós de storage aos pontos de extremidade fornecidos pelo serviço externo usado, como o storage Amazon S3 Glacier ou Microsoft Azure Blob. Para obter informações, "O que é um Cloud Storage Pool"consulte .

Portas para serviços de plataforma e Cloud Storage Pools

Por padrão, os serviços de plataforma e as comunicações do Cloud Storage Pool usam as seguintes portas:

- **80**: Para URIs de endpoint que começam com `http`
- **443**: Para URIs de endpoint que começam com `https`

Uma porta diferente pode ser especificada quando o endpoint é criado ou editado. "Referência da porta de rede"Consulte .

Se você usar um servidor proxy não transparente, também deverá "configure as configurações de proxy de armazenamento"permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet.

VLANs e serviços de plataforma e pools de armazenamento em nuvem

Não é possível usar redes VLAN para serviços de plataforma ou pools de armazenamento em nuvem. Os endpoints de destino devem estar acessíveis através da rede, administrador ou rede de clientes.

Nós do dispositivo

Você pode configurar as portas de rede nos dispositivos StorageGRID para usar os modos de ligação de porta que atendem aos seus requisitos de taxa de transferência, redundância e failover.

As portas 10/25-GbE nos dispositivos StorageGRID podem ser configuradas no modo de ligação fixa ou agregada para conexões à rede de Grade e à rede do cliente.

As portas de rede de administração de 1 GbE podem ser configuradas no modo Independent (independente) ou ative-Backup (ative-Backup) para conexões à rede de administração.

Consulte as informações sobre os modos de ligação de porta para o seu aparelho:

- "Modos de ligação de porta (SG6160)"
- "Modos de ligação de porta (SGF6112)"
- "Modos de ligação de porta (controlador SG6000-CN)"
- "Modos de ligação de porta (controlador SG5800)"
- "Modos de ligação de porta (controlador E5700SG)"
- "Modos de ligação de porta (SG110 e SG1100)"
- "Modos de ligação de porta (SG100 e SG1000)"

Instalação e provisionamento de rede

Você deve entender como a rede de Grade e as redes Admin e Client opcionais são usadas durante a implantação do nó e configuração da grade.

Implantação inicial de um nó

Ao implantar um nó pela primeira vez, você deve anexar o nó à rede de Grade e garantir que ele tenha acesso ao nó de administração principal. Se a rede de grade estiver isolada, você poderá configurar a rede de administração no nó de administração principal para acesso de configuração e instalação fora da rede de grade.

Uma rede de Grade com um gateway configurado torna-se o gateway padrão para um nó durante a implantação. O gateway padrão permite que os nós de grade em sub-redes separadas se comuniquem com o nó de administração principal antes que a grade tenha sido configurada.

Se necessário, sub-redes que contenham servidores NTP ou que necessitem de acesso ao Grid Manager ou API também podem ser configuradas como sub-redes de grade.

Registro automático de nós com nó de administração principal

Depois que os nós são implantados, eles se Registram no nó de administração principal usando a rede de grade. Em seguida, você pode usar o Gerenciador de Grade, o `configure-storagegrid.py` script Python ou a API de Instalação para configurar a grade e aprovar os nós registrados. Durante a configuração de grade, você pode configurar várias sub-redes de grade. As rotas estáticas para essas sub-redes através do gateway Grid Network serão criadas em cada nó quando você concluir a configuração da grade.

Desativando a rede Admin ou a rede do cliente

Se pretender desativar a rede de administração ou a rede de cliente, pode remover a configuração deles durante o processo de aprovação do nó ou pode utilizar a ferramenta alterar IP após a conclusão da instalação (consulte "Configurar endereços IP").

Diretrizes de pós-instalação

Depois de concluir a implantação e a configuração do nó de grade, siga estas diretrizes para endereçamento DHCP e alterações na configuração da rede.

- Se o DHCP foi usado para atribuir endereços IP, configure uma reserva DHCP para cada endereço IP nas redes que estão sendo usadas.

  Só pode configurar o DHCP durante a fase de implementação. Não é possível configurar o DHCP durante

a configuração.

> Os nós reiniciam quando a configuração da rede de Grade é alterada pelo DHCP, o que pode causar interrupções se uma alteração de DHCP afetar vários nós ao mesmo tempo.

- Você deve usar os procedimentos alterar IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. "Configurar endereços IP"Consulte .
- Se você fizer alterações na configuração de rede, incluindo alterações de roteamento e gateway, a conetividade do cliente para o nó de administração principal e outros nós de grade pode ser perdida. Dependendo das alterações de rede aplicadas, talvez seja necessário restabelecer essas conexões.

Referência da porta de rede

Comunicações internas do nó da grade

O firewall interno do StorageGRID permite conexões de entrada a portas específicas na rede de Grade. As conexões também são aceitas em portas definidas pelos pontos de extremidade do balanceador de carga.

> A NetApp recomenda que você ative o tráfego ICMP (Protocolo de mensagens de Controle de Internet) entre nós de grade. Permitir tráfego ICMP pode melhorar o desempenho do failover quando um nó de grade não pode ser alcançado.

Além do ICMP e das portas listadas na tabela, o StorageGRID usa o protocolo de redundância de roteador virtual (VRRP). VRRP é um protocolo de internet que usa o número de protocolo IP 112. O StorageGRID utiliza VRRP apenas no modo unicast. O VRRP é necessário somente se "grupos de alta disponibilidade" estiver configurado.

Diretrizes para nós baseados em Linux

Se as políticas de rede empresarial restringirem o acesso a qualquer uma dessas portas, você poderá remapear as portas no momento da implantação usando um parâmetro de configuração de implantação. Para obter mais informações sobre o mapeamento de portas e os parâmetros de configuração de implantação, consulte:

- "Instale o StorageGRID no Red Hat Enterprise Linux"
- "Instale o StorageGRID no Ubuntu ou Debian"

Diretrizes para nós baseados em VMware

Configure as portas a seguir somente se você precisar definir restrições de firewall externas à rede VMware.

Se as políticas de rede empresarial restringirem o acesso a qualquer uma dessas portas, você poderá remapear as portas quando implantar nós usando o VMware vSphere Web Client ou usando uma configuração de arquivo de configuração ao automatizar a implantação do nó de grade. Para obter mais informações sobre o mapeamento de portas e os parâmetros de configuração de implantação, "Instale o StorageGRID no VMware"consulte .

Diretrizes para nós de dispositivo

Se as políticas de rede empresarial restringirem o acesso a qualquer uma dessas portas, você poderá remapear as portas usando o Instalador de dispositivos StorageGRID. "Opcional: Remapear as portas de rede

para o dispositivo"Consulte .

Portas internas do StorageGRID

Porta	TCP ou UDP	De	Para	Detalhes
22	TCP	Nó de administração principal	Todos os nós	Para procedimentos de manutenção, o nó Admin principal deve ser capaz de se comunicar com todos os outros nós usando SSH na porta 22. Permitir tráfego SSH de outros nós é opcional.
80	TCP	Aparelhos	Nó de administração principal	Usado pelos dispositivos StorageGRID para se comunicar com o nó de administração principal para iniciar a instalação.
123	UDP	Todos os nós	Todos os nós	Serviço de protocolo de tempo de rede. Cada nó sincroniza seu tempo com cada outro nó usando NTP.
443	TCP	Todos os nós	Nó de administração principal	Utilizado para comunicar o estado ao nó de administração principal durante a instalação e outros procedimentos de manutenção.
1055	TCP	Todos os nós	Nó de administração principal	Tráfego interno para instalação, expansão, recuperação e outros procedimentos de manutenção.
1139	TCP	Nós de storage	Nós de storage	Tráfego interno entre nós de storage.
1501	TCP	Todos os nós	Nós de storage com ADC	Geração de relatórios, auditoria e configuração de tráfego interno.
1502	TCP	Todos os nós	Nós de storage	Tráfego interno relacionado a S3 e Swift.
1504	TCP	Todos os nós	Nós de administração	Relatórios de serviço NMS e tráfego interno de configuração.
1505	TCP	Todos os nós	Nós de administração	Tráfego interno do serviço AMS.
1506	TCP	Todos os nós	Todos os nós	Tráfego interno do estado do servidor.

Porta	TCP ou UDP	De	Para	Detalhes
1507	TCP	Todos os nós	Nós de gateway	Tráfego interno do balanceador de carga.
1508	TCP	Todos os nós	Nó de administração principal	Tráfego interno de gerenciamento de configuração.
1511	TCP	Todos os nós	Nós de storage	Tráfego interno de metadados.
7001	TCP	Nós de storage	Nós de storage	Comunicação de cluster entre nós Cassandra TLS.
7443	TCP	Todos os nós	Nó de administração principal	Tráfego interno para instalação, expansão, recuperação, outros procedimentos de manutenção e relatórios de erros.
8011	TCP	Todos os nós	Nó de administração principal	Tráfego interno para instalação, expansão, recuperação e outros procedimentos de manutenção.
8443	TCP	Nó de administração principal	Nós do dispositivo	Tráfego interno relacionado com o procedimento do modo de manutenção.
9042	TCP	Nós de storage	Nós de storage	Porta cliente Cassandra.
9999	TCP	Todos os nós	Todos os nós	Tráfego interno para vários serviços. Inclui procedimentos de manutenção, métricas e atualizações de rede.
10226	TCP	Nós de storage	Nó de administração principal	Usado pelos dispositivos StorageGRID para encaminhar pacotes AutoSupport do Gerenciador de sistemas SANtricity da série e para o nó de administração principal.
10342	TCP	Todos os nós	Nó de administração principal	Tráfego interno para instalação, expansão, recuperação e outros procedimentos de manutenção.
18000	TCP	Nós de administração/storage	Nós de storage com ADC	Tráfego interno do serviço de conta.

Porta	TCP ou UDP	De	Para	Detalhes
18001	TCP	Nós de administração/storage	Nós de storage com ADC	Tráfego interno da Federação de identidades.
18002	TCP	Nós de administração/storage	Nós de storage	Tráfego interno da API relacionado a protocolos de objeto.
18003	TCP	Nós de administração/storage	Nós de storage com ADC	Tráfego interno dos serviços da plataforma.
18017	TCP	Nós de administração/storage	Nós de storage	Tráfego interno do serviço Data Mover para Cloud Storage Pools.
18019	TCP	Nós de storage	Nós de storage	Tráfego interno do serviço de bloco para codificação de apagamento.
18082	TCP	Nós de administração/storage	Nós de storage	Tráfego interno relacionado com S3.
18083	TCP	Todos os nós	Nós de storage	Tráfego interno relacionado com Swift.
18086	TCP	Todos os nós de grade	Todos os nós de storage	Tráfego interno relacionado ao serviço LDR.
18200	TCP	Nós de administração/storage	Nós de storage	Estatísticas adicionais sobre solicitações de clientes.
19000	TCP	Nós de administração/storage	Nós de storage com ADC	Tráfego interno do serviço Keystone.

Informações relacionadas

"Comunicações externas"

Comunicações externas

Os clientes precisam se comunicar com nós de grade para obter e recuperar conteúdo. As portas usadas dependem dos protocolos de storage de objetos escolhidos. Essas portas precisam estar acessíveis ao cliente.

Acesso restrito às portas

Se as políticas de rede empresarial restringirem o acesso a qualquer uma das portas, você poderá fazer um dos seguintes procedimentos:

- "pontos de extremidade do balanceador de carga"Utilize para permitir o acesso em portas definidas pelo utilizador.
- Remapear portas ao implantar nós. No entanto, você não deve remapear os pontos de extremidade do balanceador de carga. Consulte as informações sobre o mapeamento de portas para o nó StorageGRID:
  - "As chaves de remapa de porta para StorageGRID no Red Hat Enterprise Linux"
  - "Port Remap chaves para StorageGRID no Ubuntu ou Debian"
  - "Remapear portas para StorageGRID no VMware"
  - "Opcional: Remapear as portas de rede para o dispositivo"

Portas usadas para comunicações externas

A tabela a seguir mostra as portas usadas para tráfego nos nós.

> Esta lista não inclui portas que possam ser configuradas como "pontos de extremidade do balanceador de carga".

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
22	TCP	SSH	Serviço de laptop	Todos os nós	SSH ou acesso ao console é necessário para procedimentos com etapas do console. Opcionalmente, você pode usar a porta 2022 em vez de 22.
25	TCP	SMTP	Nós de administração	Servidor de e-mail	Usado para alertas e AutoSupport baseados em e-mail. Você pode substituir a configuração de porta padrão de 25 usando a página servidores de e-mail.
53	TCP/UDP	DNS	Todos os nós	Servidores DNS	Usado para DNS.
67	UDP	DHCP	Todos os nós	Serviço DHCP	Usado opcionalmente para suportar a configuração de rede baseada em DHCP. O serviço dhclient não é executado para grades configuradas estaticamente.
68	UDP	DHCP	Serviço DHCP	Todos os nós	Usado opcionalmente para suportar a configuração de rede baseada em DHCP. O serviço dhclient não é executado para grades que usam endereços IP estáticos.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
80	TCP	HTTP	Navegador	Nós de administração	A porta 80 redireciona para a porta 443 para a interface de usuário do nó de administrador.
80	TCP	HTTP	Navegador	Aparelhos	A porta 80 redireciona para a porta 8443 para o instalador do dispositivo StorageGRID.
80	TCP	HTTP	Nós de storage com ADC	AWS	Usado para mensagens de serviços de plataforma enviadas para a AWS ou outros serviços externos que usam HTTP. Os locatários podem substituir a configuração padrão de porta HTTP de 80 ao criar um endpoint.
80	TCP	HTTP	Nós de storage	AWS	As solicitações do Cloud Storage Pools enviadas para destinos da AWS que usam HTTP. Os administradores de grade podem substituir a configuração padrão de porta HTTP de 80 ao configurar um pool de armazenamento em nuvem.
111	TCP/UDP	RPCBind	Cliente NFS	Nós de administração	Usado pela exportação de auditoria baseada em NFS (portmap). **Nota:** esta porta é necessária apenas se a exportação de auditoria baseada em NFS estiver ativada. **Observação:** o suporte para NFS foi obsoleto e será removido em uma versão futura.
123	UDP	NTP	Nós NTP primários	NTP externo	Serviço de protocolo de tempo de rede. Os nós selecionados como fontes NTP primárias também sincronizam os horários do relógio com as fontes de hora NTP externas.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
161	TCP/UDP	SNMP	Cliente SNMP	Todos os nós	Usado para polling SNMP. Todos os nós fornecem informações básicas; os nós de administração também fornecem dados de alerta. O padrão é a porta UDP 161 quando configurada. **Nota:** esta porta só é necessária e só é aberta no firewall do nó se o SNMP estiver configurado. Se você pretende usar SNMP, você pode configurar portas alternativas. **Observação:** para obter informações sobre como usar o SNMP com o StorageGRID, entre em Contato com o representante da conta do NetApp.
162	TCP/UDP	Notificaçõ es SNMP	Todos os nós	Destinos de notificação	Notificações e traps SNMP de saída padrão para a porta UDP 162. **Nota:** esta porta só é necessária se o SNMP estiver ativado e os destinos de notificação estiverem configurados. Se você pretende usar SNMP, você pode configurar portas alternativas. **Observação:** para obter informações sobre como usar o SNMP com o StorageGRID, entre em Contato com o representante da conta do NetApp.
389	TCP/UDP	LDAP	Nós de storage com ADC	Ative Directory/LDAP	Usado para conetar-se a um servidor ative Directory ou LDAP para Federação de identidade.
443	TCP	HTTPS	Navegador	Nós de administração	Usado por navegadores da Web e clientes de API de gerenciamento para acessar o Gerenciador de Grade e o Gerenciador de Tenant. **Nota**: Se você fechar as portas 443 ou 8443 do Gerenciador de Grade, qualquer usuário conetado atualmente em uma porta bloqueada, incluindo você, perderá o acesso ao Gerenciador de Grade, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados. "Configurar controles de firewall"Consulte para configurar endereços IP privilegiados.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
443	TCP	HTTPS	Nós de administração	Ative Directory	Usado por nós de administração que se conetam ao ative Directory se o logon único (SSO) estiver ativado.
443	TCP	HTTPS	Nós de storage com ADC	AWS	Usado para mensagens de serviços de plataforma enviadas para a AWS ou outros serviços externos que usam HTTPS. Os locatários podem substituir a configuração padrão de porta HTTP de 443 ao criar um endpoint.
443	TCP	HTTPS	Nós de storage	AWS	Solicitações do Cloud Storage Pools enviadas para destinos da AWS que usam HTTPS. Os administradores de grade podem substituir a configuração padrão de porta HTTPS de 443 ao configurar um pool de armazenamento em nuvem.
903	TCP	NFS	Cliente NFS	Nós de administração	Usado pela exportação de auditoria baseada em NFS (`rpc.mountd`). **Nota:** esta porta é necessária apenas se a exportação de auditoria baseada em NFS estiver ativada. **Observação:** o suporte para NFS foi obsoleto e será removido em uma versão futura.
2022	TCP	SSH	Serviço de laptop	Todos os nós	SSH ou acesso ao console é necessário para procedimentos com etapas do console. Opcionalmente, você pode usar a porta 22 em vez de 2022.
2049	TCP	NFS	Cliente NFS	Nós de administração	Usado pela exportação de auditoria baseada em NFS (NFS). **Nota:** esta porta é necessária apenas se a exportação de auditoria baseada em NFS estiver ativada. **Observação:** o suporte para NFS foi obsoleto e será removido em uma versão futura.
5353	UDP	MDNS	Todos os nós	Todos os nós	Fornece o serviço de DNS multicast (mDNS) que é usado para alterações de IP de grade completa e para descoberta de nó de administrador principal durante a instalação, expansão e recuperação.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
5696	TCP	KMIP	Aparelho	KMS	Tráfego externo KMIP (Key Management Interoperability Protocol) de dispositivos configurados para criptografia de nó para o servidor de gerenciamento de chaves (KMS), a menos que uma porta diferente seja especificada na página de configuração KMS do instalador do dispositivo StorageGRID.
8022	TCP	SSH	Serviço de laptop	Todos os nós	O SSH na porta 8022 concede acesso ao sistema operacional básico em plataformas de appliance e nó virtual para suporte e solução de problemas. Essa porta não é usada para nós baseados em Linux (bare metal) e não é necessária para ser acessível entre nós de grade ou durante operações normais.
8443	TCP	HTTPS	Navegador	Nós de administração	Opcional. Usado por navegadores da Web e clientes de API de gerenciamento para acessar o Gerenciador de Grade. Pode ser usado para separar as comunicações do Grid Manager e do Tenant Manager. **Nota**: Se você fechar as portas 443 ou 8443 do Gerenciador de Grade, qualquer usuário conetado atualmente em uma porta bloqueada, incluindo você, perderá o acesso ao Gerenciador de Grade, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados. "Configurar controles de firewall"Consulte para configurar endereços IP privilegiados.
9022	TCP	SSH	Serviço de laptop	Aparelhos	Concede acesso a dispositivos StorageGRID no modo de pré-configuração para suporte e solução de problemas. Esta porta não é necessária para estar acessível entre nós de grade ou durante operações normais.
9091	TCP	HTTPS	Serviço Grafana externo	Nós de administração	Usado por serviços externos Grafana para acesso seguro ao serviço StorageGRID Prometheus. **Nota:** esta porta só é necessária se o acesso Prometheus baseado em certificado estiver ativado.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
9092	TCP	Kafka	Nós de storage com ADC	Cluster Kafka	Usado para mensagens de serviços de plataforma enviadas para um cluster Kafka. Os locatários podem substituir a configuração padrão de porta Kafka de 9092 ao criar um endpoint.
9443	TCP	HTTPS	Navegador	Nós de administração	Opcional. Usado por navegadores da Web e clientes de API de gerenciamento para acessar o Gerenciador de locatários. Pode ser usado para separar as comunicações do Grid Manager e do Tenant Manager.
18082	TCP	HTTPS	S3 clientes	Nós de storage	Tráfego de clientes de S3 U diretamente para nós de storage (HTTPS).
18083	TCP	HTTPS	Clientes Swift	Nós de storage	Tráfego de cliente ágil diretamente para nós de storage (HTTPS).
18084	TCP	HTTP	S3 clientes	Nós de storage	Tráfego de cliente S3 diretamente para nós de storage (HTTP).
18085	TCP	HTTP	Clientes Swift	Nós de storage	Tráfego de cliente rápido diretamente para nós de armazenamento (HTTP).
23000-23999	TCP	HTTPS	Todos os nós na grade de origem para replicação entre grade	Nós de administração e nós de gateway na grade de destino para replicação entre grade	Esse intervalo de portas é reservado para conexões de federação de grade. Ambas as grades em uma determinada conexão usam a mesma porta.

Início rápido para StorageGRID

Siga estas etapas de alto nível para configurar e usar qualquer sistema StorageGRID.

1 Aprenda, Planeje e colete dados

Trabalhe com o representante da sua conta NetApp para entender as opções e Planejar seu novo sistema StorageGRID. Considere estes tipos de perguntas:

- Quantos dados de objetos você espera armazenar inicialmente e ao longo do tempo?

- Quantos sites você precisa?
- Quantos e quais tipos de nós você precisa em cada local?
- Quais redes StorageGRID você usará?
- Quem usará sua grade para armazenar objetos? Quais aplicativos eles usarão?
- Você tem algum requisito especial de segurança ou armazenamento?
- Você precisa cumprir com quaisquer requisitos legais ou regulamentares?

Opcionalmente, trabalhe com seu consultor de serviços profissionais da NetApp para acessar a ferramenta NetApp ConfigBuilder para concluir uma pasta de trabalho de configuração para uso ao instalar e implantar seu novo sistema. Você também pode usar essa ferramenta para ajudar a automatizar a configuração de qualquer dispositivo StorageGRID. "Automatize a instalação e a configuração do dispositivo"Consulte .

Revisão "Saiba mais sobre o StorageGRID" e "Diretrizes de rede".

Instalar nós

Um sistema StorageGRID consiste em nós individuais baseados em hardware e em software. Primeiro, você instala o hardware para cada nó de dispositivo e configura cada host Linux ou VMware.

Para concluir a instalação, instale o software StorageGRID em cada dispositivo ou host de software e conete os nós a uma grade. Durante esta etapa, você fornece nomes de sites e nós, detalhes de sub-rede e os endereços IP para seus servidores NTP e DNS.

Saiba como:

- "Instale o hardware do dispositivo"
- "Instale o StorageGRID no Red Hat Enterprise Linux"
- "Instale o StorageGRID no Ubuntu ou Debian"
- "Instale o StorageGRID no VMware"

Inicie sessão e verifique a integridade do sistema

Assim que você instalar o nó Admin principal, você pode entrar no Gerenciador de Grade. A partir daí, você pode analisar a integridade geral do seu novo sistema, ativar AutoSupport e e-mails de alerta e configurar nomes de domínio de endpoint S3.

Saiba como:

- "Faça login no Gerenciador de Grade"
- "Monitorar a integridade do sistema"
- "Configurar o AutoSupport"
- "Configurar notificações por e-mail para alertas"
- "Configurar nomes de domínio de endpoint S3"

Configurar e gerenciar

As tarefas de configuração que você precisa executar para um novo sistema StorageGRID dependem de

como você usará sua grade. No mínimo, você configura o acesso ao sistema; usa os assistentes FabricPool e S3 e gerencia várias configurações de armazenamento e segurança.

Saiba como:

- "Controle o acesso à StorageGRID"
- "Utilize o assistente de configuração S3"
- "Use o assistente de configuração do FabricPool"
- "Gerenciar a segurança"
- "Endurecimento do sistema"

Configurar o ILM

Você controla o posicionamento e a duração de cada objeto em seu sistema StorageGRID configurando uma política de gerenciamento do ciclo de vida das informações (ILM) que consiste em uma ou mais regras do ILM. As regras do ILM instruem o StorageGRID a criar e distribuir cópias de dados de objetos e como gerenciar essas cópias ao longo do tempo.

Saiba como: "Gerenciar objetos com ILM"

Use o StorageGRID

Após a conclusão da configuração inicial, as contas de locatário do StorageGRID podem usar aplicativos cliente S3 para obter, recuperar e excluir objetos.

Saiba como:

- "Use uma conta de locatário"
- "Use a API REST do S3"

Monitorar e solucionar problemas

Quando o sistema estiver funcionando, você deve monitorar suas atividades regularmente e solucionar problemas e resolver quaisquer alertas. Você também pode querer configurar um servidor syslog externo, usar monitoramento SNMP ou coletar dados adicionais.

Saiba como:

- "Monitore o StorageGRID"
- "Solucionar problemas do StorageGRID"

Expanda, mantenha e recupere

Você pode adicionar nós ou sites para expandir a capacidade ou a funcionalidade do seu sistema. Você também pode executar vários procedimentos de manutenção para recuperar de falhas ou manter seu sistema StorageGRID atualizado e com desempenho eficiente.

Saiba como:

- "Expanda uma grade"
- "Mantenha sua grade"
- "Recuperar nós"

Instale, atualize e hotfix StorageGRID

Dispositivos StorageGRID

```
https://docs.netapp.com/us-en/storagegrid-
appliances/index.html["Documentação do StorageGRID Appliance"^]Acesse para
saber como instalar, configurar e manter dispositivos de armazenamento e
serviços StorageGRID.
```

Instale o StorageGRID no Red Hat Enterprise Linux

Início rápido para instalar o StorageGRID no Red Hat Enterprise Linux

Siga estas etapas de alto nível para instalar um nó StorageGRID do Red Hat Enterprise Linux (RHEL).

Preparação

- Saiba mais "Topologia de rede e arquitetura StorageGRID"sobre .
- Saiba mais sobre as especificidades "Rede StorageGRID"do .
- Reúna e prepare o "Informações e materiais necessários".
- Prepare o "CPU e RAM"necessário .
- Fornecer para "requisitos de storage e desempenho".
- "Prepare os servidores Linux" Isso hospedará seus nós do StorageGRID.

Implantação

Implante nós de grade. Quando você implementa nós de grade, eles são criados como parte do sistema StorageGRID e conetados a uma ou mais redes.

- Para implantar nós de grade baseados em software nos hosts preparados na etapa 1, use a linha de comando do Linux e "arquivos de configuração do nó"o .
- Para implantar os nós de dispositivos StorageGRID, siga o "Início rápido para instalação de hardware".

Configuração

Quando todos os nós tiverem sido implantados, use o Gerenciador de Grade para "configure a grade e conclua a instalação".

Automatize a instalação

Para economizar tempo e fornecer consistência, você pode automatizar a instalação do serviço de host StorageGRID e a configuração de nós de grade.

- Use uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef, para automatizar:
  - Instalação do RHEL
  - Configuração de rede e armazenamento
  - Instalação do mecanismo de contêiner e do serviço host do StorageGRID
  - Implantação de nós de grade virtual

  "Automatize a instalação e a configuração do serviço de host StorageGRID"Consulte .
- Depois de implantar nós de grade, "Automatize a configuração do sistema StorageGRID" usando o script de configuração Python fornecido no arquivo de instalação.
- "Automatize a instalação e a configuração dos nós de grade do dispositivo"
- Se você é um desenvolvedor avançado de implantações do StorageGRID, automatize a instalação de nós de grade usando o "API REST de instalação".

Planeje e prepare-se para a instalação no Red Hat

Informações e materiais necessários

Antes de instalar o StorageGRID, reúna e prepare as informações e materiais necessários.

Informações necessárias

Plano de rede

Quais redes você pretende anexar a cada nó do StorageGRID. O StorageGRID suporta várias redes para separação de tráfego, segurança e conveniência administrativa.

Consulte o StorageGRID "Diretrizes de rede".

Informações de rede

Endereços IP para atribuir a cada nó de grade e aos endereços IP dos servidores DNS e NTP.

Servidores para nós de grade

Identifique um conjunto de servidores (físicos, virtuais ou ambos) que, no agregado, fornecem recursos suficientes para suportar o número e o tipo de nós do StorageGRID que você planeja implantar.

> ⓘ Se a instalação do StorageGRID não usar nós de armazenamento do StorageGRID Appliance (hardware), você deve usar o armazenamento RAID de hardware com cache de gravação (BBWC) com bateria. O StorageGRID não suporta o uso de redes de área de armazenamento virtual (VSANs), RAID de software ou nenhuma proteção RAID.

Migração de nós (se necessário)

Entenda o "requisitos para migração de nós", se você quiser executar a manutenção programada em hosts físicos sem qualquer interrupção do serviço.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Materiais necessários

Licença NetApp StorageGRID

Você deve ter uma licença NetApp válida e assinada digitalmente.

> Uma licença de não produção, que pode ser usada para testar e testar grades de prova de conceito, está incluída no arquivo de instalação do StorageGRID.

Arquivo de instalação do StorageGRID

"Baixe o arquivo de instalação do StorageGRID e extraia os arquivos".

Serviço de laptop

O sistema StorageGRID é instalado através de um computador portátil de serviço.

O computador portátil de serviço deve ter:

- Porta de rede
- Cliente SSH (por exemplo, PuTTY)
- "Navegador da Web suportado"

Documentação do StorageGRID

- "Notas de lançamento"
- "Instruções para administrar o StorageGRID"

Baixe e extraia os arquivos de instalação do StorageGRID

Você deve baixar o arquivo de instalação do StorageGRID e extrair os arquivos necessários. Opcionalmente, você pode verificar manualmente os arquivos no pacote de instalação.

Passos

1. Vá para "Página de downloads do NetApp para StorageGRID" .
2. Selecione o botão para baixar a versão mais recente ou selecione outra versão no menu suspenso e selecione **Go**.
3. Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.
4. Se for apresentada uma instrução Caution/MustRead, leia-a e selecione a caixa de verificação.

> Você deve aplicar os hotfixes necessários depois de instalar a versão do StorageGRID. Para obter mais informações, consulte "procedimento de hotfix nas instruções de recuperação e manutenção".

5. Leia o Contrato de Licença de Utilizador final, selecione a caixa de verificação e, em seguida, selecione **Accept & continue**.
6. Na coluna **Instalar StorageGRID**, selecione o arquivo de instalação .tgz ou .zip para o Red Hat Enterprise Linux.

> Selecione o `.zip` ficheiro se estiver a executar o Windows no computador portátil de serviço.

7. Salve o arquivo de instalação.
8. se você precisa verificar o arquivo de instalação:
   a. Baixe o pacote de verificação de assinatura de código StorageGRID. O nome do arquivo deste pacote usa o formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`, onde `<version-number>` está a versão do software StorageGRID.
   b. Siga os passos para "verifique manualmente os arquivos de instalação".
9. Extraia os arquivos do arquivo de instalação.
10. Escolha os arquivos que você precisa.

    Os arquivos de que você precisa dependem da topologia de grade planejada e de como implantar o sistema StorageGRID.

    Os caminhos listados na tabela são relativos ao diretório de nível superior instalado pelo arquivo de instalação extraído

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.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL.
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 `configure-storagegrid.py` 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. Você também pode usar este script para integração Ping federate.

Caminho e nome do arquivo	Descrição
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.
	Exemplo de função do Ansible e manual de estratégia para configurar hosts do RHEL para implantação de contêineres do StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.
	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.

Verificar manualmente os arquivos de instalação (opcional)

Se necessário, você pode verificar manualmente os arquivos no arquivo de instalação do StorageGRID.

Antes de começar

Você tem "download do pacote de verificação"do "Página de downloads do NetApp para StorageGRID".

Passos

1. Extraia os artefatos do pacote de verificação:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Certifique-se de que estes artefactos foram extraídos:
   - Folha de certificado: `Leaf-Cert.pem`
   - Cadeia de certificados: `CA-Int-Cert.pem`
   - Cadeia de resposta do carimbo de hora: `TS-Cert.pem`
   - Ficheiro checksum: `sha256sum`

- Assinatura do checksum: `sha256sum.sig`
- Ficheiro de resposta do carimbo de hora: `sha256sum.sig.tsr`

3. Utilize a corrente para verificar se o certificado de lâminas é válido.

   Exemplo: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

   Saída esperada: `Leaf-Cert.pem: OK`

4. Se a etapa *2* falhou devido a um certificado de folha expirado, use o `tsr` arquivo para verificar.

   Exemplo: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

   Saída esperada inclui: `Verification: OK`

5. Crie um arquivo de chave pública a partir do certificado Leaf.

   Exemplo: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

   Saída esperada: *None*

6. Use a chave pública para verificar o `sha256sum` arquivo contra `sha256sum.sig`.

   Exemplo: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

   Saída esperada: `Verified OK`

7. Verifique o `sha256sum` conteúdo do arquivo em relação às somas de verificação recém-criadas.

   Exemplo: `sha256sum -c sha256sum`

   Saída esperada: `<filename>: OK`
   `<filename>` É o nome do arquivo que você baixou.

8. "Conclua as etapas restantes" para extrair e escolher os arquivos apropriados do arquivo de instalação.

Requisitos de software para Red Hat Enterprise Linux

Você pode usar uma máquina virtual para hospedar qualquer tipo de nó StorageGRID. Você precisa de uma máquina virtual para cada nó de grade.

Para instalar o StorageGRID no Red Hat Enterprise Linux (RHEL), você deve instalar alguns pacotes de software de terceiros. Algumas distribuições Linux suportadas não contêm esses pacotes por padrão. As versões de pacotes de software em que as instalações do StorageGRID são testadas incluem as listadas nesta página.

Se você selecionar uma opção de instalação de runtime de distribuição Linux e container que exija qualquer um desses pacotes e eles não forem instalados automaticamente pela distribuição Linux, instale uma das versões listadas aqui se disponível no seu provedor ou no fornecedor de suporte para sua distribuição Linux. Caso contrário, use as versões de pacote padrão disponíveis do seu fornecedor.

Todas as opções de instalação requerem Podman ou Docker. Não instale ambos os pacotes. Instale apenas o pacote exigido pela opção de instalação.

O suporte para Docker como o mecanismo de contentor para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contentor em uma versão futura.

Versões Python testadas

- 3,5.2-2
- 3,6.8-2
- 3,6.8-38
- 3,6.9-1
- 3,7.3-1
- 3,8.10-0
- 3,9.2-1
- 3,9.10-2
- 3,9.16-1
- 3,10.6-1
- 3,11.2-6

Versões do Podman testadas

- 3,2.3-0
- 3,4.4-ds1
- 4,1.1-7
- 4,2.0-11
- 4,3.1-ds1-8-b1
- 4,4.1-8
- 4,4.1-12

Versões do Docker testadas

O suporte do Docker está obsoleto e será removido em uma versão futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1,5-2

Requisitos de CPU e RAM

Antes de instalar o software StorageGRID, verifique e configure o hardware para que ele esteja pronto para suportar o sistema StorageGRID.

Cada nó do StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Depende do total de RAM disponível e da quantidade de software que não seja StorageGRID executado no sistema
  - Geralmente, pelo menos 24 GB por nó e 2 a 16 GB menos do que a RAM total do sistema
  - Um mínimo de 64 GB para cada locatário que terá aproximadamente 5.000 buckets

Certifique-se de que o número de nós de StorageGRID que você planeja executar em cada host físico ou virtual não exceda o número de núcleos de CPU ou a RAM física disponível. Se os hosts não forem dedicados à execução do StorageGRID (não recomendado), certifique-se de considerar os requisitos de recursos dos outros aplicativos.

> ⓘ Monitore regularmente o uso da CPU e da memória para garantir que esses recursos continuem a acomodar sua carga de trabalho. Por exemplo, duplicar a alocação de RAM e CPU para nós de storage virtual forneceria recursos semelhantes aos fornecidos para nós de dispositivos StorageGRID. Além disso, se a quantidade de metadados por nó exceder 500 GB, considere aumentar a RAM por nó para 48 GB ou mais. Para obter informações sobre como gerenciar o armazenamento de metadados de objetos, aumentar a configuração espaço reservado de metadados e monitorar o uso da CPU e da memória, consulte as instruções para "administrar", "monitorização"e "a atualizar"StorageGRID.

Se o hyperthreading estiver habilitado nos hosts físicos subjacentes, você poderá fornecer 8 núcleos virtuais (4 núcleos físicos) por nó. Se o hyperthreading não estiver habilitado nos hosts físicos subjacentes, você deverá fornecer 8 núcleos físicos por nó.

Se você estiver usando máquinas virtuais como hosts e tiver controle sobre o tamanho e o número de VMs, use uma única VM para cada nó do StorageGRID e dimensione a VM de acordo.

Para implantações de produção, você não deve executar vários nós de storage no mesmo hardware de storage físico ou host virtual. Cada nó de storage em uma única implantação do StorageGRID deve estar em seu próprio domínio de falha isolado. Você pode maximizar a durabilidade e a disponibilidade dos dados de objetos se garantir que uma única falha de hardware só pode afetar um único nó de storage.

Consulte também "Requisitos de storage e desempenho".

Requisitos de storage e desempenho

Você precisa entender os requisitos de storage para nós do StorageGRID para que possa fornecer espaço suficiente para dar suporte à configuração inicial e à expansão de storage futura.

Os nós de StorageGRID exigem três categorias lógicas de storage:

- **Pool de contentores** — armazenamento de nível de desempenho (SAS ou SSD de 10K GB) para os contentores de nós, que serão atribuídos ao driver de armazenamento do mecanismo de contentor quando você instalar e configurar o mecanismo de contentor nos hosts que suportarão seus nós

StorageGRID.

- **Dados do sistema** — armazenamento em camada de desempenho (SAS ou SSD de 10K GB) para armazenamento persistente por nó de dados do sistema e logs de transações, que os serviços de host do StorageGRID consumirão e mapearão em nós individuais.
- **Dados de objeto** — armazenamento em camada de desempenho (SAS ou SSD de 10K TB) e armazenamento em massa de camada de capacidade (NL-SAS/SATA) para armazenamento persistente de dados de objetos e metadados de objetos.

Você deve usar dispositivos de bloco compatíveis com RAID para todas as categorias de armazenamento. Discos não redundantes, SSDs ou JBODs não são suportados. Você pode usar o armazenamento RAID compartilhado ou local para qualquer uma das categorias de armazenamento. No entanto, se quiser usar a funcionalidade de migração de nós no StorageGRID, você deve armazenar dados do sistema e dados de objetos no armazenamento compartilhado. Para obter mais informações, "Requisitos de migração de contêiner de nós"consulte .

Requisitos de desempenho

A performance dos volumes usados para o pool de contêineres, dados do sistema e metadados de objetos afeta significativamente o desempenho geral do sistema. Você deve usar o storage de camada de desempenho (SAS ou SSD de 10K GB) para esses volumes, a fim de garantir um desempenho de disco adequado em termos de latência, IOPS/operações de entrada/saída por segundo (IOPS) e taxa de transferência. Você pode usar o storage de camada de capacidade (NL-SAS/SATA) para o storage persistente de dados de objetos.

Os volumes usados para o pool de contêineres, dados do sistema e dados de objetos precisam ter o armazenamento em cache de gravação habilitado. O cache deve estar em uma Mídia protegida ou persistente.

Requisitos para hosts que usam storage NetApp ONTAP

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.

Número de hosts necessários

Cada local do StorageGRID requer um mínimo de três nós de storage.

> 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.

Outros tipos de nós, como nós de administração ou nós de gateway, podem ser implantados nos mesmos hosts ou podem ser implantados em seus próprios hosts dedicados, conforme necessário.

Número de volumes de storage para cada host

A tabela a seguir mostra o número de volumes de storage (LUNs) necessários para cada host e o tamanho

mínimo necessário para cada LUN, com base em quais nós serão implantados nesse host.

O tamanho máximo de LUN testado é de 39 TB.

Esses números são para cada host, não para toda a grade.

Finalidade do LUN	Categoria de armazenamento	Número de LUNs	Tamanho mínimo/LUN
Pool de armazenamento do mecanismo de contêiner	Pool de contêineres	1	Número total de nós x 100 GB
`/var/local` volume	Dados do sistema	1 para cada nó neste host	90 GB
Nó de storage	Dados de objeto	3 para cada nó de storage nesse host **Nota:** Um nó de armazenamento baseado em software pode ter 1 a 16 volumes de armazenamento; pelo menos 3 volumes de armazenamento são recomendados.	12 TB (4 TB/LUN) consulte Requisitos de storage para nós de storage para obter mais informações.
Nó de storage (somente metadados)	Metadados de objetos	1	4 TB consulte Requisitos de storage para nós de storage para obter mais informações. **Nota**: Somente um rangedb é necessário para nós de storage somente metadados.
Logs de auditoria do nó de administração	Dados do sistema	1 para cada nó de administração neste host	200 GB
Tabelas Admin Node	Dados do sistema	1 para cada nó de administração neste host	200 GB

Dependendo do nível de auditoria configurado, do tamanho das entradas do usuário, como o nome da chave do objeto S3 e da quantidade de dados de log de auditoria que você precisa preservar, talvez seja necessário aumentar o tamanho do LUN de log de auditoria em cada nó Admin. Geralmente, uma grade gera aproximadamente 1 KB de dados de auditoria por operação S3, o que significaria que um LUN de 200 GB suportaria 70 milhões de operações por dia ou 800 operações por segundo por dois a três dias.

Espaço de armazenamento mínimo para um host

A tabela a seguir mostra o espaço de armazenamento mínimo necessário para cada tipo de nó. Você pode usar essa tabela para determinar a quantidade mínima de storage que deve fornecer ao host em cada categoria de storage, com base nos nós que serão implantados nesse host.

> Snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte "recuperação do nó de grade"os procedimentos para cada tipo de nó.

Tipo de nó	Pool de contêineres	Dados do sistema	Dados de objeto
Nó de storage	100 GB	90 GB	4.000 GB
Nó de administração	100 GB	490 GB (3 LUNs)	*não aplicável*
Nó de gateway	100 GB	90 GB	*não aplicável*

Exemplo: Calculando os requisitos de armazenamento de um host

Suponha que você Planeje implantar três nós no mesmo host: Um nó de storage, um nó de administrador e um nó de gateway. Forneça no mínimo nove volumes de storage ao host. Você precisará de um mínimo de 300 GB de storage em camadas de desempenho para os contêineres de nós, 670 GB de storage em camadas de desempenho para dados do sistema e logs de transações e 12 TB de storage em camadas de capacidade para dados de objetos.

Tipo de nó	Finalidade do LUN	Número de LUNs	Tamanho da LUN
Nó de storage	Pool de armazenamento do mecanismo de contêiner	1	300 GB (100 GB/nó)
Nó de storage	`/var/local` volume	1	90 GB
Nó de storage	Dados de objeto	3	12 TB (4 TB/LUN)
Nó de administração	`/var/local` volume	1	90 GB
Nó de administração	Logs de auditoria do nó de administração	1	200 GB
Nó de administração	Tabelas Admin Node	1	200 GB
Nó de gateway	`/var/local` volume	1	90 GB

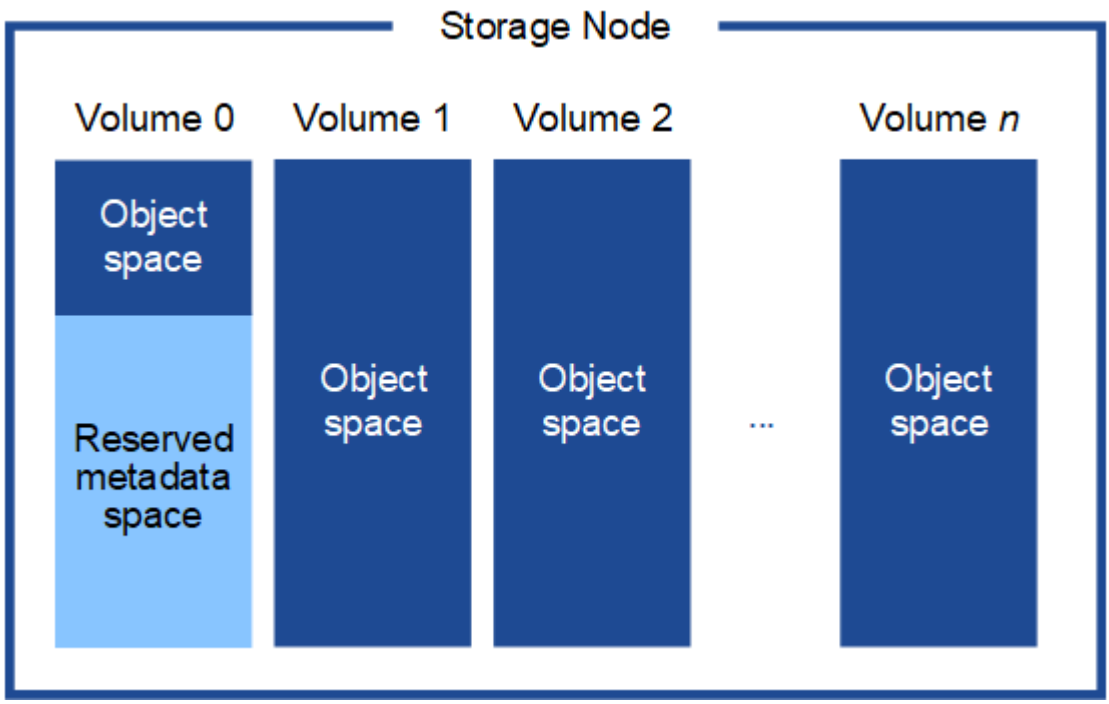
Tipo de nó	Finalidade do LUN	Número de LUNs	Tamanho da LUN
Total		**9**	• Conjunto de contentores: * 300 GB **Dados do sistema:** 670 GB **Dados do objeto:** 12.000 GB

Requisitos de storage para nós de storage

Um nó de storage baseado em software pode ter 1 a 16 volumes de armazenamento—3 ou mais volumes de armazenamento são recomendados. Cada volume de armazenamento deve ser de 4 TB ou maior.

Um nó de storage de dispositivo pode ter até 48 volumes de storage.

Como mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de storage 0 de cada nó de storage. Qualquer espaço restante no volume de armazenamento 0 e quaisquer outros volumes de armazenamento no nó de armazenamento são usados exclusivamente para dados de objeto.



Para fornecer redundância e proteger os metadados de objetos contra perda, o StorageGRID armazena três cópias dos metadados de todos os objetos no sistema em cada local. As três cópias dos metadados de objetos são distribuídas uniformemente por todos os nós de storage em cada local.

Ao instalar uma grade com nós de storage somente de metadados, a grade também deve conter um número mínimo de nós para storage de objetos. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

- Para uma grade de um único local, pelo menos dois nós de storage são configurados para objetos e metadados.

- Para uma grade de vários locais, pelo menos um nó de storage por local é configurado para objetos e metadados.

Ao atribuir espaço ao volume 0 de um novo nó de storage, você deve garantir que haja espaço adequado para a parte desse nó de todos os metadados de objetos.

- No mínimo, você deve atribuir pelo menos 4 TB ao volume 0.

> Se você usar apenas um volume de armazenamento para um nó de armazenamento e atribuir 4 TB ou menos ao volume, o nó de armazenamento poderá entrar no estado somente leitura de armazenamento na inicialização e armazenar somente metadados de objetos.

> Se você atribuir menos de 500 GB ao volume 0 (somente uso não-produção), 10% da capacidade do volume de armazenamento será reservada para metadados.

- Se você estiver instalando um novo sistema (StorageGRID 11,6 ou superior) e cada nó de armazenamento tiver 128 GB ou mais de RAM, atribua 8 TB ou mais ao volume 0. O uso de um valor maior para o volume 0 pode aumentar o espaço permitido para metadados em cada nó de storage.
- Ao configurar diferentes nós de storage para um local, use a mesma configuração para o volume 0, se possível. Se um local contiver nós de storage de tamanhos diferentes, o nó de storage com o menor volume 0 determinará a capacidade de metadados desse local.

Para obter mais detalhes, "Gerenciar o storage de metadados de objetos"visite .

Requisitos de migração de contêiner de nós

O recurso de migração de nó permite mover manualmente um nó de um host para outro. Normalmente, ambos os hosts estão no mesmo data center físico.

A migração de nós permite executar a manutenção do host físico sem interromper as operações de grade. Você move todos os nós do StorageGRID, um de cada vez, para outro host antes de colocar o host físico off-line. A migração de nós requer apenas um curto período de inatividade para cada nó e não deve afetar a operação ou a disponibilidade dos serviços de grade.

Se você quiser usar o recurso de migração de nós do StorageGRID, sua implantação deve atender a requisitos adicionais:

- Nomes de interface de rede consistentes entre hosts em um único data center físico
- Storage compartilhado para volumes de repositório de objetos e metadados do StorageGRID que podem ser acessados por todos os hosts em um único data center físico. Por exemplo, você pode usar storage arrays do NetApp e-Series.

Se você estiver usando hosts virtuais e a camada de hypervisor subjacente suportar a migração de VM, talvez queira usar essa funcionalidade em vez do recurso de migração de nós no StorageGRID. Nesse caso, você pode ignorar esses requisitos adicionais.

Antes de executar a migração ou a manutenção do hipervisor, encerre os nós com simplicidade. Consulte as instruções para "fechando um nó de grade".

Migração do VMware Live não suportada

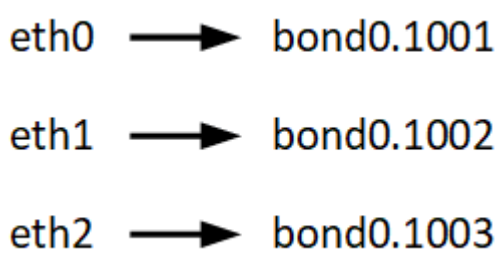
Ao executar a instalação bare-metal nas VMs VMware, o OpenStack Live Migration e o VMware Live vMotion fazem com que o tempo do relógio da máquina virtual salte e não seja compatível com nós de grade de qualquer tipo. Embora raros, tempos de clock incorretos podem resultar em perda de dados ou atualizações de configuração.

A migração fria é suportada. Na migração fria, você desliga os nós do StorageGRID antes de migrá-los entre hosts. Consulte as instruções para "fechando um nó de grade".

Nomes de interface de rede consistentes

Para mover um nó de um host para outro, o serviço de host StorageGRID precisa ter alguma confiança de que a conetividade de rede externa que o nó tem em seu local atual pode ser duplicada no novo local. Ele obtém essa confiança através do uso de nomes de interface de rede consistentes nos hosts.

Suponha, por exemplo, que o StorageGRID NodeA em execução no Host1 foi configurado com os seguintes mapeamentos de interface:



O lado esquerdo das setas corresponde às interfaces tradicionais vistas de dentro de um contentor StorageGRID (ou seja, as interfaces de rede de Grade, Admin e Cliente, respetivamente). O lado direito das setas corresponde às interfaces de host reais que fornecem essas redes, que são três interfaces VLAN subordinadas à mesma ligação de interface física.

Agora, suponha que você queira migrar NodeA para Host2. Se o Host2 também tiver interfaces chamadas bond0,1001, bond0,1002 e bond0,1003, o sistema permitirá a movimentação, assumindo que as interfaces com nomes semelhantes fornecerão a mesma conetividade no Host2 como no Host1. Se Host2 não tiver interfaces com os mesmos nomes, a movimentação não será permitida.

Há muitas maneiras de obter nomes consistentes de interface de rede entre vários hosts; "Configurando a rede host"consulte para obter alguns exemplos.

Armazenamento compartilhado

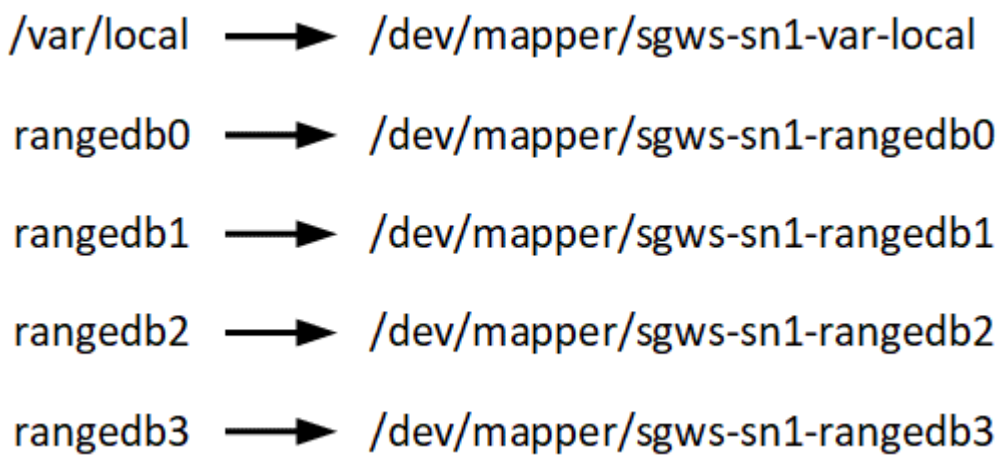
Para realizar migrações de nós rápidas e de baixa sobrecarga, o recurso de migração de nós do StorageGRID não move fisicamente os dados dos nós. Em vez disso, a migração de nós é realizada como um par de operações de exportação e importação, da seguinte forma:

1. Durante a operação de "exportação de nó", uma pequena quantidade de dados de estado persistente é extraída do contentor de nó em execução no HostA e armazenada em cache no volume de dados do sistema desse nó. Em seguida, o contentor de nó no HostA é desinstanciado.
2. Durante a operação de "importação de nó", o contentor de nó no HostB que usa a mesma interface de rede e mapeamentos de armazenamento de bloco que estavam em vigor no HostA é instanciado. Em seguida, os dados de estado persistente em cache são inseridos na nova instância.

Dado este modo de operação, todos os dados do sistema do nó e volumes de armazenamento de objetos

devem estar acessíveis a partir de HostA e HostB para que a migração seja permitida e funcione. Além disso, eles devem ter sido mapeados para o nó usando nomes que são garantidos para se referir aos mesmos LUNs no HostA e HostB.

O exemplo a seguir mostra uma solução para o mapeamento de dispositivos de bloco para um nó de armazenamento StorageGRID, onde o multipathing DM está em uso nos hosts, e o campo alias foi usado `/etc/multipath.conf` para fornecer nomes de dispositivos de bloco consistentes e amigáveis disponíveis em todos os hosts.



Preparar os anfitriões (Red Hat)

Como as configurações de todo o host mudam durante a instalação

Em sistemas bare metal, o StorageGRID faz algumas alterações nas configurações de todo o host `sysctl`.

As seguintes alterações são feitas:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288
```

```
# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536
```

```
# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Instale o Linux

Você deve instalar o StorageGRID em todos os hosts de grade do Red Hat Enterprise Linux. Para obter uma lista de versões suportadas, utilize a ferramenta de Matriz de interoperabilidade do NetApp.

Antes de começar

Certifique-se de que seu sistema operacional atenda aos requisitos mínimos de versão do kernel do StorageGRID, conforme listado abaixo. Use o comando `uname -r` para obter a versão do kernel do seu sistema operacional ou consulte o fornecedor do seu sistema operacional.

Versão Red Hat Enterprise Linux	Versão mínima do kernel	Nome do pacote do kernel
8,8 (obsoleto)	4.18.0-477.10.1.el8_8.x86_64	kernel-4.18.0-477.10.1.el8_8.x86_64
8,10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9,0 (obsoleto)	5.14.0-70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64
9,2 (obsoleto)	5.14.0-284.11.1.el9_2.x86_64	kernel-5.14.0-284.11.1.el9_2.x86_64
9,4	5.14.0-427.18.1.el9_4.x86_64	kernel-5.14.0-427.18.1.el9_4.x86_64

Passos

1. Instale o Linux em todos os hosts de grade física ou virtual de acordo com as instruções do distribuidor ou seu procedimento padrão.

   > Se você estiver usando o instalador padrão do Linux, selecione a configuração do software "nó de computação", se disponível, ou o ambiente base "instalação mínima". Não instale nenhum ambiente de desktop gráfico.

2. Certifique-se de que todos os hosts tenham acesso aos repositórios de pacotes, incluindo o canal Extras.

   Você pode precisar desses pacotes adicionais mais tarde neste procedimento de instalação.

3. Se a troca estiver ativada:

a. Execute o seguinte comando: `$ sudo swapoff --all`

b. Remova todas as entradas de troca de `/etc/fstab` para persistir as configurações.

> A falha ao desativar completamente a troca pode reduzir drasticamente o desempenho.

Configurar a rede host (Red Hat Enterprise Linux)

Depois de concluir a instalação do Linux em seus hosts, você pode precisar executar alguma configuração adicional para preparar um conjunto de interfaces de rede em cada host que são adequadas para mapear nos nós do StorageGRID que você implantará posteriormente.

Antes de começar

- Você revisou o "Diretrizes de rede da StorageGRID".
- Você revisou as informações "requisitos de migração de contêiner de nós"sobre .
- Se você estiver usando hosts virtuais, leia o Considerações e recomendações para clonagem de endereços MAC antes de configurar a rede host.

> Se você estiver usando VMs como hosts, selecione VMXNET 3 como o adaptador de rede virtual. O adaptador de rede VMware E1000 causou problemas de conetividade com os contentores StorageGRID implantados em determinadas distribuições do Linux.

Sobre esta tarefa

Os nós de grade devem ser capazes de acessar a rede de grade e, opcionalmente, as redes Admin e Client. Você fornece esse acesso criando mapeamentos que associam a interface física do host às interfaces virtuais para cada nó de grade. Ao criar interfaces de host, use nomes amigáveis para facilitar a implantação em todos os hosts e habilitar a migração.

A mesma interface pode ser compartilhada entre o host e um ou mais nós. Por exemplo, você pode usar a mesma interface para acesso ao host e acesso à rede de administração de nó, para facilitar a manutenção do host e do nó. Embora a mesma interface possa ser compartilhada entre o host e os nós individuais, todos devem ter endereços IP diferentes. Os endereços IP não podem ser compartilhados entre nós ou entre o host e qualquer nó.

Você pode usar a mesma interface de rede de host para fornecer a interface de rede de grade para todos os nós de StorageGRID no host; você pode usar uma interface de rede de host diferente para cada nó; ou você pode fazer algo entre eles. No entanto, você normalmente não fornecerá a mesma interface de rede de host que as interfaces de rede de Grade e Admin para um único nó ou como a interface de rede de Grade para um nó e a interface de rede de Cliente para outro.

Você pode concluir esta tarefa de várias maneiras. Por exemplo, se seus hosts forem máquinas virtuais e você estiver implantando um ou dois nós de StorageGRID para cada host, você poderá criar o número correto de interfaces de rede no hypervisor e usar um mapeamento de 1 para 1. Se você estiver implantando vários nós em hosts bare metal para uso em produção, poderá aproveitar o suporte da pilha de rede Linux para VLAN e LACP para tolerância a falhas e compartilhamento de largura de banda. As seções a seguir fornecem abordagens detalhadas para ambos os exemplos. Você não precisa usar nenhum desses exemplos; você pode usar qualquer abordagem que atenda às suas necessidades.

Não use dispositivos bond ou bridge diretamente como a interface de rede do contentor. Isso pode impedir a inicialização do nó causada por um problema de kernel com o uso do MACVLAN com dispositivos de ligação e ponte no namespace do contentor. Em vez disso, use um dispositivo não-bond, como um par VLAN ou Ethernet virtual (vete). Especifique este dispositivo como a interface de rede no arquivo de configuração do nó.

Informações relacionadas

"Criando arquivos de configuração de nó"

Considerações e recomendações para clonagem de endereços MAC

A clonagem de endereços MAC faz com que o contentor use o endereço MAC do host e o host use o endereço MAC de um endereço especificado ou gerado aleatoriamente. Você deve usar a clonagem de endereços MAC para evitar o uso de configurações de rede de modo promíscuo.

Ativar a clonagem MAC

Em certos ambientes, a segurança pode ser aprimorada por meio da clonagem de endereços MAC, pois permite que você use uma NIC virtual dedicada para a rede Admin, rede Grid e rede Client. Ter o contentor usar o endereço MAC da NIC dedicada no host permite evitar o uso de configurações de rede de modo promíscuas.

A clonagem de endereços MAC destina-se a ser usada com instalações de servidores virtuais e pode não funcionar corretamente com todas as configurações de dispositivos físicos.

Se um nó não iniciar devido a uma interface de destino de clonagem MAC estar ocupada, talvez seja necessário definir o link para "baixo" antes de iniciar o nó. Além disso, é possível que o ambiente virtual possa impedir a clonagem de MAC em uma interface de rede enquanto o link estiver ativo. Se um nó não definir o endereço MAC e iniciar devido a uma interface estar ocupada, definir o link para "baixo" antes de iniciar o nó pode corrigir o problema.

A clonagem de endereços MAC está desativada por padrão e deve ser definida por chaves de configuração de nós. Você deve ativá-lo quando instalar o StorageGRID.

Há uma chave para cada rede:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Definir a chave como "verdadeiro" faz com que o contentor use o endereço MAC da NIC do host. Além disso, o host usará o endereço MAC da rede de contentores especificada. Por padrão, o endereço do contentor é um endereço gerado aleatoriamente, mas se você tiver definido um usando a `_NETWORK_MAC` chave de configuração do nó, esse endereço será usado em vez disso. O host e o contentor sempre terão endereços MAC diferentes.

Ativar a clonagem MAC em um host virtual sem também ativar o modo promíscuo no hypervisor pode fazer com que a rede de host Linux usando a interface do host pare de funcionar.

Casos de uso de clonagem DE MAC

Existem dois casos de uso a considerar com clonagem MAC:

- Clonagem DE MAC não ativada: Quando a `_CLONE_MAC` chave no arquivo de configuração do nó não estiver definida ou definida como "falsa", o host usará o MAC da NIC do host e o contentor terá um MAC gerado pelo StorageGRID, a menos que um MAC seja especificado na `_NETWORK_MAC` chave. Se um endereço for definido na `_NETWORK_MAC` chave, o contentor terá o endereço especificado na `_NETWORK_MAC` chave. Esta configuração de chaves requer o uso do modo promíscuo.
- Clonagem DO MAC ativada: Quando a `_CLONE_MAC` chave no arquivo de configuração do nó é definida como "verdadeiro", o contentor usa o MAC da NIC do host e o host usa um MAC gerado pelo StorageGRID, a menos que um MAC seja especificado na `_NETWORK_MAC` chave. Se um endereço for definido na `_NETWORK_MAC` chave, o host usará o endereço especificado em vez de um gerado. Nesta configuração de chaves, você não deve usar o modo promíscuo.

> ⓘ Se você não quiser usar a clonagem de endereços MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes dos atribuídos pelo hypervisor, verifique se as propriedades de segurança nos níveis de switch virtual e grupo de portas estão definidas como **Accept** para modo promíscuo, alterações de endereço MAC e transmissões forjadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Para ativar a clonagem MAC, consulte o "instruções para criar arquivos de configuração de nó".

Exemplo de clonagem DE MAC

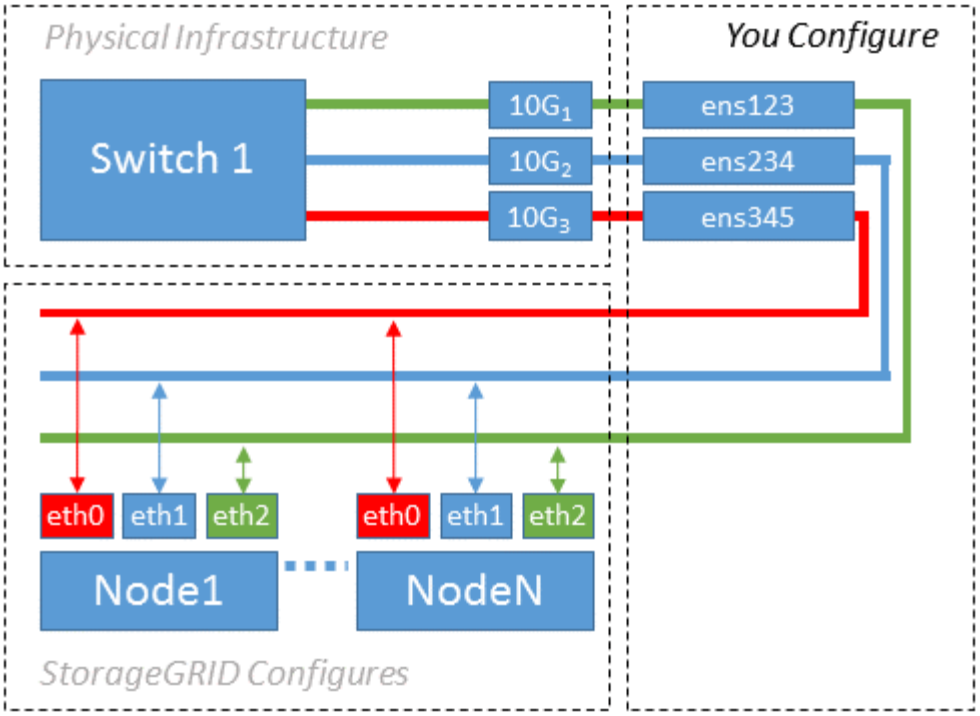
Exemplo de clonagem MAC ativada com um host com endereço MAC de 11:22:33:44:55:66 para a interface ens256 e as seguintes chaves no arquivo de configuração do nó:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Resultado: O MAC do host para ens256 é B2:9c:02:C2:27:10 e o MAC da rede Admin é 11:22:33:44:55:66

Exemplo 1: Mapeamento de 1 para 1 para NICs físicos ou virtuais

O exemplo 1 descreve um mapeamento de interface física simples que requer pouca ou nenhuma configuração do lado do host.



O sistema operacional Linux cria as `ensXYZ` interfaces automaticamente durante a instalação ou inicialização, ou quando as interfaces são hot-added. Não é necessária nenhuma configuração além de garantir que as interfaces estejam configuradas para serem criadas automaticamente após a inicialização. Você tem que determinar qual `ensXYZ` corresponde à rede StorageGRID (Grade, Administrador ou Cliente) para que você possa fornecer os mapeamentos corretos posteriormente no processo de configuração.

Observe que a figura mostra vários nós de StorageGRID; no entanto, você normalmente usaria essa configuração para VMs de nó único.

Se o Switch 1 for um switch físico, você deverá configurar as portas conetadas às interfaces 10G1 a 10G3 para o modo de acesso e colocá-las nas VLANs apropriadas.

Exemplo 2: VLANs de transporte de ligação LACP

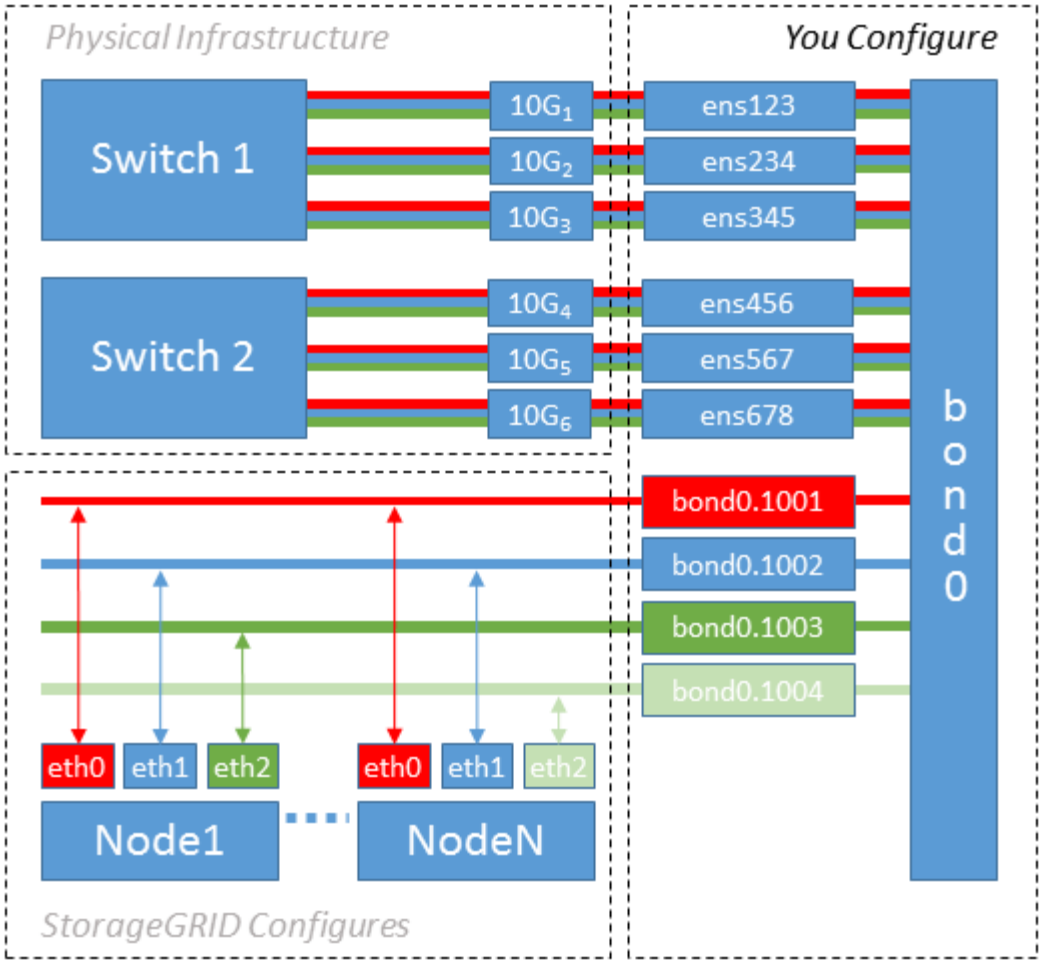
Sobre esta tarefa

O exemplo 2 assume que você está familiarizado com a ligação de interfaces de rede e com a criação de interfaces VLAN na distribuição Linux que você está usando.

O exemplo 2 descreve um esquema genérico, flexível e baseado em VLAN que facilita o compartilhamento de toda a largura de banda de rede disponível em todos os nós em um único host. Este exemplo é particularmente aplicável a hosts de metal nu.

Para entender esse exemplo, suponha que você tenha três sub-redes separadas para redes Grid, Admin e Client em cada data center. As sub-redes estão em VLANs separadas (1001, 1002 e 1003) e são apresentadas ao host em uma porta de tronco ligada ao LACP (bond0). Você configuraria três interfaces VLAN na ligação: bond0,1001, bond0,1002 e bond0,1003.

Se você precisar de VLANs e sub-redes separadas para redes de nós no mesmo host, você pode adicionar interfaces VLAN na ligação e mapeá-las no host (mostrado como bond0,1004 na ilustração).



Passos

1. Agregue todas as interfaces de rede físicas que serão usadas para conetividade de rede StorageGRID em uma única ligação LACP.

   Use o mesmo nome para o vínculo em cada host. Por exemplo, `bond0`.

2. Crie interfaces VLAN que usam essa ligação como seu "dispositivo físico" associado, usando a convenção de nomenclatura de interface VLAN padrão `physdev-name.VLAN ID`.

   Observe que as etapas 1 e 2 exigem a configuração apropriada nos switches de borda que terminam as outras extremidades dos links de rede. As portas do switch de borda também devem ser agregadas em um canal de porta LACP, configurado como um tronco, e ter permissão para passar todas as VLANs necessárias.

   Arquivos de configuração de interface de exemplo para este esquema de configuração de rede por host são fornecidos.

Informações relacionadas

"Exemplo /etc/sysconfig/network-scripts"

Configurar o armazenamento do host

Você deve alocar volumes de storage de bloco a cada host.

Antes de começar

Você revisou os tópicos a seguir, que fornecem informações necessárias para realizar esta tarefa:

- "Requisitos de storage e desempenho"
- "Requisitos de migração de contêiner de nós"

Sobre esta tarefa

Ao alocar LUNs (Block Storage volumes) para hosts, use as tabelas em "requisitos de armazenamento" para determinar o seguinte:

- Número de volumes necessários para cada host (com base no número e nos tipos de nós que serão implantados nesse host)
- Categoria de storage para cada volume (ou seja, dados do sistema ou dados de objeto)
- Tamanho de cada volume

Você usará essas informações, bem como o nome persistente atribuído pelo Linux a cada volume físico quando implantar nós do StorageGRID no host.

> Você não precisa particionar, formatar ou montar qualquer um desses volumes; você só precisa garantir que eles sejam visíveis para os hosts.

> Somente um LUN de dados de objeto é necessário para nós de storage somente de metadados.

Evite usar arquivos de dispositivo especiais "brutos" (`/dev/sdb`, por exemplo) ao compor sua lista de nomes de volume. Esses arquivos podem mudar através das reinicializações do host, o que afetará o funcionamento adequado do sistema. Se você estiver usando iSCSI LUNs e Device Mapper Multipathing, considere usar alias de multipath no `/dev/mapper` diretório, especialmente se a topologia SAN incluir caminhos de rede redundantes para o armazenamento compartilhado. Em alternativa, pode utilizar as ligações virtuais criadas pelo sistema em `/dev/disk/by-path/` para os nomes de dispositivos persistentes.

Por exemplo:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Os resultados serão diferentes para cada instalação.

Atribua nomes amigáveis a cada um desses volumes de storage de bloco para simplificar a instalação inicial do StorageGRID e os procedimentos de manutenção futuros. Se você estiver usando o driver multipath de mapeamento de dispositivos para acesso redundante a volumes de armazenamento compartilhados, você poderá usar o `alias` campo em `/etc/multipath.conf` seu arquivo.

Por exemplo:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

Usar o campo alias dessa forma faz com que os aliases apareçam como dispositivos de bloco `/dev/mapper` no diretório do host, permitindo que você especifique um nome amigável e facilmente validado sempre que uma operação de configuração ou manutenção exigir a especificação de um volume de armazenamento de bloco.

Se você estiver configurando o armazenamento compartilhado para suportar a migração de nós do StorageGRID e usando multipathing do Mapeador de dispositivos, você poderá criar e instalar um comum `/etc/multipath.conf` em todos os hosts localizados. Apenas certifique-se de usar um volume de armazenamento diferente do mecanismo de contêiner em cada host. Usar aliases e incluir o nome de host de destino no alias para cada LUN de volume de armazenamento do mecanismo de contentor tornará isso fácil de lembrar e é recomendado.

O suporte para Docker como o mecanismo de contentor para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contentor em uma versão futura.

Informações relacionadas

"Configure o volume de armazenamento do motor do recipiente"

Configure o volume de armazenamento do motor do recipiente

Antes de instalar o mecanismo de contentor (Docker ou Podman), talvez seja necessário formatar o volume de armazenamento e montá-lo.

> O suporte para Docker como o mecanismo de contentor para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contentor em uma versão futura.

Sobre esta tarefa

Você pode ignorar essas etapas se você planeja usar o armazenamento local para o volume de armazenamento Docker ou Podman e tem espaço suficiente disponível na partição do host que contém `/var/lib/docker` para Docker e `/var/lib/containers` Podman.

> O Podman é suportado apenas no Red Hat Enterprise Linux (RHEL).

Passos

1. Crie um sistema de arquivos no volume de armazenamento do mecanismo de contentor:

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

2. Monte o volume de armazenamento do motor do recipiente:
   - Para Docker:

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

   - Para Podman:

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

3. Adicione uma entrada para container-storage-volume-volume-device ao /etc/fstab.

   Essa etapa garante que o volume de storage seja remontado automaticamente após a reinicialização do host.

Instale o Docker

O sistema StorageGRID é executado no Red Hat Enterprise Linux como uma coleção de contentores. Se você optou por usar o mecanismo de contentor Docker, siga estas etapas para instalar o Docker. Caso contrárioInstale o Podman, .

Passos

1. Instale o Docker seguindo as instruções para sua distribuição Linux.

   Se o Docker não estiver incluído na sua distribuição Linux, você poderá baixá-lo a partir do site do Docker.

2. Certifique-se de que o Docker foi ativado e iniciado executando os dois comandos a seguir:

   ```
   sudo systemctl enable docker
   ```

   ```
   sudo systemctl start docker
   ```

3. Confirme que instalou a versão esperada do Docker inserindo o seguinte:

   ```
   sudo docker version
   ```

   As versões Cliente e servidor devem ser 1.11.0 ou posterior.

Instale o Podman

O sistema StorageGRID é executado no Red Hat Enterprise Linux como uma coleção de contentores. Se você escolheu usar o motor de contentor Podman, siga estas etapas para instalar o Podman. Caso contrárioInstale o Docker, .

O Podman é suportado apenas no Red Hat Enterprise Linux (RHEL).

Passos

1. Instale o Podman e o Podman-Docker seguindo as instruções para sua distribuição Linux.

   Você também deve instalar o pacote Podman-Docker quando instalar o Podman.

2. Confirme que instalou a versão esperada do Podman e do Podman-Docker inserindo o seguinte:

   ```
   sudo docker version
   ```

   O pacote Podman-Docker permite que você use comandos Docker.

   As versões Cliente e servidor devem ser 3.2.3 ou posterior.

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

Instalar os serviços de host do StorageGRID

Você usa o pacote RPM do StorageGRID para instalar os serviços de host do StorageGRID.

Sobre esta tarefa

Estas instruções descrevem como instalar os serviços host a partir dos pacotes RPM. Como alternativa, você pode usar os metadados do repositório DNF incluídos no arquivo de instalação para instalar os pacotes RPM remotamente. Veja as instruções do repositório DNF para o seu sistema operacional Linux.

Passos

1. Copie os pacotes RPM do StorageGRID para cada um de seus hosts ou disponibilize-os no armazenamento compartilhado.

   Por exemplo, coloque-os `/tmp` no diretório, para que você possa usar o comando exemplo na próxima etapa.

2. Faça login em cada host como root ou usando uma conta com permissão sudo e execute os seguintes comandos na ordem especificada:

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
```

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
```

> Tem de instalar primeiro o pacote de imagens e o pacote de serviço em segundo lugar.

> Se você colocou os pacotes em um diretório diferente `/tmp`do , modifique o comando para refletir o caminho usado.

Automatize a instalação do StorageGRID no Red Hat Enterprise Linux

Você pode automatizar a instalação do serviço de host StorageGRID e a configuração de nós de grade.

Automatizar a implantação pode ser útil em qualquer um dos seguintes casos:

- Você já usa uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef, para implantar e configurar hosts físicos ou virtuais.
- Você pretende implantar várias instâncias do StorageGRID.
- Você está implantando uma instância grande e complexa do StorageGRID.

O serviço de host StorageGRID é instalado por um pacote e conduzido por arquivos de configuração. Você pode criar os arquivos de configuração usando um destes métodos:

- "Crie os arquivos de configuração" interativamente durante uma instalação manual.
- Prepare os arquivos de configuração com antecedência (ou programaticamente) para habilitar a instalação automatizada usando estruturas de orquestração padrão, como descrito neste artigo.

  O StorageGRID fornece scripts Python opcionais para automatizar a configuração de dispositivos StorageGRID e todo o sistema StorageGRID (a "grade"). Você pode usar esses scripts diretamente ou inspecioná-los para aprender a usar as "API REST de instalação do StorageGRID"ferramentas de implantação e configuração da grade que você mesmo desenvolve.

Automatize a instalação e a configuração do serviço de host StorageGRID

É possível automatizar a instalação do serviço de host StorageGRID usando estruturas de orquestração padrão, como Ansible, Puppet, Chef, Fabric ou SaltStack.

O serviço de host do StorageGRID é empacotado em RPM e é conduzido por arquivos de configuração que podem ser preparados com antecedência (ou programaticamente) para habilitar a instalação automatizada. Se você já usa uma estrutura de orquestração padrão para instalar e configurar o RHEL, adicionar StorageGRID aos seus playbooks ou receitas deve ser simples.

Veja o exemplo de função e manual do Ansible `/extras` na pasta fornecida com o arquivo de instalação. O manual de estratégia do Ansible mostra como a `storagegrid` função prepara o host e instala o StorageGRID nos servidores de destino. Você pode personalizar a função ou o manual de estratégia conforme necessário.

> O manual de estratégia de exemplo não inclui as etapas necessárias para criar dispositivos de rede antes de iniciar o serviço de host StorageGRID. Adicione estas etapas antes de finalizar e usar o manual de estratégia.

Você pode automatizar todas as etapas para preparar os hosts e implantar nós de grade virtual.

Exemplo de função e manual de estratégia do Ansible

Exemplo de função do Ansible e manual de estratégia são fornecidos com o arquivo de instalação `/extras` na pasta. O manual de estratégia do Ansible mostra como a `storagegrid` função prepara os hosts e instala o StorageGRID nos servidores de destino. Você pode personalizar a função ou o manual de estratégia conforme necessário.

As tarefas de instalação no exemplo de função fornecido `storagegrid` usam o `ansible.builtin.dnf` módulo para executar a instalação a partir dos arquivos RPM locais ou de um repositório Yum remoto. Se o módulo não estiver disponível ou não for compatível, talvez seja necessário editar as tarefas apropriadas do Ansible nos arquivos a seguir para usar o `yum` módulo ou `ansible.builtin.yum`:

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`

- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Automatize a configuração do StorageGRID

Depois de implantar os nós de grade, você pode automatizar a configuração do sistema StorageGRID.

Antes de começar

- Você sabe a localização dos seguintes arquivos do arquivo de instalação.

Nome do ficheiro	Descrição
configure-StorageGRID.py	Script Python usado para automatizar a configuração
configure-StorageGRID.sample.json	Exemplo de arquivo de configuração para uso com o script
configure-StorageGRID.blank.json	Arquivo de configuração em branco para uso com o script

- Criou um `configure-storagegrid.json` ficheiro de configuração. Para criar este ficheiro, pode modificar o ficheiro de configuração de exemplo (`configure-storagegrid.sample.json`) ou o ficheiro de configuração em branco (`configure-storagegrid.blank.json`).

Sobre esta tarefa

Você pode usar o `configure-storagegrid.py` script Python e o `configure-storagegrid.json` arquivo de configuração para automatizar a configuração do seu sistema StorageGRID.

> Você também pode configurar o sistema usando o Gerenciador de Grade ou a API de Instalação.

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Mude para o diretório onde você extraiu o arquivo de instalação.

   Por exemplo:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   ```
   `platform`onde está `debs`, `rpms`, `vsphere` ou .
   ```

3. Execute o script Python e use o arquivo de configuração que você criou.

   Por exemplo:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Resultado

Um arquivo do Pacote de recuperação `.zip` é gerado durante o processo de configuração e é baixado para o diretório onde você está executando o processo de instalação e configuração. Você deve fazer backup do arquivo do pacote de recuperação para que você possa recuperar o sistema StorageGRID se um ou mais nós de grade falhar. Por exemplo, copie-o para um local de rede seguro e de backup e para um local seguro de armazenamento em nuvem.

> 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.

Se você especificou que senhas aleatórias serão geradas, abra o `Passwords.txt` arquivo e procure as senhas necessárias para acessar seu sistema StorageGRID.

```
###################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip           #####
#####   Safeguard this file as it will be needed in case of a     #####
#####                 StorageGRID node recovery.                  #####
###################################################################
```

O sistema StorageGRID é instalado e configurado quando é apresentada uma mensagem de confirmação.

```
StorageGRID has been configured and installed.
```

Informações relacionadas

"API REST de instalação"

Implantar nós de grade virtual (Red Hat)

Crie arquivos de configuração de nós para implantações do Red Hat Enterprise Linux

Os arquivos de configuração de nó são pequenos arquivos de texto que fornecem as informações que o serviço de host do StorageGRID precisa para iniciar um nó e conectá-lo à rede apropriada e bloquear recursos de armazenamento. Os arquivos de configuração de nós são usados para nós virtuais e não são usados para nós do dispositivo.

Local para arquivos de configuração de nó

Coloque o arquivo de configuração para cada nó do StorageGRID `/etc/storagegrid/nodes` no diretório no host onde o nó será executado. Por exemplo, se você planeja executar um nó de administrador, um nó de gateway e um nó de armazenamento no HostA, você deve colocar três arquivos de configuração de nó no `/etc/storagegrid/nodes` HostA.

Você pode criar os arquivos de configuração diretamente em cada host usando um editor de texto, como vim ou nano, ou você pode criá-los em outro lugar e movê-los para cada host.

Nomenclatura de arquivos de configuração de nó

Os nomes dos arquivos de configuração são significativos. O formato é `node-name.conf`, onde `node-name` é um nome atribuído ao nó. Esse nome aparece no Instalador do StorageGRID e é usado para operações de manutenção de nós, como a migração de nós.

Os nomes dos nós devem seguir estas regras:

- Deve ser único
- Deve começar com uma letra
- Pode conter os carateres De A a Z e de a a z
- Pode conter os números de 0 a 9
- Pode conter um ou mais hífens (-)
- Não deve ter mais de 32 carateres, não incluindo a `.conf` extensão

Quaisquer arquivos `/etc/storagegrid/nodes` que não sigam essas convenções de nomenclatura não serão analisados pelo serviço host.

Se você tiver uma topologia de vários locais planejada para sua grade, um esquema típico de nomes de nós pode ser:

```
site-nodetype-nodenumber.conf
```

Por exemplo, você pode usar `dc1-adm1.conf` para o primeiro nó de administrador no data center 1 e `dc2-sn3.conf` para o terceiro nó de storage no data center 2. No entanto, você pode usar qualquer esquema que desejar, desde que todos os nomes de nós sigam as regras de nomenclatura.

Conteúdo de um arquivo de configuração de nó

Um arquivo de configuração contém pares chave/valor, com uma chave e um valor por linha. Para cada par chave/valor, siga estas regras:

- A chave e o valor devem ser separados por um sinal igual (=) e espaço em branco opcional.
- As teclas não podem conter espaços.
- Os valores podem conter espaços incorporados.
- Qualquer espaço em branco à frente ou à direita é ignorado.

A tabela a seguir define os valores para todas as chaves suportadas. Cada chave tem uma das seguintes designações:

- **Obrigatório**: Necessário para cada nó ou para os tipos de nó especificados
- **Melhor prática**: Opcional, embora recomendado
- **Opcional**: Opcional para todos os nós

Teclas de rede Admin

ADMIN_IP

Valor	Designação
Rede de grade IPv4 endereço do nó de administração principal para a grade à qual esse nó pertence. Use o mesmo valor que você especificou para GRID_NETWORK_IP para o nó de grade com NODE_TYPE e ADMIN_ROLE. Se você omitir esse parâmetro, o nó tentará descobrir um nó Admin primário usando mDNS. "Como os nós de grade descobrem o nó de administração principal" **Nota**: Este valor é ignorado, e pode ser proibido, no nó Admin principal.	Prática recomendada

ADMIN_NETWORK_CONFIG

Valor	Designação
DHCP, ESTÁTICO OU DESATIVADO	Opcional

ADMIN_NETWORK_ESL

Valor	Designação
Lista de sub-redes separadas por vírgulas na notação CIDR à qual esse nó deve se comunicar usando o gateway de rede Admin. Exemplo: `172.16.0.0/21,172.17.0.0/21`	Opcional

ADMIN_NETWORK_GATEWAY

Valor	Designação

Endereço IPv4 do gateway de rede de administração local para este nó. Deve estar na sub-rede definida por ADMIN_network_IP e ADMIN_network_MASK. Este valor é ignorado para redes configuradas por DHCP.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Obrigatório se `ADMIN_NETWORK_ESL` for especificado. Opcional caso contrário.

ADMIN_NETWORK_IP

Valor	Designação

Endereço IPv4 deste nó na rede Admin. Esta chave só é necessária quando ADMIN_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessário quando ADMIN_NETWORK_CONFIG é ESTÁTICO.
	
	Opcional caso contrário.

ADMIN_NETWORK_MAC

Valor	Designação
O endereço MAC da interface de rede de administração no contentor. Este campo é opcional. Se omitido, um endereço MAC será gerado automaticamente. Deve ser 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: `b2:9c:02:c2:27:10`	Opcional

ADMIN_NETWORK_MASK

Valor	Designação

IPv4 máscara de rede para este nó, na rede Admin. Especifique esta chave quando ADMIN_NETWORK_CONFIG estiver ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessário se Admin_network_IP for especificado e ADMIN_network_CONFIG for ESTÁTICO.
	
	Opcional caso contrário.

ADMIN_NETWORK_MTU

Valor	Designação

A unidade de transmissão máxima (MTU) para este nó na rede Admin. Não especifique se ADMIN_NETWORK_CONFIG é DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 é usado.
 	
Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão.
 	
IMPORTANTE: O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.
 	
Exemplos:
 	
`1500`
 	
`8192`
	Opcional

ADMIN_NETWORK_TARGET

Valor	Designação

Nome do dispositivo host que você usará para acesso à rede de administração pelo nó StorageGRID. Apenas são suportados nomes de interface de rede. Normalmente, você usa um nome de interface diferente do que foi especificado para GRID_NETWORK_TARGET ou CLIENT_network_TARGET.
 	
Nota: Não use dispositivos bond ou bridge como destino de rede. Configure uma VLAN (ou outra interface virtual) em cima do dispositivo de ligação ou use um par bridge e Ethernet virtual (vete).
 	
Prática recomendada:Especifique um valor mesmo que este nó não tenha inicialmente um endereço IP de rede Admin. Em seguida, você pode adicionar um endereço IP de rede Admin mais tarde, sem ter que reconfigurar o nó no host.
 	
Exemplos:
 	
`bond0.1002`
 	
`ens256`
	Prática recomendada

ADMIN_NETWORK_TARGET_TYPE

Valor	Designação
Interface (este é o único valor suportado.)	Opcional

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou Falso Defina a chave como "true" para fazer com que o contentor StorageGRID use o endereço MAC da interface de destino do host na rede de administração. **Prática recomendada:** em redes onde o modo promíscuo seria necessário, use a chave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC em vez disso. Para obter mais detalhes sobre clonagem MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Prática recomendada

ADMIN_ROLE

Valor	Designação
Primário ou não primário Esta chave só é necessária quando NODE_TYPE: VM_Admin_Node; não a especifique para outros tipos de nó.	Obrigatório quando NODE_TYPE é VM_Admin_Node Opcional caso contrário.

Bloquear chaves de dispositivo

BLOCK_DEVICE_AUDIT_LOGS

Valor	Designação

Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento persistente de logs de auditoria.
 	
Exemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	Necessário para nós com NODE_TYPE: VM_Admin_Node. Não o especifique para outros tipos de nó.

BLOCK_DEVICE_RANGEDB_NNN

Valor	Designação

Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento de objetos persistente. Esta chave é necessária apenas para nós com NODE_TYPE: VM_Storage_Node; não a especifique para outros tipos de nó.
 	
Somente block_DEVICE_RANGEDB_000 é necessário; o resto é opcional. O dispositivo de bloco especificado para block_DEVICE_RANGEDB_000 deve ter pelo menos 4 TB; os outros podem ser menores.
 	
Não deixe lacunas. Se você especificar block_DEVICE_RANGEDB_005, você também deve especificar BLOCK_DEVICE_RANGEDB_004.
 	
Nota: Para compatibilidade com implantações existentes, chaves de dois dígitos são suportadas para nós atualizados.
 	
Exemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	Obrigatório:
	
	BLOCK_DEVICE_RANGEDB_000
	
	Opcional:
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

BLOCK_DEVICE_TABLES

Valor	Designação

Caminho e nome do arquivo especial do dispositivo de bloco este nó usará para armazenamento persistente de tabelas de banco de dados. Esta chave é necessária apenas para nós com NODE_TYPE: VM_Admin_Node; não a especifique para outros tipos de nó.
 	
Exemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	Obrigatório

BLOCK_DEVICE_VAR_LOCAL

Valor	Designação

Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para seu `/var/local` armazenamento persistente.
 	
Exemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	Obrigatório

Chaves da rede do cliente

CLIENT_NETWORK_CONFIG

Valor	Designação
DHCP, ESTÁTICO OU DESATIVADO	Opcional

CLIENT_NETWORK_GATEWAY

Valor	Designação

Endereço IPv4 do gateway de rede de cliente local para este nó, que deve estar na sub-rede definida por CLIENT_network_IP e CLIENT_network_MASK. Este valor é ignorado para redes configuradas por DHCP.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Opcional

CLIENT_NETWORK_IP

Valor	Designação

Endereço IPv4 deste nó na rede do cliente.
 	
Esta chave só é necessária quando CLIENT_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessário quando CLIENT_NETWORK_CONFIG é ESTÁTICO
	
	Opcional caso contrário.

CLIENT_NETWORK_MAC

Valor	Designação
O endereço MAC da interface de rede do cliente no contentor. Este campo é opcional. Se omitido, um endereço MAC será gerado automaticamente. Deve ser 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: `b2:9c:02:c2:27:20`	Opcional

CLIENT_NETWORK_MASK

Valor	Designação

IPv4 máscara de rede para este nó na rede do cliente.
 	
Especifique esta chave quando CLIENT_NETWORK_CONFIG for STATIC; não a especifique para outros valores.
 	
Exemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessário se CLIENT_network_IP for especificado e CLIENT_network_CONFIG for ESTÁTICO
	
	Opcional caso contrário.

CLIENT_NETWORK_MTU

Valor	Designação

A unidade de transmissão máxima (MTU) para este nó na rede do cliente. Não especifique se CLIENT_NETWORK_CONFIG é DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 é usado.
 	
Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão.
 	
IMPORTANTE: O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.
 	
Exemplos:
 	
`1500`
 	
`8192`
	Opcional

CLIENT_NETWORK_TARGET

Valor	Designação

Nome do dispositivo host que você usará para acesso à rede do cliente pelo nó StorageGRID. Apenas são suportados nomes de interface de rede. Normalmente, você usa um nome de interface diferente do que foi especificado para GRID_Network_TARGET ou ADMIN_network_TARGET.
 	
Nota: Não use dispositivos bond ou bridge como destino de rede. Configure uma VLAN (ou outra interface virtual) em cima do dispositivo de ligação ou use um par bridge e Ethernet virtual (vete).
 	
Prática recomendada: Especifique um valor mesmo que este nó não tenha inicialmente um endereço IP de rede do cliente. Em seguida, você pode adicionar um endereço IP da rede do cliente mais tarde, sem ter que reconfigurar o nó no host.
 	
Exemplos:
 	
`bond0.1003`
 	
`ens423`
	Prática recomendada

CLIENT_NETWORK_TARGET_TYPE

Valor	Designação
Interface (este é apenas o valor suportado.)	Opcional

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou Falso Defina a chave como "true" para fazer com que o contentor StorageGRID use o endereço MAC da interface de destino do host na rede do cliente. **Melhor prática:** em redes onde o modo promíscuo seria necessário, use a chave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC em vez disso. Para obter mais detalhes sobre clonagem MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Prática recomendada

Chaves de rede de grade

GRID_NETWORK_CONFIG

Valor	Designação
ESTÁTICO ou DHCP O padrão é ESTÁTICO se não for especificado.	Prática recomendada

GRID_NETWORK_GATEWAY

Valor	Designação
Endereço IPv4 do gateway de rede local para este nó, que deve estar na sub-rede definida por GRID_Network_IP e GRID_NETWORK_MASK. Este valor é ignorado para redes configuradas por DHCP. Se a rede de Grade for uma única sub-rede sem gateway, use o endereço de gateway padrão para a sub-rede (X.Y.z.1) ou o valor GRID_Network_IP deste nó; qualquer valor simplificará expansões futuras de rede de Grade.	Obrigatório

GRID_NETWORK_IP

Valor	Designação

Endereço IPv4 deste nó na rede de Grade. Esta chave só é necessária quando GRID_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessário quando GRID_NETWORK_CONFIG é ESTÁTICO
	
	Opcional caso contrário.

GRID_NETWORK_MAC

Valor	Designação
O endereço MAC da interface Grid Network no contentor. Deve ser 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: `b2:9c:02:c2:27:30`	Opcional Se omitido, um endereço MAC será gerado automaticamente.

GRID_NETWORK_MASK

Valor	Designação

IPv4 máscara de rede para este nó na rede de Grade. Especifique esta chave quando GRID_NETWORK_CONFIG estiver ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessário quando GRID_Network_IP é especificado e GRID_NETWORK_CONFIG é ESTÁTICO.
	
	Opcional caso contrário.

GRID_NETWORK_MTU

Valor	Designação

A unidade de transmissão máxima (MTU) para este nó na rede de Grade. Não especifique se GRID_NETWORK_CONFIG é DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 é usado.
 	
Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão.
 	
IMPORTANTE: O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.
 	
IMPORTANTE: Para obter o melhor desempenho da rede, todos os nós devem ser configurados com valores MTU semelhantes em suas interfaces Grid Network. 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.
 	
Exemplos:
 	
`1500`
 	
`8192`
	Opcional

GRID_NETWORK_TARGET

Valor	Designação

Nome do dispositivo host que você usará para acesso à rede de Grade pelo nó StorageGRID. Apenas são suportados nomes de interface de rede. Normalmente, você usa um nome de interface diferente do que foi especificado para ADMIN_NETWORK_TARGET ou CLIENT_network_TARGET.
 	
Nota: Não use dispositivos bond ou bridge como destino de rede. Configure uma VLAN (ou outra interface virtual) em cima do dispositivo de ligação ou use um par bridge e Ethernet virtual (vete).
 	
Exemplos:
 	
`bond0.1001`
 	
`ens192`
	Obrigatório

GRID_NETWORK_TARGET_TYPE

Valor	Designação
Interface (este é o único valor suportado.)	Opcional

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou Falso Defina o valor da chave como "true" para fazer com que o contentor StorageGRID use o endereço MAC da interface de destino do host na rede de Grade. **Melhor prática:** em redes onde o modo promíscuo seria necessário, use a chave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC em vez disso. Para obter mais detalhes sobre clonagem MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Prática recomendada

Chave de senha de instalação (temporária)

CUSTOM_TEMPORARY_PASSWORD_HASH

Valor	Designação
Para o nó de administração principal, defina uma senha temporária padrão para a API de instalação do StorageGRID durante a instalação. **Nota**: Defina uma senha de instalação somente no nó Admin principal. Se você tentar definir uma senha em outro tipo de nó, a validação do arquivo de configuração do nó falhará. Definir este valor não tem efeito quando a instalação estiver concluída. Se esta chave for omitida, por padrão nenhuma senha temporária será definida. Como alternativa, você pode definir uma senha temporária usando a API de instalação do StorageGRID. Deve ser um `crypt()` hash de senha SHA-512 com formato `$6$<salt>$<password hash>` para uma senha de pelo menos 8 e não mais de 32 carateres. Esse hash pode ser gerado usando ferramentas CLI, como o `openssl passwd` comando no modo SHA-512.	Prática recomendada

Chave de interfaces

Interface_TARGET_nnnn

Valor	Designação
Nome e descrição opcional para uma interface extra que você deseja adicionar a este nó. Você pode adicionar várias interfaces extras a cada nó. Para *nnnnn*, especifique um número exclusivo para cada entrada INTERFACE_TARGET que você está adicionando. Para o valor, 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. Exemplo: `INTERFACE_TARGET_0001=ens256, Trunk` 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.	Opcional

Tecla RAM máxima

MÁXIMO_RAM

Valor	Designação

A quantidade máxima de RAM que este nó pode consumir. Se esta chave for omitida, o nó não tem restrições de memória. Ao definir este campo para um nó de nível de produção, especifique um valor que seja pelo menos 24 GB e 16 a 32 GB menor que a RAM total do sistema.
 	
Nota: O valor da RAM afeta o espaço reservado de metadados real de um nó. Consulte "Descrição do que é Metadata Reserved Space".
 	
O formato deste campo é *`numberunit`*, onde *`unit`* pode ser `b`, `k`, , `m` `g` ou .
 	
Exemplos:
 	
`24g`
 	
`38654705664b`
 	
Nota: Se você quiser usar essa opção, você deve habilitar o suporte do kernel para cgroups de memória.
	Opcional

Chaves de tipo de nó

NODE_TYPE (TIPO DE NÓ)

Valor	Designação
Tipo de nó: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway	Obrigatório

TIPO_ARMAZENAMENTO

Valor	Designação
Define o tipo de objetos que um nó de storage contém. Para obter mais informações, "Tipos de nós de storage"consulte . Esta chave é necessária apenas para nós com NODE_TYPE: VM_Storage_Node; não a especifique para outros tipos de nó. Tipos de armazenamento: • combinado • dados • metadados **Nota**: Se o STORAGE_TYPE não for especificado, o tipo Storage Node é definido como combinado (dados e metadados) por padrão.	Opcional

Teclas de remapeamento de portas

PORT_REMAP

Valor	Designação
Remapeia qualquer porta usada por um nó para comunicações internas de nó de grade ou comunicações externas. O remapeamento de portas é necessário se as políticas de rede empresarial restringirem uma ou mais portas usadas pelo StorageGRID, conforme descrito em "Comunicações internas do nó da grade" ou "Comunicações externas". **IMPORTANTE**: Não remapegue as portas que você está planejando usar para configurar pontos de extremidade do balanceador de carga. **Nota**: Se apenas PORT_REMAP estiver definido, o mapeamento especificado será usado para comunicações de entrada e saída. Se Port_REMAP_INBOUND também for especificado, PORT_REMAP se aplica apenas às comunicações de saída. O formato usado é: *`network type/protocol/default port used by grid node/new port`*, Onde *`network type`* está grade, admin ou cliente e *`protocol`* é tcp ou udp. Exemplo: `PORT_REMAP = client/tcp/18082/443` Você também pode remapear várias portas usando uma lista separada por vírgulas. Exemplo: `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	Opcional

PORT_REMAP_INBOUND

Valor	Designação
Remapeia as comunicações de entrada para a porta especificada. Se você especificar PORT_REMAP_INBOUND, mas não especificar um valor para PORT_REMAP, as comunicações de saída para a porta não serão alteradas. **IMPORTANTE**: Não remapegue as portas que você está planejando usar para configurar pontos de extremidade do balanceador de carga. O formato usado é: *`network type/protocol/remapped port /default port used by grid node`*, Onde *`network type`* está grade, admin ou cliente e *`protocol`* é tcp ou udp. Exemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22` Você também pode remapear várias portas de entrada usando uma lista separada por vírgulas. Exemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	Opcional

Como os nós de grade descobrem o nó de administração principal

Os nós de grade se comunicam com o nó de administração principal para configuração e gerenciamento. Cada nó de grade deve saber o endereço IP do nó de administração principal na rede de grade.

Para garantir que um nó de grade possa acessar o nó Admin principal, você pode fazer um dos seguintes procedimentos ao implantar o nó:

- Você pode usar o parâmetro Admin_IP para inserir o endereço IP do nó de administrador principal manualmente.
- Você pode omitir o parâmetro ADMIN_IP para que o nó de grade descubra o valor automaticamente. A deteção automática é especialmente útil quando a rede de Grade usa DHCP para atribuir o endereço IP ao nó Admin principal.

A deteção automática do nó de administração principal é realizada usando um sistema de nome de domínio multicast (mDNS). Quando o nó de administração principal é iniciado pela primeira vez, ele publica seu endereço IP usando mDNS. Outros nós na mesma sub-rede podem então consultar o endereço IP e adquiri-lo automaticamente. No entanto, como o tráfego IP multicast não é normalmente roteável entre sub-redes, os nós em outras sub-redes não podem adquirir o endereço IP do nó de administração principal diretamente.

Se utilizar a deteção automática:

- Você deve incluir a configuração Admin_IP para pelo menos um nó de grade em todas as sub-redes às quais o nó Admin principal não esteja diretamente conetado. Esse nó de grade publicará o endereço IP do nó de administrador principal para outros nós na sub-rede para serem detetados com mDNS.
- Certifique-se de que a sua infra-estrutura de rede suporta a passagem de tráfego IP multi-cast dentro de uma sub-rede.

Exemplo de arquivos de configuração de nó

Você pode usar os arquivos de configuração de nó de exemplo para ajudar a configurar os arquivos de configuração de nó para o seu sistema StorageGRID. Os exemplos mostram arquivos de configuração de nós para todos os tipos de nós de grade.

Para a maioria dos nós, você pode adicionar informações de endereçamento de rede de administrador e cliente (IP, máscara, gateway, etc.) ao configurar a grade usando o Gerenciador de Grade ou a API de instalação. A exceção é o nó de administração principal. Se você quiser navegar até o IP de rede Admin do nó de administração principal para concluir a configuração da grade (porque a rede de grade não está roteada, por exemplo), você deve configurar a conexão de rede Admin para o nó de administração principal em seu arquivo de configuração de nó. Isso é mostrado no exemplo.

Nos exemplos, o destino rede cliente foi configurado como uma prática recomendada, mesmo que a rede cliente esteja desativada por padrão.

Exemplo para nó de administração principal

- Exemplo de nome de arquivo*: `/etc/storagegrid/nodes/dc1-adm1.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Exemplo para nó de storage

- Exemplo de nome do arquivo:* `/etc/storagegrid/nodes/dc1-sn1.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-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
```

Exemplo para Gateway Node

- Exemplo de nome do arquivo:* `/etc/storagegrid/nodes/dc1-gw1.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemplo para um nó de administração não primário

- Exemplo de nome do arquivo:* `/etc/storagegrid/nodes/dc1-adm2.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Valide a configuração do StorageGRID

Depois de criar arquivos de configuração `/etc/storagegrid/nodes` para cada um dos nós do StorageGRID, você deve validar o conteúdo desses arquivos.

Para validar o conteúdo dos arquivos de configuração, execute o seguinte comando em cada host:

```
sudo storagegrid node validate all
```

Se os arquivos estiverem corretos, a saída mostra **PASSADO** para cada arquivo de configuração, como mostrado no exemplo.

> Ao usar apenas um LUN em nós somente metadados, você pode receber uma mensagem de aviso que pode ser ignorada.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

> Para uma instalação automatizada, pode suprimir esta saída utilizando as `-q` opções ou `--quiet` do `storagegrid` comando (por exemplo, `storagegrid --quiet…`). Se você suprimir a saída, o comando terá um valor de saída não zero se quaisquer avisos de configuração ou erros foram detetados.

Se os arquivos de configuração estiverem incorretos, os problemas serão exibidos como **AVISO** e **ERRO**, conforme mostrado no exemplo. Se forem encontrados quaisquer erros de configuração, é necessário corrigi-

los antes de continuar com a instalação.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Inicie o serviço de host do 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.

Passos

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
```

3. Se qualquer nó retornar um status de "não está em execução" ou "parado", execute o seguinte comando:

```
sudo storagegrid node start node-name
```

4. 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
```

Configurar a grade e a instalação completa (Red Hat)

Navegue até o Gerenciador de Grade

Use o Gerenciador de Grade para definir todas as informações necessárias para configurar o sistema StorageGRID.

Antes de começar

O nó Admin principal deve ser implantado e ter concluído a sequência inicial de inicialização.

Passos

1. Abra o navegador da Web e navegue até:

   `https://primary_admin_node_ip`

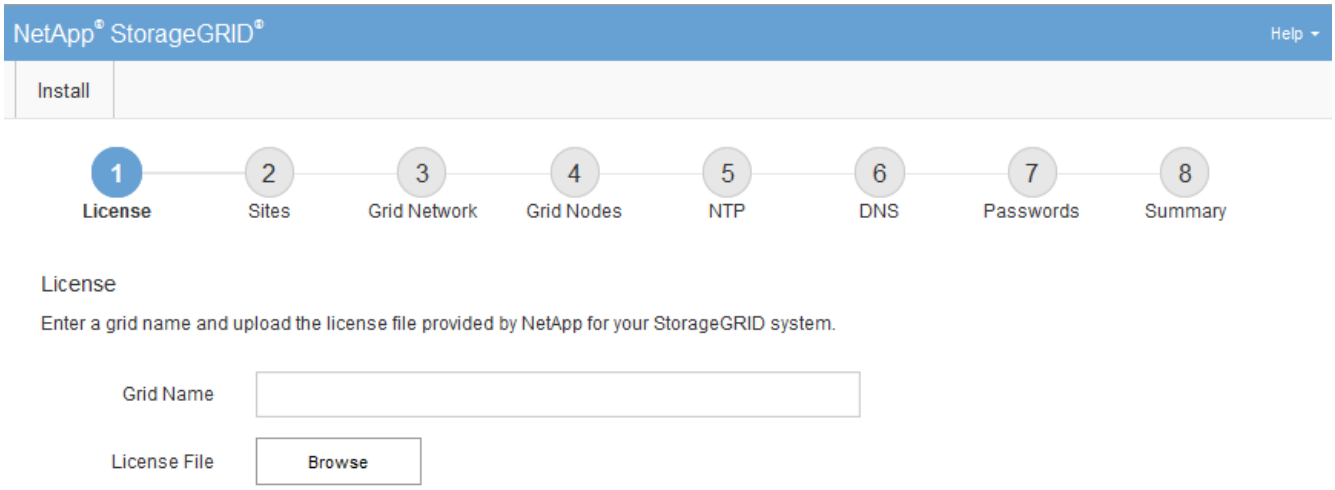
   Como alternativa, você pode acessar o Gerenciador de Grade na porta 8443:

   `https://primary_admin_node_ip:8443`

   Você pode usar o endereço IP do nó de administrador principal IP na rede de grade ou na rede de administração, conforme apropriado para a configuração da rede.

2. Gerencie uma senha temporária do instalador conforme necessário:
   - Se já tiver sido definida uma palavra-passe utilizando um destes métodos, introduza a palavra-passe para prosseguir.
     - Um usuário define a senha ao acessar o instalador anteriormente
     - A senha foi importada automaticamente do arquivo de configuração do nó em `/etc/storagegrid/nodes/<node_name>.conf`
   - Se não tiver sido definida uma palavra-passe, defina opcionalmente uma palavra-passe para proteger o instalador do StorageGRID.
3. Selecione **Instalar um sistema StorageGRID**.

É apresentada a página utilizada para configurar um sistema StorageGRID.



Especifique as informações da licença do StorageGRID

Você deve especificar o nome do seu sistema StorageGRID e fazer o upload do arquivo de licença fornecido pelo NetApp.

Passos

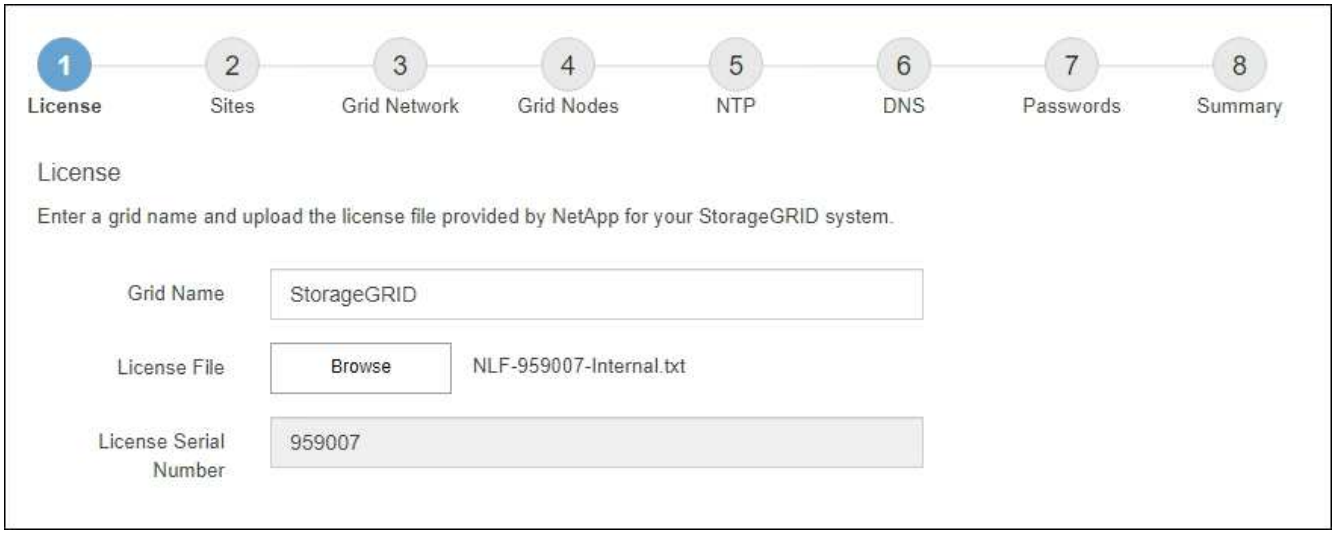
1. Na página Licença, insira um nome significativo para o seu sistema StorageGRID no campo **Nome da Grade**.

   Após a instalação, o nome é exibido na parte superior do menu nós.

2. Selecione **Procurar**, localize o ficheiro de licença NetApp (`NLF-unique-id.txt`) e selecione **abrir**.

   O ficheiro de licença é validado e o número de série é apresentado.

   > O arquivo de instalação do StorageGRID inclui uma licença gratuita que não fornece nenhum direito de suporte para o produto. Você pode atualizar para uma licença que oferece suporte após a instalação.



3. Selecione **seguinte**.

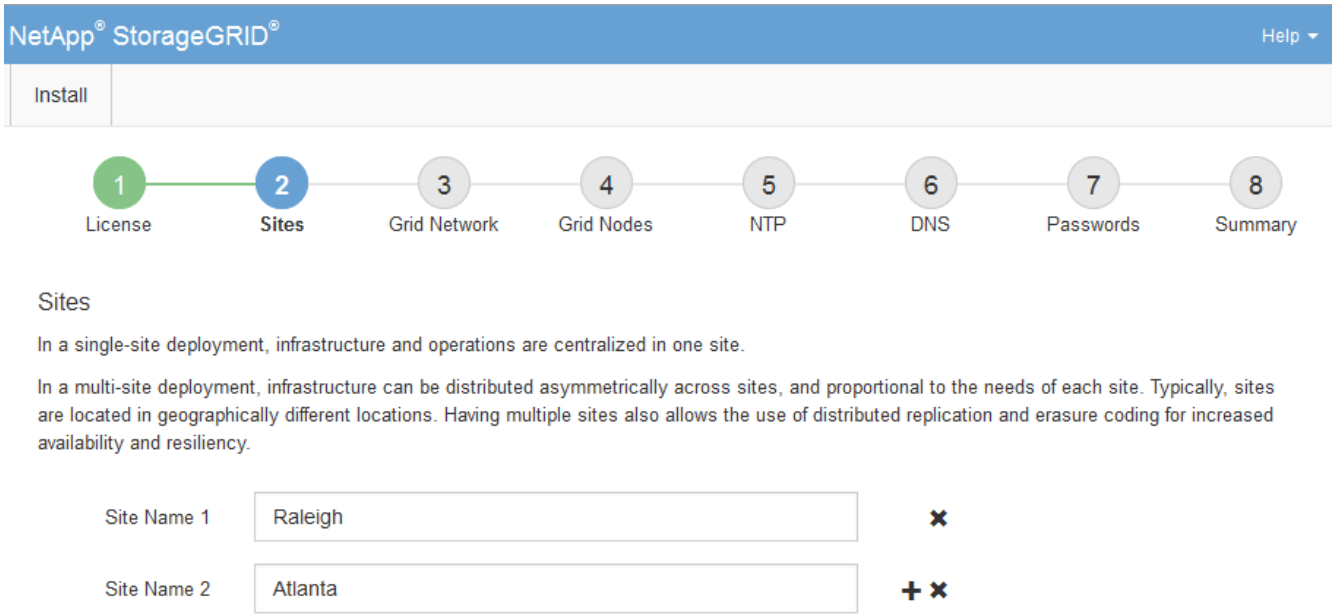
Adicione sites

Você deve criar pelo menos um site quando estiver instalando o StorageGRID. Você pode criar sites adicionais para aumentar a confiabilidade e a capacidade de storage do seu sistema StorageGRID.

Passos

1. Na página Sites, insira o **Nome do Site**.
2. Para adicionar sites adicionais, clique no sinal de adição ao lado da última entrada do site e digite o nome na nova caixa de texto **Nome do site**.

   Adicione tantos locais adicionais quanto necessário para a topologia da grade. Você pode adicionar até 16 sites.



3. Clique em **seguinte**.

Especifique as sub-redes da rede de Grade

Você deve especificar as sub-redes que são usadas na rede de Grade.

Sobre esta tarefa

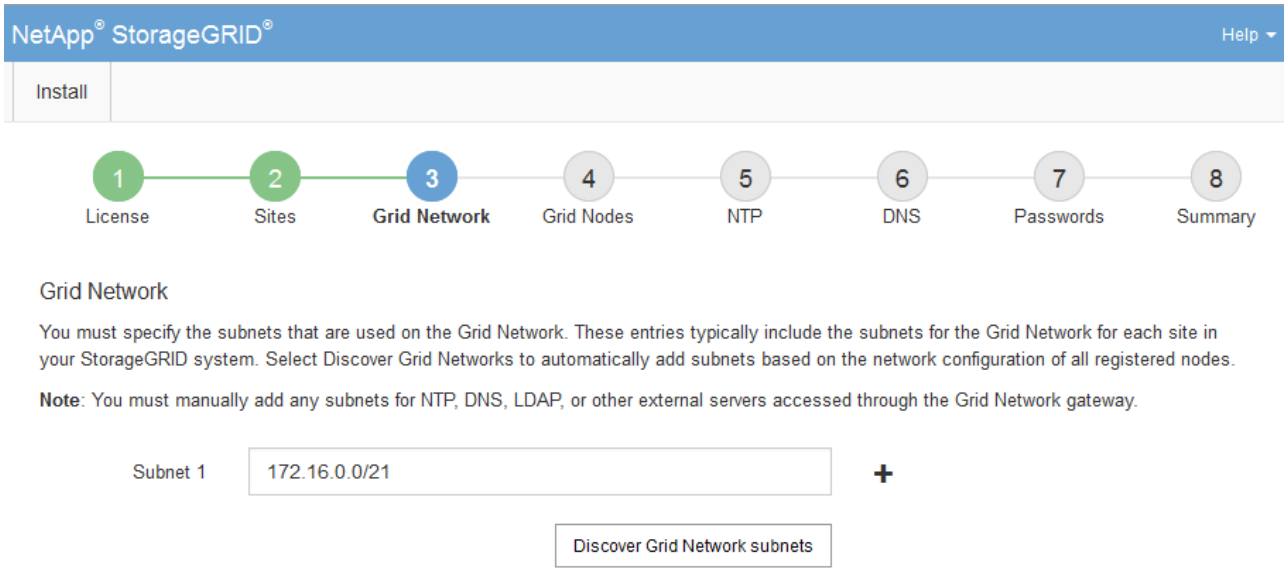
As entradas de sub-rede incluem as sub-redes para a rede de Grade para cada site no seu sistema StorageGRID, juntamente com quaisquer sub-redes que precisam ser acessíveis através da rede de Grade.

Se você tiver várias sub-redes de grade, o gateway de rede de grade é necessário. Todas as sub-redes de grade especificadas devem ser acessíveis através deste gateway.

Passos

1. Especifique o endereço de rede CIDR para pelo menos uma rede de Grade na caixa de texto **Subnet 1**.
2. Clique no sinal de mais ao lado da última entrada para adicionar uma entrada de rede adicional. Você deve especificar todas as sub-redes para todos os sites na rede de Grade.

- Se você já implantou pelo menos um nó, clique em **descobrir sub-redes de redes de Grade** para preencher automaticamente a Lista de sub-redes de rede de Grade com as sub-redes relatadas pelos nós de grade que se registraram no Gerenciador de Grade.
- Você deve adicionar manualmente quaisquer sub-redes para NTP, DNS, LDAP ou outros servidores externos acessados através do gateway de rede de Grade.



3. Clique em **seguinte**.

Aprovar nós de grade pendentes

Você deve aprovar cada nó de grade antes que ele possa ingressar no sistema StorageGRID.

Antes de começar

Você implantou todos os nós de grade de dispositivos virtuais e StorageGRID.

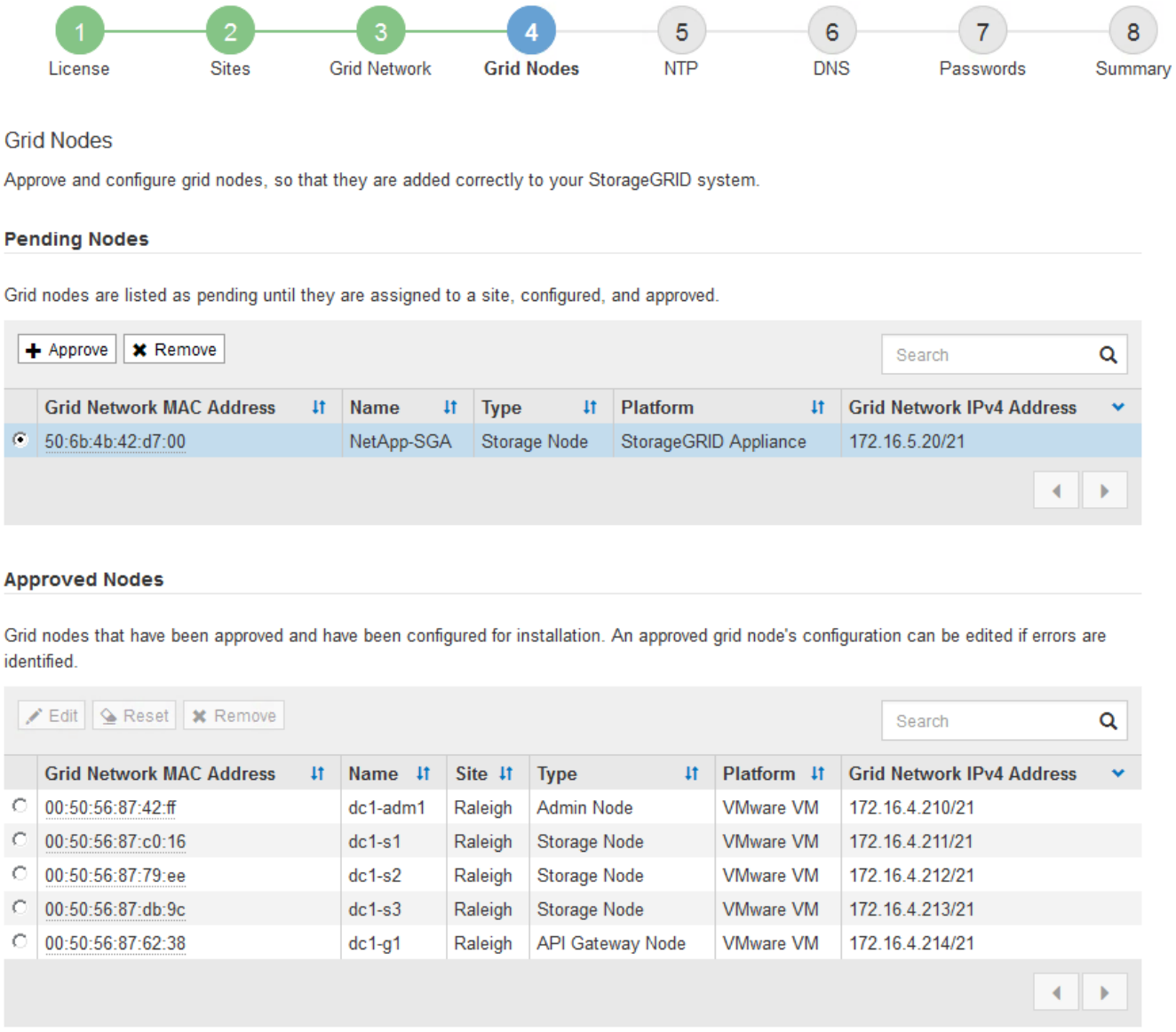
> É mais eficiente executar uma única instalação de todos os nós, em vez de instalar alguns nós agora e alguns nós depois.

Passos

1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade implantados.

> Se um nó de grade estiver ausente, confirme que ele foi implantado com sucesso e que tem o IP de rede de grade correto do nó de administrador principal definido para ADMIN_IP.

2. Selecione o botão de opção ao lado de um nó pendente que você deseja aprovar.



3. Clique em **Approve**.
4. Em Configurações gerais, modifique as configurações para as seguintes propriedades, conforme necessário:
   - **Site**: O nome do sistema do site para este nó de grade.
   - **Nome**: O nome do sistema para o nó. O nome padrão é o nome que você especificou quando configurou o nó.

     Os nomes de sistema são necessários para operações internas do StorageGRID e não podem ser alterados após a conclusão da instalação. No entanto, durante esta etapa do processo de instalação, você pode alterar os nomes do sistema conforme necessário.

     - **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.

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.

- * Tipo de armazenamento* (somente nós de armazenamento): Especifique que um novo nó de armazenamento seja usado exclusivamente para dados, somente metadados ou ambos. As opções são **dados e metadados** ("combinados"), **somente dados** e **somente metadados**.

  "Tipos de nós de storage"Consulte para obter informações sobre os requisitos para esses tipos de nós.

- **ADC Service** (somente nós de armazenamento): Selecione **Automático** para permitir que o sistema determine se o nó requer 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. Não é possível adicionar o serviço ADC a um nó depois que ele é implantado.

5. Na rede de Grade, modifique as configurações para as seguintes propriedades, conforme necessário:

   - **Endereço IPv4 (CIDR)**: O endereço de rede CIDR para a interface Grid Network (eth0 dentro do contentor). Por exemplo: 192.168.1.234/21
   - **Gateway**: O gateway Grid Network. Por exemplo: 192.168.0.1

     O gateway é necessário se houver várias sub-redes de grade.

   Se você selecionou DHCP para a configuração da rede de Grade e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

6. Se pretender configurar a rede de administração para o nó da grelha, adicione ou atualize as definições na secção rede de administração, conforme necessário.

   Insira as sub-redes de destino das rotas fora desta interface na caixa de texto **sub-redes (CIDR)**. Se houver várias sub-redes Admin, o gateway Admin é necessário.

   Se você selecionou DHCP para a configuração da rede Admin e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

   Appliances: para um appliance StorageGRID, se a rede de administração não tiver sido configurada durante a instalação inicial usando o Instalador de appliance StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

   a. Reinicie o aparelho: No Instalador de dispositivos, selecione **Avançado** > **Reiniciar**.

      A reinicialização pode levar vários minutos.

   b. Selecione **Configure Networking** > **Link Configuration** e ative as redes apropriadas.
   c. Selecione **Configurar rede** > **Configuração IP** e configure as redes ativadas.
   d. Volte à página inicial e clique em **Iniciar instalação**.

e. No Gerenciador de Grade: Se o nó estiver listado na tabela de nós aprovados, remova o nó.

f. Remova o nó da tabela nós pendentes.

g. Aguarde que o nó reapareça na lista de nós pendentes.

h. Confirme se você pode configurar as redes apropriadas. Eles já devem ser preenchidos com as informações fornecidas na página Configuração IP do Instalador de dispositivos.

   Para obter informações adicionais, consulte as instruções de instalação do modelo do seu aparelho.

7. Se pretender configurar a rede do cliente para o nó da grelha, adicione ou atualize as definições na secção rede do cliente, conforme necessário. Se a rede do cliente estiver configurada, o gateway é necessário e ele se torna o gateway padrão para o nó após a instalação.

   > Se você selecionou DHCP para a configuração da rede do cliente e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

   Appliances: para um appliance StorageGRID, se a rede cliente não tiver sido configurada durante a instalação inicial usando o Instalador de appliance StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

   a. Reinicie o aparelho: No Instalador de dispositivos, selecione **Avançado** > **Reiniciar**.

      A reinicialização pode levar vários minutos.

   b. Selecione **Configure Networking** > **Link Configuration** e ative as redes apropriadas.

   c. Selecione **Configurar rede** > **Configuração IP** e configure as redes ativadas.

   d. Volte à página inicial e clique em **Iniciar instalação**.

   e. No Gerenciador de Grade: Se o nó estiver listado na tabela de nós aprovados, remova o nó.

   f. Remova o nó da tabela nós pendentes.

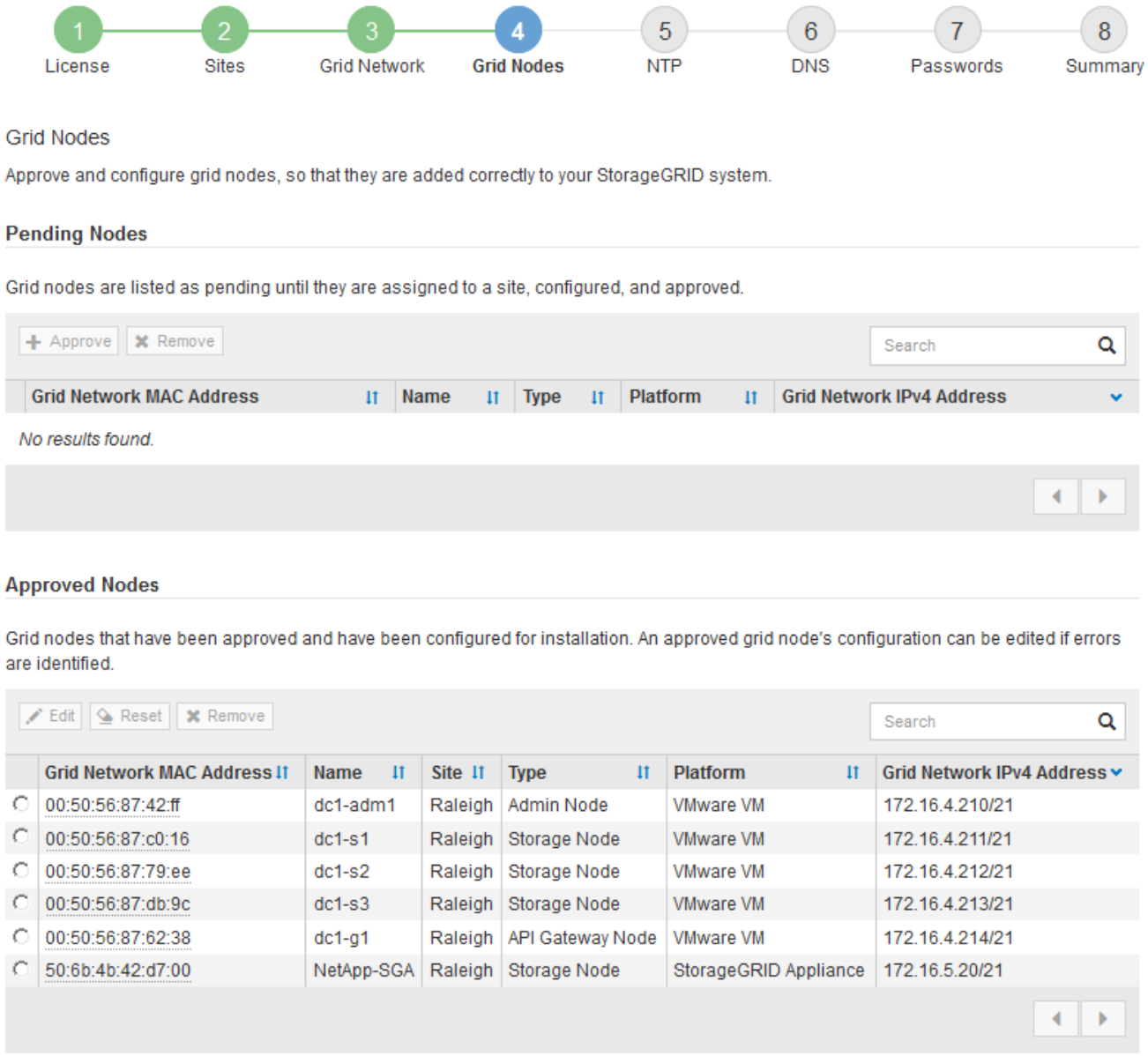
   g. Aguarde que o nó reapareça na lista de nós pendentes.

   h. Confirme se você pode configurar as redes apropriadas. Eles já devem ser preenchidos com as informações fornecidas na página Configuração IP do Instalador de dispositivos.

      Para obter informações adicionais, consulte as instruções de instalação do seu aparelho.

8. Clique em **Salvar**.

   A entrada do nó de grade se move para a lista de nós aprovados.



9. Repita estas etapas para cada nó de grade pendente que você deseja aprovar.

   Você deve aprovar todos os nós que deseja na grade. No entanto, você pode retornar a esta página a qualquer momento antes de clicar em **Instalar** na página Resumo. Você pode modificar as propriedades de um nó de grade aprovado selecionando seu botão de opção e clicando em **Editar**.

10. Quando terminar de aprovar nós de grade, clique em **Next**.

Especifique as informações do servidor Network Time Protocol

Você deve especificar as informações de configuração do protocolo de tempo de rede (NTP) para o sistema StorageGRID, para que as operações executadas em servidores separados possam ser mantidas sincronizadas.

Sobre esta tarefa

Você deve especificar endereços IPv4 para os servidores NTP.

Tem de especificar servidores NTP externos. Os servidores NTP especificados devem usar o protocolo NTP.

Você deve especificar quatro referências de servidor NTP do estrato 3 ou melhor para evitar problemas com a deriva de tempo.

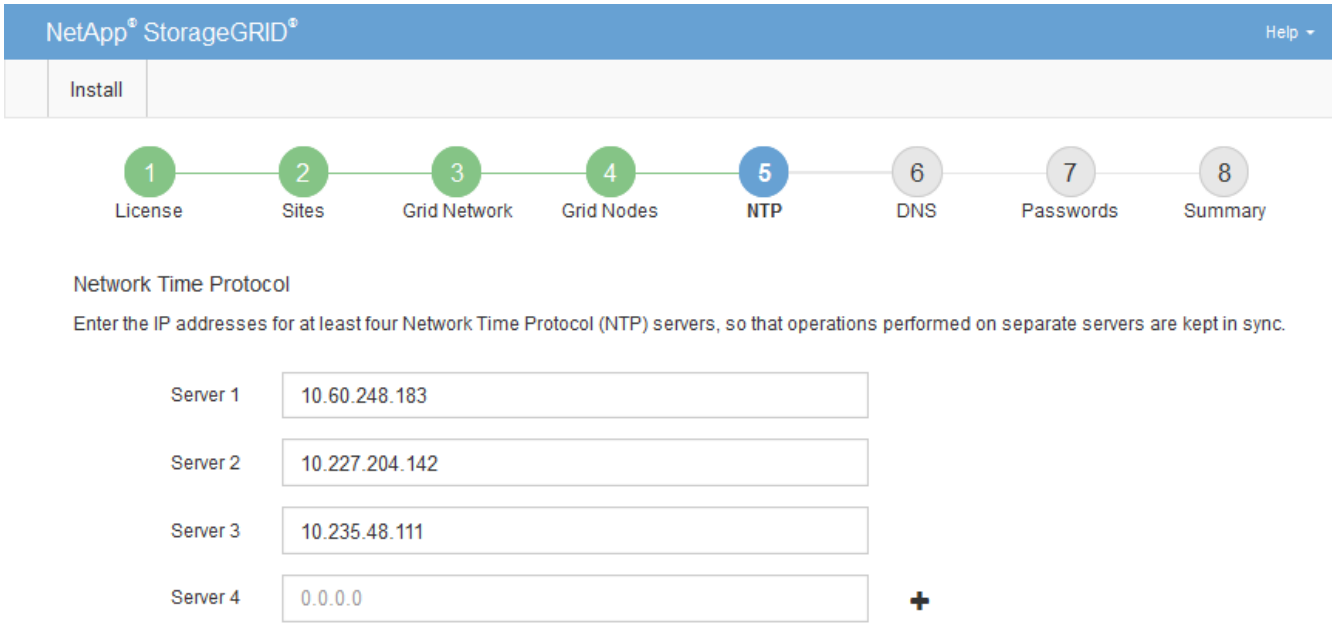
> Ao especificar a fonte NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft 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"

Os servidores NTP externos são usados pelos nós aos quais você atribuiu funções primárias NTP anteriormente.

> 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.

Passos

1. Especifique os endereços IPv4 para pelo menos quatro servidores NTP nas caixas de texto **Server 1** para **Server 4**.
2. Se necessário, selecione o sinal de adição ao lado da última entrada para adicionar entradas adicionais do servidor.



3. Selecione **seguinte**.

Especifique as informações do servidor DNS

Você deve especificar informações de DNS para seu sistema StorageGRID, para que

você possa acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

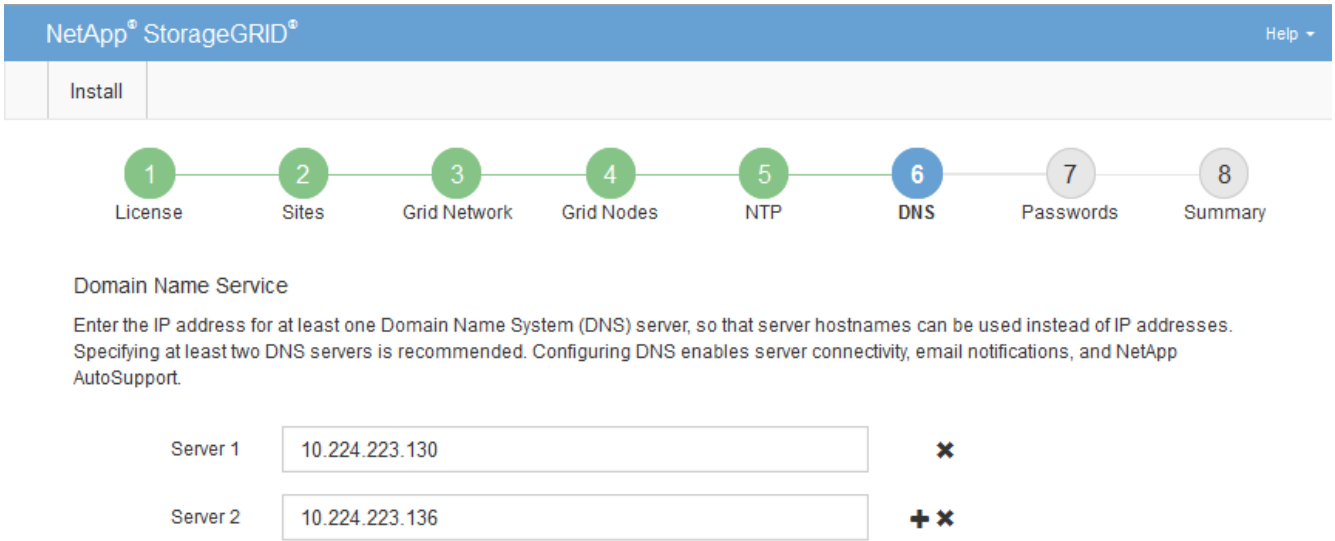
Especificar "Informações do servidor DNS" permite que você use nomes de host de nome de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações de e-mail e AutoSupport.

Para garantir o funcionamento correto, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três serão usados por causa das limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, pode "Personalize a lista de servidores DNS"usar um conjunto diferente de até três servidores DNS para nós individuais (normalmente todos os nós em um site).

Se possível, use servidores DNS que cada site pode acessar localmente para garantir que um site islanded possa resolver os FQDNs para destinos externos.

Passos

1. Especifique o endereço IPv4 para pelo menos um servidor DNS na caixa de texto **Server 1**.
2. Se necessário, selecione o sinal de adição ao lado da última entrada para adicionar entradas adicionais do servidor.



A prática recomendada é especificar pelo menos dois servidores DNS. Você pode especificar até seis servidores DNS.

3. Selecione **seguinte**.

Especifique as senhas do sistema StorageGRID

Como parte da instalação do sistema StorageGRID, você precisa inserir as senhas a serem usadas para proteger o sistema e executar tarefas de manutenção.

Sobre esta tarefa

Use a página Instalar senhas para especificar a senha de provisionamento e a senha de usuário raiz de gerenciamento de grade.

- A senha de provisionamento é usada como uma chave de criptografia e não é armazenada pelo sistema StorageGRID.

- Você deve ter a senha de provisionamento para procedimentos de instalação, expansão e manutenção, incluindo o download do Pacote de recuperação. Portanto, é importante que você armazene a senha de provisionamento em um local seguro.
- Você pode alterar a senha de provisionamento do Gerenciador de Grade se tiver a senha atual.
- A senha do usuário raiz de gerenciamento de grade pode ser alterada usando o Gerenciador de Grade.
- As senhas do console de linha de comando e SSH geradas aleatoriamente são armazenadas no `Passwords.txt` arquivo no Pacote de recuperação.

Passos

1. Em **frase-passe de aprovisionamento**, introduza a frase-passe de aprovisionamento que será necessária para efetuar alterações na topologia de grelha do seu sistema StorageGRID.

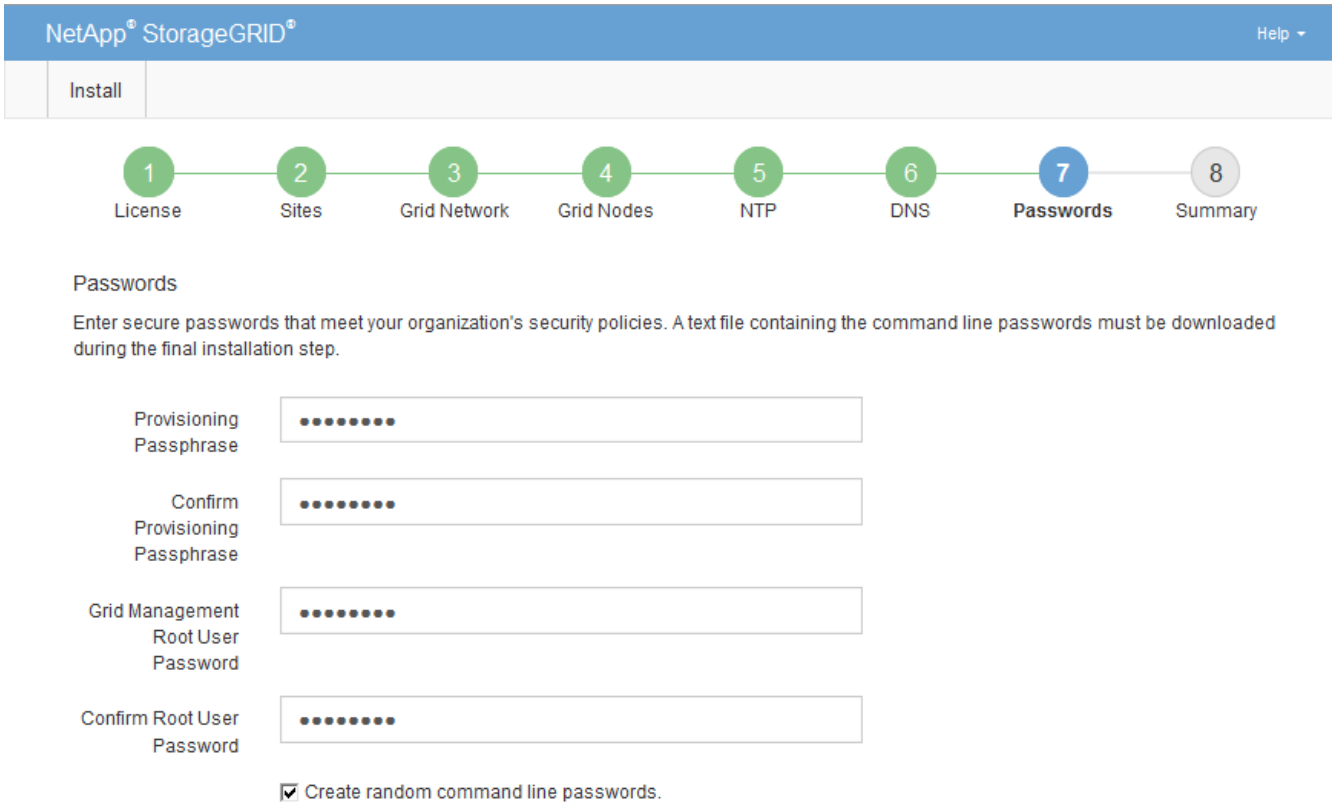
   Armazene a senha de provisionamento em um local seguro.

   > Se após a conclusão da instalação e você quiser alterar a senha de provisionamento mais tarde, você pode usar o Gerenciador de Grade. Selecione **CONFIGURATION** > **access control**> **Grid passwords**.

2. Em **Confirm Provisioning Passphrase** (confirmar frase-passe de aprovisionamento), volte a introduzir a frase-passe de aprovisionamento para a confirmar.
3. Em **Grid Management Root User Password**, insira a senha a ser usada para acessar o Grid Manager como usuário "root".

   Guarde a palavra-passe num local seguro.

4. Em **Confirm root User Password**, digite novamente a senha do Grid Manager para confirmá-la.



5. Se você estiver instalando uma grade para fins de prova de conceito ou demonstração, desmarque a caixa de seleção **criar senhas de linha de comando aleatórias**.

   Para implantações de produção, senhas aleatórias devem sempre ser usadas por razões de segurança. Limpar **criar senhas de linha de comando aleatórias** somente para grades de demonstração se você quiser usar senhas padrão para acessar nós de grade da linha de comando usando a conta "root" ou "admin".

   > Você será solicitado a baixar o arquivo do pacote de recuperação (`sgws-recovery-package-id-revision.zip`) depois de clicar em **Instalar** na página Resumo. Você deve "transfira este ficheiro"concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas `Passwords.txt` no arquivo, contido no arquivo Pacote de recuperação.

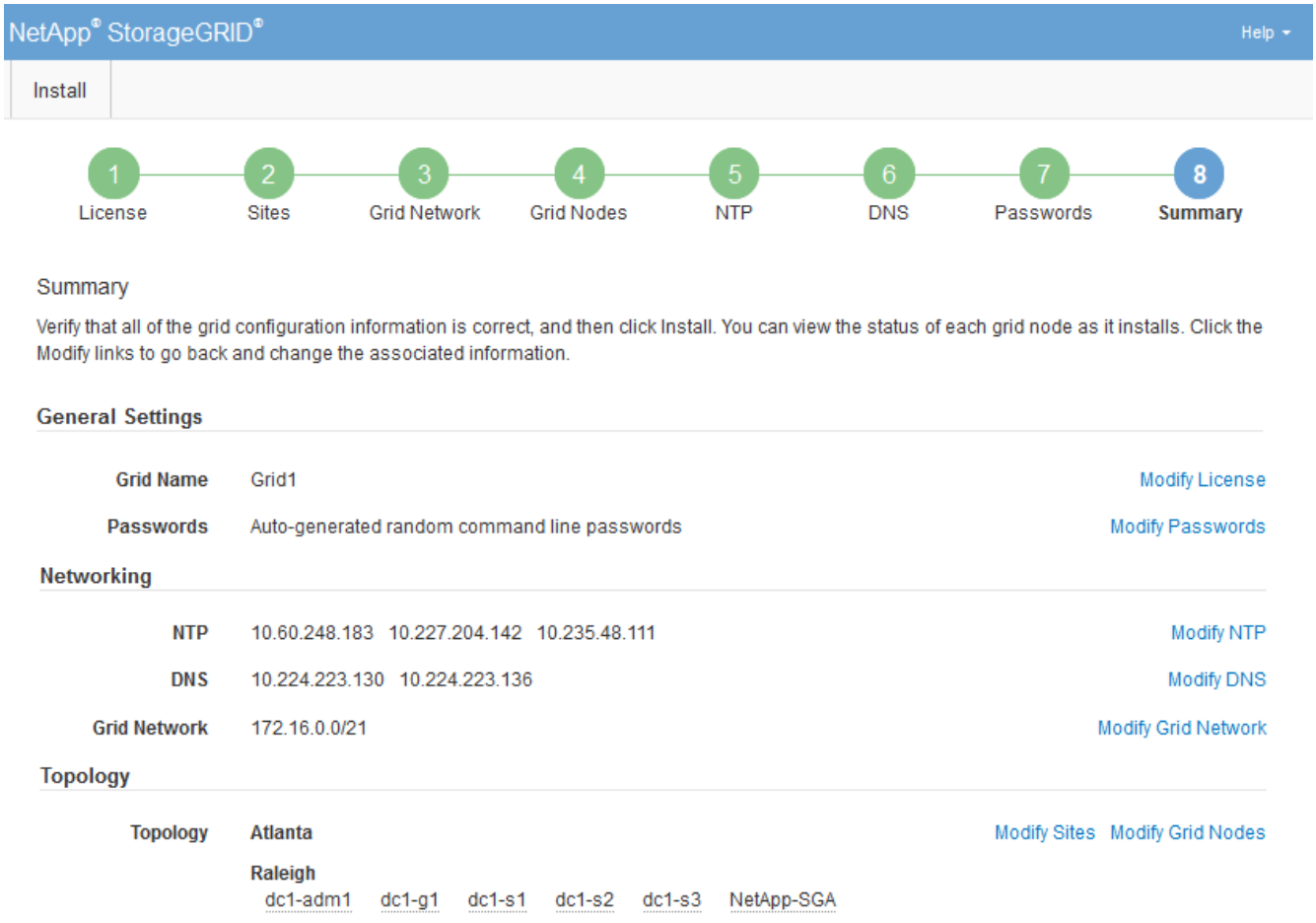
6. Clique em **seguinte**.

Revise sua configuração e conclua a instalação

Você deve analisar cuidadosamente as informações de configuração inseridas para garantir que a instalação seja concluída com êxito.

Passos

1. Veja a página **Summary**.



2. Verifique se todas as informações de configuração da grade estão corretas. Use os links Modificar na página Resumo para voltar e corrigir quaisquer erros.

3. Clique em **Instalar**.

> Se um nó estiver configurado para usar a rede do cliente, o gateway padrão para esse nó alterna da rede da grade para a rede do cliente quando você clica em **Instalar**. Se você perder a conetividade, deve garantir que está acessando o nó de administração principal por meio de uma sub-rede acessível. "Diretrizes de rede"Consulte para obter detalhes.

4. Clique em **Download Recovery Package**.

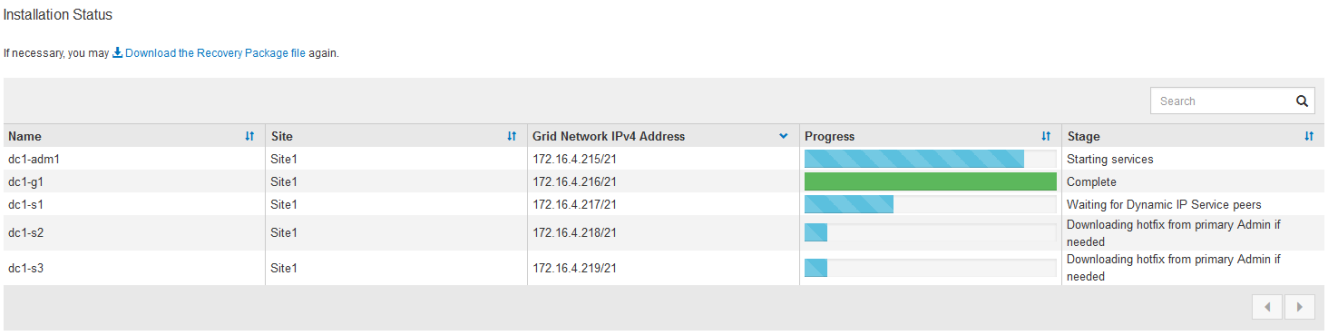
   Quando a instalação progride até o ponto em que a topologia da grade é definida, você será solicitado a baixar o arquivo do Pacote de recuperação (`.zip`) e confirmar que você pode acessar com êxito o conteúdo desse arquivo. Você deve baixar o arquivo do pacote de recuperação para que você possa recuperar o sistema StorageGRID se um ou mais nós de grade falharem. A instalação continua em segundo plano, mas você não pode concluir a instalação e acessar o sistema StorageGRID até baixar e verificar esse arquivo.

5. Verifique se você pode extrair o conteúdo do `.zip` arquivo e salvá-lo em 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.

6. Marque a caixa de seleção **Eu baixei e verifiquei com êxito o arquivo do pacote de recuperação** e clique em **Avançar**.

   Se a instalação ainda estiver em andamento, a página de status será exibida. Esta página indica o progresso da instalação para cada nó de grade.



   Quando o estágio completo é alcançado para todos os nós de grade, a página de login do Gerenciador de Grade é exibida.

7. Inicie sessão no Grid Manager utilizando o utilizador "root" e a palavra-passe especificada durante a instalação.

Diretrizes de pós-instalação

Depois de concluir a implantação e a configuração do nó de grade, siga estas diretrizes para endereçamento DHCP e alterações na configuração da rede.

- Se o DHCP foi usado para atribuir endereços IP, configure uma reserva DHCP para cada endereço IP nas redes que estão sendo usadas.

  Só pode configurar o DHCP durante a fase de implementação. Não é possível configurar o DHCP durante

a configuração.

> Os nós reiniciam quando a configuração da rede de Grade é alterada pelo DHCP, o que pode causar interrupções se uma alteração de DHCP afetar vários nós ao mesmo tempo.

- Você deve usar os procedimentos alterar IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. "Configurar endereços IP"Consulte .
- Se você fizer alterações na configuração de rede, incluindo alterações de roteamento e gateway, a conetividade do cliente para o nó de administração principal e outros nós de grade pode ser perdida. Dependendo das alterações de rede aplicadas, talvez seja necessário restabelecer essas conexões.

API REST de instalação

O StorageGRID fornece a API de instalação do StorageGRID para executar tarefas de instalação.

A API usa a plataforma de API de código aberto Swagger para fornecer a documentação da API. O Swagger permite que desenvolvedores e não desenvolvedores interajam com a API em uma interface de usuário que ilustra como a API responde a parâmetros e opções. Esta documentação pressupõe que você esteja familiarizado com as tecnologias da Web padrão e o formato de dados JSON.

> Todas as operações de API executadas usando a página da Documentação da API são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Cada comando REST API inclui o URL da API, uma ação HTTP, quaisquer parâmetros de URL necessários ou opcionais e uma resposta de API esperada.

API de instalação do StorageGRID

A API de instalação do StorageGRID só está disponível quando você estiver configurando inicialmente o sistema StorageGRID e se precisar executar uma recuperação do nó de administração principal. A API de instalação pode ser acessada por HTTPS a partir do Gerenciador de Grade.

Para acessar a documentação da API, vá para a página da Web de instalação no nó de administração principal e selecione **Ajuda** > **Documentação da API** na barra de menus.

A API de instalação do StorageGRID inclui as seguintes seções:

- **Config** — operações relacionadas à versão do produto e versões da API. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **Grid** — operações de configuração em nível de grade. Você pode obter e atualizar configurações de grade, incluindo detalhes de grade, sub-redes de rede de grade, senhas de grade e endereços IP de servidor NTP e DNS.
- **Nodes** — operações de configuração em nível de nó. Você pode recuperar uma lista de nós de grade, excluir um nó de grade, configurar um nó de grade, exibir um nó de grade e redefinir a configuração de um nó de grade.
- **Provisão** — operações de provisionamento. Você pode iniciar a operação de provisionamento e exibir o status da operação de provisionamento.
- **Recovery** — operações de recuperação do nó de administração principal. Você pode redefinir informações, carregar o pacote de recuperação, iniciar a recuperação e exibir o status da operação de

recuperação.

- **Recovery-package** — operações para baixar o Recovery Package.
- **Sites** — operações de configuração no nível do local. Você pode criar, exibir, excluir e modificar um site.
- **Temporary-password** — operações na senha temporária para proteger a mgmt-api durante a instalação.

Onde ir a seguir

Depois de concluir uma instalação, execute as tarefas de integração e configuração necessárias. Você pode executar as tarefas opcionais conforme necessário.

Tarefas necessárias

- "Crie uma conta de locatário" Para o protocolo cliente S3 que será utilizado para armazenar objetos no seu sistema StorageGRID.
- "Controle o acesso ao sistema" configurando grupos e contas de usuário. Opcionalmente, você pode "configure uma fonte de identidade federada" (como ative Directory ou OpenLDAP), para que você possa importar grupos de administração e usuários. Ou, você pode "crie grupos locais e usuários".
- Integre e teste os "S3 API" aplicativos cliente que você usará para carregar objetos para seu sistema StorageGRID.
- "Configure as regras de gerenciamento do ciclo de vida das informações (ILM) e a política ILM" você deseja usar para proteger os dados do objeto.
- Se a instalação incluir nós de storage do dispositivo, use o SANtricity os para concluir as seguintes tarefas:
  - Ligue a cada dispositivo StorageGRID.
  - Verifique a receção dos dados do AutoSupport.

    ```
    https://docs.netapp.com/us-en/storagegrid-
    appliances/installconfig/configuring-hardware.html["Configure o
    hardware"^]Consulte .
    ```

- Analise e siga o "Diretrizes de fortalecimento do sistema StorageGRID" para eliminar os riscos de segurança.
- "Configurar notificações por e-mail para alertas do sistema".

Tarefas opcionais

- "Atualize os endereços IP do nó da grade" Se eles foram alterados desde que você planejou sua implantação e gerou o Pacote de recuperação.
- "Configurar a criptografia de armazenamento", se necessário.
- "Configurar a compressão de armazenamento" para reduzir o tamanho dos objetos armazenados, se necessário.
- "Configurar interfaces VLAN" para isolar e particionar o tráfego de rede, se necessário.
- "Configurar grupos de alta disponibilidade" Para melhorar a disponibilidade de conexão para os clientes Grid Manager, Tenant Manager e S3, se necessário.

- "Configurar pontos de extremidade do balanceador de carga" Para conetividade de cliente S3, se necessário.

Solucionar problemas de instalação

Se ocorrerem problemas durante a instalação do sistema StorageGRID, pode aceder aos ficheiros de registo de instalação. O suporte técnico também pode precisar usar os arquivos de log de instalação para resolver problemas.

Os seguintes arquivos de log de instalação estão disponíveis no contentor que está executando cada nó:

- `/var/local/log/install.log` (encontrado em todos os nós da grade)
- `/var/local/log/gdu-server.log` (Encontrado no nó de administração principal)

Os seguintes arquivos de log de instalação estão disponíveis no host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

Para saber como acessar os arquivos de log, "Colete arquivos de log e dados do sistema"consulte .

Informações relacionadas

"Solucionar problemas de um sistema StorageGRID"

Exemplo /etc/sysconfig/network-scripts

Você pode usar os arquivos de exemplo para agregar quatro interfaces físicas do Linux em uma única ligação LACP e, em seguida, estabelecer três interfaces de VLAN que subtendem a ligação para uso como interfaces de rede StorageGRID, Admin e rede cliente.

Interfaces físicas

Observe que os switches nas outras extremidades dos links também devem tratar as quatro portas como um único tronco LACP ou canal de porta, e devem passar pelo menos as três VLANs referenciadas com tags.

`/etc/sysconfig/network-scripts/ifcfg-ens160`

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

`/etc/sysconfig/network-scripts/ifcfg-ens192`

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Interface Bond

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

Interfaces VLAN

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Instale o StorageGRID no Ubuntu ou Debian

Início rápido para instalar o StorageGRID no Ubuntu ou Debian

Siga estes passos de alto nível para instalar um nó Ubuntu ou Debian StorageGRID.

1. **Preparação**

- Saiba mais "Topologia de rede e arquitetura StorageGRID"sobre .
- Saiba mais sobre as especificidades "Rede StorageGRID"do .
- Reúna e prepare o "Informações e materiais necessários".
- Prepare o "CPU e RAM"necessário .
- Fornecer para "requisitos de storage e desempenho".
- "Prepare os servidores Linux" Isso hospedará seus nós do StorageGRID.

Implantação

Implante nós de grade. Quando você implementa nós de grade, eles são criados como parte do sistema StorageGRID e conetados a uma ou mais redes.

- Para implantar nós de grade baseados em software nos hosts preparados na etapa 1, use a linha de comando do Linux e "arquivos de configuração do nó"o .
- Para implantar os nós de dispositivos StorageGRID, siga o "Início rápido para instalação de hardware".

Configuração

Quando todos os nós tiverem sido implantados, use o Gerenciador de Grade para "configure a grade e conclua a instalação".

Automatize a instalação

Para economizar tempo e fornecer consistência, você pode automatizar a instalação do serviço de host StorageGRID e a configuração de nós de grade.

- Use uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef, para automatizar:
  - Instalação do Ubuntu ou Debian
  - Configuração de rede e armazenamento
  - Instalação do mecanismo de contêiner e do serviço host do StorageGRID
  - Implantação de nós de grade virtual

  "Automatize a instalação e a configuração do serviço de host StorageGRID"Consulte .
- Depois de implantar nós de grade, "Automatize a configuração do sistema StorageGRID" usando o script de configuração Python fornecido no arquivo de instalação.
- "Automatize a instalação e a configuração dos nós de grade do dispositivo"
- Se você é um desenvolvedor avançado de implantações do StorageGRID, automatize a instalação de nós de grade usando o "API REST de instalação".

Planeje e prepare-se para instalação no Ubuntu ou Debian

Informações e materiais necessários

Antes de instalar o StorageGRID, reúna e prepare as informações e materiais necessários.

Informações necessárias

Plano de rede

Quais redes você pretende anexar a cada nó do StorageGRID. O StorageGRID suporta várias redes para separação de tráfego, segurança e conveniência administrativa.

Consulte o StorageGRID "Diretrizes de rede".

Informações de rede

Endereços IP para atribuir a cada nó de grade e aos endereços IP dos servidores DNS e NTP.

Servidores para nós de grade

Identifique um conjunto de servidores (físicos, virtuais ou ambos) que, no agregado, fornecem recursos suficientes para suportar o número e o tipo de nós do StorageGRID que você planeja implantar.

> Se a instalação do StorageGRID não usar nós de armazenamento do StorageGRID Appliance (hardware), você deve usar o armazenamento RAID de hardware com cache de gravação (BBWC) com bateria. O StorageGRID não suporta o uso de redes de área de armazenamento virtual (VSANs), RAID de software ou nenhuma proteção RAID.

Migração de nós (se necessário)

Entenda o "requisitos para migração de nós", se você quiser executar a manutenção programada em hosts físicos sem qualquer interrupção do serviço.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Materiais necessários

Licença NetApp StorageGRID

Você deve ter uma licença NetApp válida e assinada digitalmente.

> Uma licença de não produção, que pode ser usada para testar e testar grades de prova de conceito, está incluída no arquivo de instalação do StorageGRID.

Arquivo de instalação do StorageGRID

"Baixe o arquivo de instalação do StorageGRID e extraia os arquivos".

Serviço de laptop

O sistema StorageGRID é instalado através de um computador portátil de serviço.

O computador portátil de serviço deve ter:

- Porta de rede
- Cliente SSH (por exemplo, PuTTY)
- "Navegador da Web suportado"

Documentação do StorageGRID

- "Notas de lançamento"
- "Instruções para administrar o StorageGRID"

Baixe e extraia os arquivos de instalação do StorageGRID

Você deve baixar o arquivo de instalação do StorageGRID e extrair os arquivos necessários. Opcionalmente, você pode verificar manualmente os arquivos no pacote de instalação.

Passos

1. Vá para "Página de downloads do NetApp para StorageGRID" .
2. Selecione o botão para baixar a versão mais recente ou selecione outra versão no menu suspenso e selecione **Go**.
3. Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.
4. Se for apresentada uma instrução Caution/MustRead, leia-a e selecione a caixa de verificação.

   Você deve aplicar os hotfixes necessários depois de instalar a versão do StorageGRID. Para obter mais informações, consulte a. "procedimento de hotfix nas instruções de recuperação e manutenção"

5. Leia o Contrato de Licença de Utilizador final, selecione a caixa de verificação e, em seguida, selecione **Accept & continue**.
6. Na coluna **Install StorageGRID**, selecione o arquivo de instalação .tgz ou .zip para Ubuntu ou Debian.

   Selecione o `.zip` ficheiro se estiver a executar o Windows no computador portátil de serviço.

7. Salve o arquivo de instalação.
8. se você precisa verificar o arquivo de instalação:
   a. Baixe o pacote de verificação de assinatura de código StorageGRID. O nome do arquivo deste pacote usa o formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`, onde `<version-number>` está a versão do software StorageGRID.
   b. Siga os passos para "verifique manualmente os arquivos de instalação".
9. Extraia os arquivos do arquivo de instalação.
10. Escolha os arquivos que você precisa.

    Os arquivos de que você precisa dependem da topologia de grade planejada e de como você implantará seu sistema StorageGRID.

    Os caminhos listados na tabela são relativos ao diretório de nível superior instalado pelo arquivo de instalação extraído.

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 `/debs/storagegrid-webscale-images-version-SHA.deb`.
	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. Você também pode usar este script para integração Ping federate.
	Um exemplo de arquivo de configuração para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` 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.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.

Caminho e nome do arquivo	Descrição
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.
	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.

Verificar manualmente os arquivos de instalação (opcional)

Se necessário, você pode verificar manualmente os arquivos no arquivo de instalação do StorageGRID.

Antes de começar

Você tem "download do pacote de verificação"do "Página de downloads do NetApp para StorageGRID".

Passos

1. Extraia os artefatos do pacote de verificação:

   ```
   tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
   ```

2. Certifique-se de que estes artefactos foram extraídos:
   - Folha de certificado: `Leaf-Cert.pem`
   - Cadeia de certificados: `CA-Int-Cert.pem`
   - Cadeia de resposta do carimbo de hora: `TS-Cert.pem`
   - Ficheiro checksum: `sha256sum`
   - Assinatura do checksum: `sha256sum.sig`
   - Ficheiro de resposta do carimbo de hora: `sha256sum.sig.tsr`
3. Utilize a corrente para verificar se o certificado de lâminas é válido.

   Exemplo: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

   Saída esperada: `Leaf-Cert.pem: OK`

4. Se a etapa *2* falhou devido a um certificado de folha expirado, use o `tsr` arquivo para verificar.

   Exemplo: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

Saída esperada inclui: `Verification: OK`

5. Crie um arquivo de chave pública a partir do certificado Leaf.

   Exemplo: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

   Saída esperada: *None*

6. Use a chave pública para verificar o `sha256sum` arquivo contra `sha256sum.sig`.

   Exemplo: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

   Saída esperada: `Verified OK`

7. Verifique o `sha256sum` conteúdo do arquivo em relação às somas de verificação recém-criadas.

   Exemplo: `sha256sum -c sha256sum`

   Saída esperada: *<filename>*`: OK`
   <filename> É o nome do arquivo que você baixou.

8. "Conclua as etapas restantes" para extrair e escolher os arquivos de instalação apropriados.

Requisitos de software para Ubuntu e Debian

Você pode usar uma máquina virtual para hospedar qualquer tipo de nó StorageGRID. Você precisa de uma máquina virtual para cada nó de grade.

Para instalar o StorageGRID no Ubuntu ou Debian, você deve instalar alguns pacotes de software de terceiros. Algumas distribuições Linux suportadas não contêm esses pacotes por padrão. As versões de pacotes de software em que as instalações do StorageGRID são testadas incluem as listadas nesta página.

Se você selecionar uma opção de instalação de runtime de distribuição Linux e container que exija qualquer um desses pacotes e eles não forem instalados automaticamente pela distribuição Linux, instale uma das versões listadas aqui se disponível no seu provedor ou no fornecedor de suporte para sua distribuição Linux. Caso contrário, use as versões de pacote padrão disponíveis do seu fornecedor.

Todas as opções de instalação requerem Podman ou Docker. Não instale ambos os pacotes. Instale apenas o pacote exigido pela opção de instalação.

> O suporte para Docker como o mecanismo de contentor para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contentor em uma versão futura.

Versões Python testadas

- 3,5.2-2
- 3,6.8-2
- 3,6.8-38
- 3,6.9-1

- 3,7.3-1
- 3,8.10-0
- 3,9.2-1
- 3,9.10-2
- 3,9.16-1
- 3,10.6-1
- 3,11.2-6

Versões do Podman testadas

- 3,2.3-0
- 3,4.4-ds1
- 4,1.1-7
- 4,2.0-11
- 4,3.1-ds1-8-b1
- 4,4.1-8
- 4,4.1-12

Versões do Docker testadas

O suporte do Docker está obsoleto e será removido em uma versão futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1,5-2

Requisitos de CPU e RAM

Antes de instalar o software StorageGRID, verifique e configure o hardware para que ele esteja pronto para suportar o sistema StorageGRID.

Cada nó do StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Depende do total de RAM disponível e da quantidade de software que não seja StorageGRID executado no sistema
  - Geralmente, pelo menos 24 GB por nó e 2 a 16 GB menos do que a RAM total do sistema
  - Um mínimo de 64 GB para cada locatário que terá aproximadamente 5.000 buckets

Certifique-se de que o número de nós de StorageGRID que você planeja executar em cada host físico ou virtual não exceda o número de núcleos de CPU ou a RAM física disponível. Se os hosts não forem dedicados à execução do StorageGRID (não recomendado), certifique-se de considerar os requisitos de recursos dos outros aplicativos.

> Monitore regularmente o uso da CPU e da memória para garantir que esses recursos continuem a acomodar sua carga de trabalho. Por exemplo, duplicar a alocação de RAM e CPU para nós de storage virtual forneceria recursos semelhantes aos fornecidos para nós de dispositivos StorageGRID. Além disso, se a quantidade de metadados por nó exceder 500 GB, considere aumentar a RAM por nó para 48 GB ou mais. Para obter informações sobre como gerenciar o armazenamento de metadados de objetos, aumentar a configuração espaço reservado de metadados e monitorar o uso da CPU e da memória, consulte as instruções para "administrar", "monitorização"e "a atualizar"StorageGRID.

Se o hyperthreading estiver habilitado nos hosts físicos subjacentes, você poderá fornecer 8 núcleos virtuais (4 núcleos físicos) por nó. Se o hyperthreading não estiver habilitado nos hosts físicos subjacentes, você deverá fornecer 8 núcleos físicos por nó.

Se você estiver usando máquinas virtuais como hosts e tiver controle sobre o tamanho e o número de VMs, use uma única VM para cada nó do StorageGRID e dimensione a VM de acordo.

Para implantações de produção, você não deve executar vários nós de storage no mesmo hardware de storage físico ou host virtual. Cada nó de storage em uma única implantação do StorageGRID deve estar em seu próprio domínio de falha isolado. Você pode maximizar a durabilidade e a disponibilidade dos dados de objetos se garantir que uma única falha de hardware só pode afetar um único nó de storage.

Consulte também "Requisitos de storage e desempenho".

Requisitos de storage e desempenho

Você precisa entender os requisitos de storage para nós do StorageGRID para que possa fornecer espaço suficiente para dar suporte à configuração inicial e à expansão de storage futura.

Os nós de StorageGRID exigem três categorias lógicas de storage:

- **Pool de contentores** — armazenamento de nível de desempenho (SAS ou SSD de 10K GB) para os contentores de nós, que serão atribuídos ao driver de armazenamento do Docker quando você instalar e configurar o Docker nos hosts que suportarão seus nós do StorageGRID.
- **Dados do sistema** — armazenamento em camada de desempenho (SAS ou SSD de 10K GB) para armazenamento persistente por nó de dados do sistema e logs de transações, que os serviços de host do StorageGRID consumirão e mapearão em nós individuais.
- **Dados de objeto** — armazenamento em camada de desempenho (SAS ou SSD de 10K TB) e armazenamento em massa de camada de capacidade (NL-SAS/SATA) para armazenamento persistente de dados de objetos e metadados de objetos.

Você deve usar dispositivos de bloco compatíveis com RAID para todas as categorias de armazenamento. Discos não redundantes, SSDs ou JBODs não são suportados. Você pode usar o armazenamento RAID compartilhado ou local para qualquer uma das categorias de armazenamento. No entanto, se quiser usar a funcionalidade de migração de nós no StorageGRID, você deve armazenar dados do sistema e dados de objetos no armazenamento compartilhado. Para obter mais informações, "Requisitos de migração de contêiner de nós"consulte .

Requisitos de desempenho

A performance dos volumes usados para o pool de contêineres, dados do sistema e metadados de objetos afeta significativamente o desempenho geral do sistema. Você deve usar o storage de camada de desempenho (SAS ou SSD de 10K GB) para esses volumes, a fim de garantir um desempenho de disco adequado em termos de latência, IOPS/operações de entrada/saída por segundo (IOPS) e taxa de transferência. Você pode usar o storage de camada de capacidade (NL-SAS/SATA) para o storage persistente de dados de objetos.

Os volumes usados para o pool de contêineres, dados do sistema e dados de objetos precisam ter o armazenamento em cache de gravação habilitado. O cache deve estar em uma Mídia protegida ou persistente.

Requisitos para hosts que usam storage NetApp ONTAP

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.

Número de hosts necessários

Cada local do StorageGRID requer um mínimo de três nós de storage.

> 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.

Outros tipos de nós, como nós de administração ou nós de gateway, podem ser implantados nos mesmos hosts ou podem ser implantados em seus próprios hosts dedicados, conforme necessário.

Número de volumes de storage para cada host

A tabela a seguir mostra o número de volumes de storage (LUNs) necessários para cada host e o tamanho mínimo necessário para cada LUN, com base em quais nós serão implantados nesse host.

O tamanho máximo de LUN testado é de 39 TB.

> Esses números são para cada host, não para toda a grade.

Finalidade do LUN	Categoria de armazenamento	Número de LUNs	Tamanho mínimo/LUN
Pool de armazenamento do mecanismo de contêiner	Pool de contêineres	1	Número total de nós x 100 GB

Finalidade do LUN	Categoria de armazenamento	Número de LUNs	Tamanho mínimo/LUN
`/var/local` volume	Dados do sistema	1 para cada nó neste host	90 GB
Nó de storage	Dados de objeto	3 para cada nó de storage nesse host **Nota:** Um nó de armazenamento baseado em software pode ter 1 a 16 volumes de armazenamento; pelo menos 3 volumes de armazenamento são recomendados.	12 TB (4 TB/LUN) consulte Requisitos de storage para nós de storage para obter mais informações.
Nó de storage (somente metadados)	Metadados de objetos	1	4 TB consulte Requisitos de storage para nós de storage para obter mais informações. **Nota**: Somente um rangedb é necessário para nós de storage somente metadados.
Logs de auditoria do nó de administração	Dados do sistema	1 para cada nó de administração neste host	200 GB
Tabelas Admin Node	Dados do sistema	1 para cada nó de administração neste host	200 GB

Dependendo do nível de auditoria configurado, do tamanho das entradas do usuário, como o nome da chave do objeto S3 e da quantidade de dados de log de auditoria que você precisa preservar, talvez seja necessário aumentar o tamanho do LUN de log de auditoria em cada nó Admin. Geralmente, uma grade gera aproximadamente 1 KB de dados de auditoria por operação S3, o que significaria que um LUN de 200 GB suportaria 70 milhões de operações por dia ou 800 operações por segundo por dois a três dias.

Espaço de armazenamento mínimo para um host

A tabela a seguir mostra o espaço de armazenamento mínimo necessário para cada tipo de nó. Você pode usar essa tabela para determinar a quantidade mínima de storage que deve fornecer ao host em cada categoria de storage, com base nos nós que serão implantados nesse host.

Snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte "recuperação do nó de grade"os procedimentos para cada tipo de nó.

Tipo de nó	Pool de contêineres	Dados do sistema	Dados de objeto
Nó de storage	100 GB	90 GB	4.000 GB
Nó de administração	100 GB	490 GB (3 LUNs)	*não aplicável*
Nó de gateway	100 GB	90 GB	*não aplicável*

Exemplo: Calculando os requisitos de armazenamento de um host

Suponha que você Planeje implantar três nós no mesmo host: Um nó de storage, um nó de administrador e um nó de gateway. Forneça no mínimo nove volumes de storage ao host. Você precisará de um mínimo de 300 GB de storage em camadas de desempenho para os contêineres de nós, 670 GB de storage em camadas de desempenho para dados do sistema e logs de transações e 12 TB de storage em camadas de capacidade para dados de objetos.

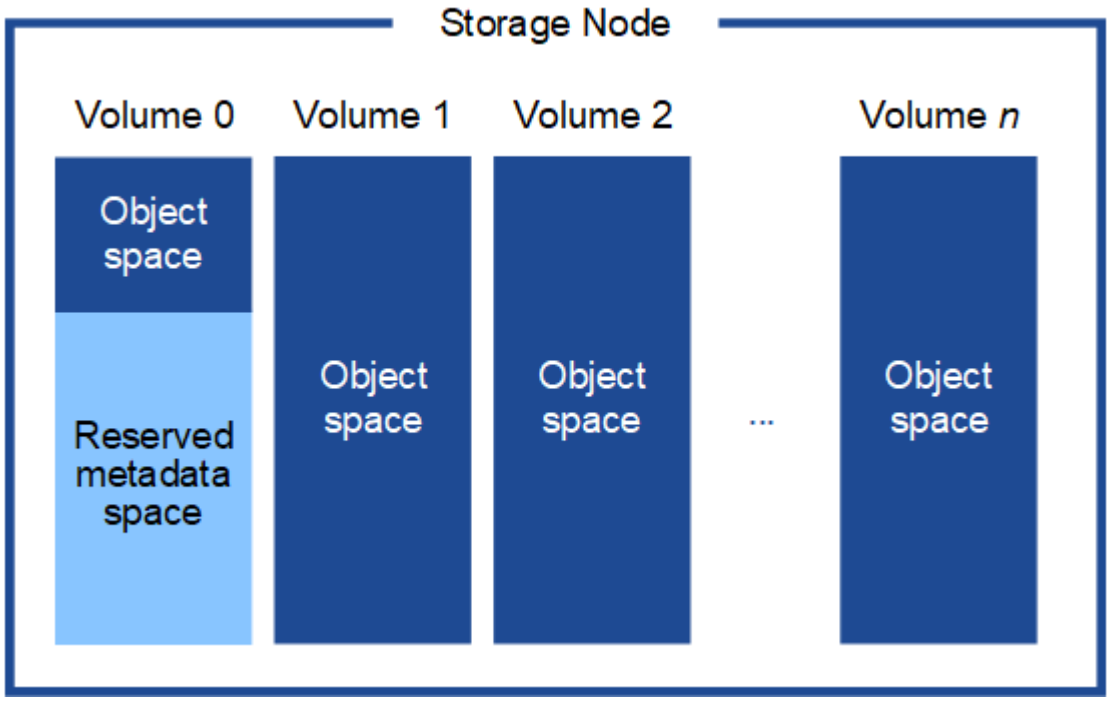
Tipo de nó	Finalidade do LUN	Número de LUNs	Tamanho da LUN
Nó de storage	Pool de armazenamento do Docker	1	300 GB (100 GB/nó)
Nó de storage	`/var/local` volume	1	90 GB
Nó de storage	Dados de objeto	3	12 TB (4 TB/LUN)
Nó de administração	`/var/local` volume	1	90 GB
Nó de administração	Logs de auditoria do nó de administração	1	200 GB
Nó de administração	Tabelas Admin Node	1	200 GB
Nó de gateway	`/var/local` volume	1	90 GB
Total		**9**	• Conjunto de contentores: * 300 GB **Dados do sistema:** 670 GB **Dados do objeto:** 12.000 GB

Requisitos de storage para nós de storage

Um nó de storage baseado em software pode ter 1 a 16 volumes de armazenamento—3 ou mais volumes de armazenamento são recomendados. Cada volume de armazenamento deve ser de 4 TB ou maior.

Um nó de storage de dispositivo pode ter até 48 volumes de storage.

Como mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de storage 0 de cada nó de storage. Qualquer espaço restante no volume de armazenamento 0 e quaisquer outros volumes de armazenamento no nó de armazenamento são usados exclusivamente para dados de objeto.



Para fornecer redundância e proteger os metadados de objetos contra perda, o StorageGRID armazena três cópias dos metadados de todos os objetos no sistema em cada local. As três cópias dos metadados de objetos são distribuídas uniformemente por todos os nós de storage em cada local.

Ao instalar uma grade com nós de storage somente de metadados, a grade também deve conter um número mínimo de nós para storage de objetos. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

- Para uma grade de um único local, pelo menos dois nós de storage são configurados para objetos e metadados.
- Para uma grade de vários locais, pelo menos um nó de storage por local é configurado para objetos e metadados.

Ao atribuir espaço ao volume 0 de um novo nó de storage, você deve garantir que haja espaço adequado para a parte desse nó de todos os metadados de objetos.

- No mínimo, você deve atribuir pelo menos 4 TB ao volume 0.

Se você usar apenas um volume de armazenamento para um nó de armazenamento e atribuir 4 TB ou menos ao volume, o nó de armazenamento poderá entrar no estado somente leitura de armazenamento na inicialização e armazenar somente metadados de objetos.

Se você atribuir menos de 500 GB ao volume 0 (somente uso não-produção), 10% da capacidade do volume de armazenamento será reservada para metadados.

- Se você estiver instalando um novo sistema (StorageGRID 11,6 ou superior) e cada nó de armazenamento tiver 128 GB ou mais de RAM, atribua 8 TB ou mais ao volume 0. O uso de um valor maior para o volume 0 pode aumentar o espaço permitido para metadados em cada nó de storage.
- Ao configurar diferentes nós de storage para um local, use a mesma configuração para o volume 0, se possível. Se um local contiver nós de storage de tamanhos diferentes, o nó de storage com o menor volume 0 determinará a capacidade de metadados desse local.

Para obter mais detalhes, "Gerenciar o storage de metadados de objetos"visite .

Requisitos de migração de contêiner de nós

O recurso de migração de nó permite mover manualmente um nó de um host para outro. Normalmente, ambos os hosts estão no mesmo data center físico.

A migração de nós permite executar a manutenção do host físico sem interromper as operações de grade. Você move todos os nós do StorageGRID, um de cada vez, para outro host antes de colocar o host físico off-line. A migração de nós requer apenas um curto período de inatividade para cada nó e não deve afetar a operação ou a disponibilidade dos serviços de grade.

Se você quiser usar o recurso de migração de nós do StorageGRID, sua implantação deve atender a requisitos adicionais:

- Nomes de interface de rede consistentes entre hosts em um único data center físico
- Storage compartilhado para volumes de repositório de objetos e metadados do StorageGRID que podem ser acessados por todos os hosts em um único data center físico. Por exemplo, você pode usar storage arrays do NetApp e-Series.

Se você estiver usando hosts virtuais e a camada de hypervisor subjacente suportar a migração de VM, talvez queira usar essa funcionalidade em vez do recurso de migração de nós no StorageGRID. Nesse caso, você pode ignorar esses requisitos adicionais.

Antes de executar a migração ou a manutenção do hipervisor, encerre os nós com simplicidade. Consulte as instruções para "fechando um nó de grade".

Migração do VMware Live não suportada

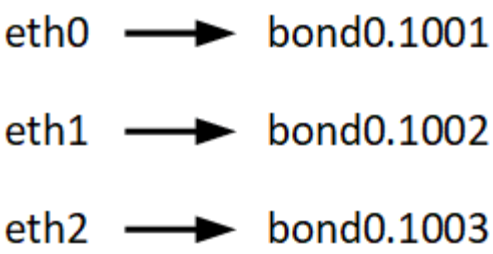
Ao executar a instalação bare-metal nas VMs VMware, o OpenStack Live Migration e o VMware Live vMotion fazem com que o tempo do relógio da máquina virtual salte e não seja compatível com nós de grade de qualquer tipo. Embora raros, tempos de clock incorretos podem resultar em perda de dados ou atualizações de configuração.

A migração fria é suportada. Na migração fria, você desliga os nós do StorageGRID antes de migrá-los entre hosts. Consulte as instruções para "fechando um nó de grade".

Nomes de interface de rede consistentes

Para mover um nó de um host para outro, o serviço de host StorageGRID precisa ter alguma confiança de que a conetividade de rede externa que o nó tem em seu local atual pode ser duplicada no novo local. Ele obtém essa confiança através do uso de nomes de interface de rede consistentes nos hosts.

Suponha, por exemplo, que o StorageGRID NodeA em execução no Host1 foi configurado com os seguintes mapeamentos de interface:



O lado esquerdo das setas corresponde às interfaces tradicionais vistas de dentro de um contentor StorageGRID (ou seja, as interfaces de rede de Grade, Admin e Cliente, respetivamente). O lado direito das setas corresponde às interfaces de host reais que fornecem essas redes, que são três interfaces VLAN subordinadas à mesma ligação de interface física.

Agora, suponha que você queira migrar NodeA para Host2. Se o Host2 também tiver interfaces chamadas bond0,1001, bond0,1002 e bond0,1003, o sistema permitirá a movimentação, assumindo que as interfaces com nomes semelhantes fornecerão a mesma conetividade no Host2 como no Host1. Se Host2 não tiver interfaces com os mesmos nomes, a movimentação não será permitida.

Há muitas maneiras de obter nomes consistentes de interface de rede entre vários hosts; "Configure a rede host"consulte para obter alguns exemplos.

Armazenamento compartilhado

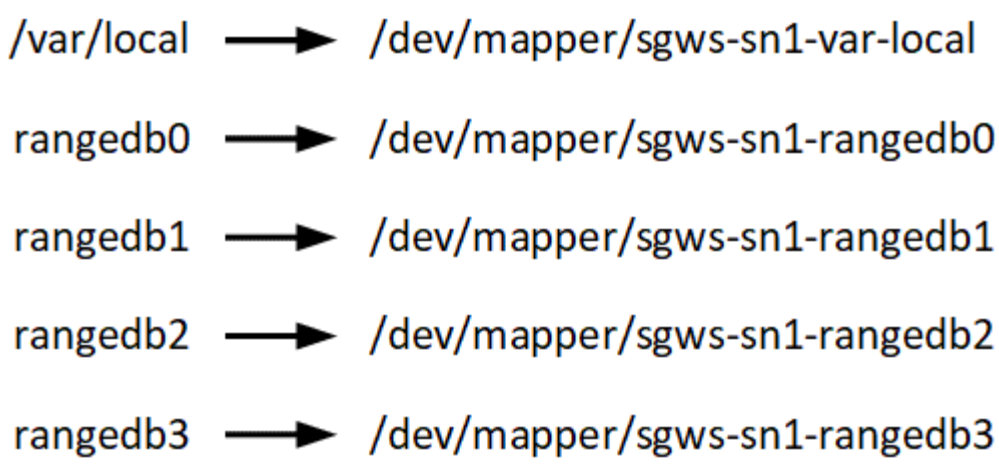
Para realizar migrações de nós rápidas e de baixa sobrecarga, o recurso de migração de nós do StorageGRID não move fisicamente os dados dos nós. Em vez disso, a migração de nós é realizada como um par de operações de exportação e importação, da seguinte forma:

Passos

1. Durante a operação de "exportação de nó", uma pequena quantidade de dados de estado persistente é extraída do contentor de nó em execução no HostA e armazenada em cache no volume de dados do sistema desse nó. Em seguida, o contentor de nó no HostA é desinstanciado.
2. Durante a operação de "importação de nó", o contentor de nó no HostB que usa a mesma interface de rede e mapeamentos de armazenamento de bloco que estavam em vigor no HostA é instanciado. Em seguida, os dados de estado persistente em cache são inseridos na nova instância.

Dado este modo de operação, todos os dados do sistema do nó e volumes de armazenamento de objetos devem estar acessíveis a partir de HostA e HostB para que a migração seja permitida e funcione. Além disso, eles devem ter sido mapeados para o nó usando nomes que são garantidos para se referir aos mesmos LUNs no HostA e HostB.

O exemplo a seguir mostra uma solução para o mapeamento de dispositivos de bloco para um nó de armazenamento StorageGRID, onde o multipathing DM está em uso nos hosts, e o campo alias foi usado `/etc/multipath.conf` para fornecer nomes de dispositivos de bloco consistentes e amigáveis disponíveis em todos os hosts.



Preparar os hosts (Ubuntu ou Debian)

Como as configurações de todo o host mudam durante a instalação

Em sistemas bare metal, o StorageGRID faz algumas alterações nas configurações de todo o host `sysctl`.

As seguintes alterações são feitas:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
```

```
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
```

```
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Instale o Linux

Você deve instalar o StorageGRID em todos os hosts de grade Ubuntu ou Debian. Para obter uma lista de versões suportadas, utilize a ferramenta de Matriz de interoperabilidade do NetApp.

Antes de começar

Certifique-se de que seu sistema operacional atenda aos requisitos mínimos de versão do kernel do StorageGRID, conforme listado abaixo. Use o comando `uname -r` para obter a versão do kernel do seu sistema operacional ou consulte o fornecedor do seu sistema operacional.

Nota: o suporte para Ubuntu versões 18,04 e 20,04 foi obsoleto e será removido em uma versão futura.

Versão Ubuntu	Versão mínima do kernel	Nome do pacote do kernel
18.04.6 (obsoleto)	5,4.0-150-genérico	linux-image-5,4.0-150-generic/bionic-updates, bionic-security, agora 5,4.0-150,167-18.04.1
20.04.5 (obsoleto)	5,4.0-131-genérico	linux-image-5,4.0-131-generic/focal-updates, agora 5,4.0-131,147
22.04.1	5.15.0-47-genérico	linux-image-5.15.0-47-generic/jammy-updates, jammy-security, agora 5.15.0-47,51
24,04	6,8.0-31-genérico	linux-image-6,8.0-31-generic/noble, agora 6,8.0-31,31

Nota: o suporte para a versão 11 do Debian foi obsoleto e será removido em uma versão futura.

Versão Debian	Versão mínima do kernel	Nome do pacote do kernel
11 (obsoleto)	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/estável, agora 5.10.150-1
12	6,1.0-9-amd64	linux-image-6,1.0-9-amd64/stable, agora 6,1.27-1

Passos

1. Instale o Linux em todos os hosts de grade física ou virtual de acordo com as instruções do distribuidor ou seu procedimento padrão.

> Não instale nenhum ambiente de desktop gráfico. Ao instalar o Ubuntu, você deve selecionar **utilitários de sistema padrão**. Selecionar **OpenSSH Server** é recomendado para habilitar o acesso ssh aos seus hosts Ubuntu. Todas as outras opções podem permanecer limpas.

2. Certifique-se de que todos os hosts tenham acesso aos repositórios de pacotes Ubuntu ou Debian.
3. Se a troca estiver ativada:
   a. Execute o seguinte comando: `$ sudo swapoff --all`
   b. Remova todas as entradas de troca de `/etc/fstab` para persistir as configurações.

> A falha ao desativar completamente a troca pode reduzir drasticamente o desempenho.

Compreender a instalação do perfil AppArmor

Se você estiver operando em um ambiente Ubuntu auto-implantado e usando o sistema de controle de acesso obrigatório AppArmor, os perfis AppArmor associados aos pacotes instalados no sistema base podem ser bloqueados pelos pacotes correspondentes instalados com o StorageGRID.

Por padrão, os perfis AppArmor são instalados para os pacotes que você instala no sistema operacional base. Quando você executa esses pacotes a partir do contentor do sistema StorageGRID, os perfis AppArmor são bloqueados. Os pacotes base DHCP, MySQL, NTP e tcdump entram em conflito com o AppArmor, e outros pacotes básicos também podem entrar em conflito.

Você tem duas opções para lidar com perfis AppArmor:

- Desative perfis individuais para os pacotes instalados no sistema base que se sobrepõem aos pacotes no contentor do sistema StorageGRID. Quando você desativa perfis individuais, uma entrada aparece nos arquivos de log do StorageGRID indicando que AppArmor está habilitado.

  Use os seguintes comandos:

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

  Exemplo:

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- Desative o AppArmor completamente. Para o Ubuntu 9,10 ou posterior, siga as instruções na comunidade online do Ubuntu: "Desativar AppArmor". Desabilitar o AppArmor por completo pode não ser possível em versões mais recentes do Ubuntu.

  Depois de desativar o AppArmor, nenhuma entrada indicando que o AppArmor está habilitado aparecerá nos arquivos de log do StorageGRID.

Configurar a rede host (Ubuntu ou Debian)

Depois de concluir a instalação do Linux em seus hosts, você pode precisar executar alguma configuração adicional para preparar um conjunto de interfaces de rede em cada

host que são adequadas para mapear nos nós do StorageGRID que você implantará posteriormente.

Antes de começar

- Você revisou o "Diretrizes de rede da StorageGRID".
- Você revisou as informações "requisitos de migração de contêiner de nós"sobre .
- Se você estiver usando hosts virtuais, leia o Considerações e recomendações para clonagem de endereços MAC antes de configurar a rede host.

> Se você estiver usando VMs como hosts, selecione VMXNET 3 como o adaptador de rede virtual. O adaptador de rede VMware E1000 causou problemas de conetividade com os contentores StorageGRID implantados em determinadas distribuições do Linux.

Sobre esta tarefa

Os nós de grade devem ser capazes de acessar a rede de grade e, opcionalmente, as redes Admin e Client. Você fornece esse acesso criando mapeamentos que associam a interface física do host às interfaces virtuais para cada nó de grade. Ao criar interfaces de host, use nomes amigáveis para facilitar a implantação em todos os hosts e habilitar a migração.

A mesma interface pode ser compartilhada entre o host e um ou mais nós. Por exemplo, você pode usar a mesma interface para acesso ao host e acesso à rede de administração de nó, para facilitar a manutenção do host e do nó. Embora a mesma interface possa ser compartilhada entre o host e os nós individuais, todos devem ter endereços IP diferentes. Os endereços IP não podem ser compartilhados entre nós ou entre o host e qualquer nó.

Você pode usar a mesma interface de rede de host para fornecer a interface de rede de grade para todos os nós de StorageGRID no host; você pode usar uma interface de rede de host diferente para cada nó; ou você pode fazer algo entre eles. No entanto, você normalmente não fornecerá a mesma interface de rede de host que as interfaces de rede de Grade e Admin para um único nó ou como a interface de rede de Grade para um nó e a interface de rede de Cliente para outro.

Você pode concluir esta tarefa de várias maneiras. Por exemplo, se seus hosts forem máquinas virtuais e você estiver implantando um ou dois nós de StorageGRID para cada host, você poderá criar o número correto de interfaces de rede no hypervisor e usar um mapeamento de 1 para 1. Se você estiver implantando vários nós em hosts bare metal para uso em produção, poderá aproveitar o suporte da pilha de rede Linux para VLAN e LACP para tolerância a falhas e compartilhamento de largura de banda. As seções a seguir fornecem abordagens detalhadas para ambos os exemplos. Você não precisa usar nenhum desses exemplos; você pode usar qualquer abordagem que atenda às suas necessidades.

> Não use dispositivos bond ou bridge diretamente como a interface de rede do contentor. Isso pode impedir a inicialização do nó causada por um problema de kernel com o uso do MACVLAN com dispositivos de ligação e ponte no namespace do contentor. Em vez disso, use um dispositivo não-bond, como um par VLAN ou Ethernet virtual (vete). Especifique este dispositivo como a interface de rede no arquivo de configuração do nó.

Considerações e recomendações para clonagem de endereços MAC

A clonagem de endereços MAC faz com que o contentor use o endereço MAC do host e o host use o endereço MAC de um endereço especificado ou gerado aleatoriamente. Você deve usar a clonagem de endereços MAC para evitar o uso de configurações de rede de modo promíscuo.

Ativar a clonagem MAC

Em certos ambientes, a segurança pode ser aprimorada por meio da clonagem de endereços MAC, pois permite que você use uma NIC virtual dedicada para a rede Admin, rede Grid e rede Client. Ter o contentor usar o endereço MAC da NIC dedicada no host permite evitar o uso de configurações de rede de modo promíscuas.

> A clonagem de endereços MAC destina-se a ser usada com instalações de servidores virtuais e pode não funcionar corretamente com todas as configurações de dispositivos físicos.

> Se um nó não iniciar devido a uma interface de destino de clonagem MAC estar ocupada, talvez seja necessário definir o link para "baixo" antes de iniciar o nó. Além disso, é possível que o ambiente virtual possa impedir a clonagem de MAC em uma interface de rede enquanto o link estiver ativo. Se um nó não definir o endereço MAC e iniciar devido a uma interface estar ocupada, definir o link para "baixo" antes de iniciar o nó pode corrigir o problema.

A clonagem de endereços MAC está desativada por padrão e deve ser definida por chaves de configuração de nós. Você deve ativá-lo quando instalar o StorageGRID.

Há uma chave para cada rede:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Definir a chave como "verdadeiro" faz com que o contentor use o endereço MAC da NIC do host. Além disso, o host usará o endereço MAC da rede de contentores especificada. Por padrão, o endereço do contentor é um endereço gerado aleatoriamente, mas se você tiver definido um usando a `_NETWORK_MAC` chave de configuração do nó, esse endereço será usado em vez disso. O host e o contentor sempre terão endereços MAC diferentes.

> Ativar a clonagem MAC em um host virtual sem também ativar o modo promíscuo no hypervisor pode fazer com que a rede de host Linux usando a interface do host pare de funcionar.

Casos de uso de clonagem DE MAC

Existem dois casos de uso a considerar com clonagem MAC:

- Clonagem DE MAC não ativada: Quando a `_CLONE_MAC` chave no arquivo de configuração do nó não estiver definida ou definida como "falsa", o host usará o MAC da NIC do host e o contentor terá um MAC gerado pelo StorageGRID, a menos que um MAC seja especificado na `_NETWORK_MAC` chave. Se um endereço for definido na `_NETWORK_MAC` chave, o contentor terá o endereço especificado na `_NETWORK_MAC` chave. Esta configuração de chaves requer o uso do modo promíscuo.
- Clonagem DO MAC ativada: Quando a `_CLONE_MAC` chave no arquivo de configuração do nó é definida como "verdadeiro", o contentor usa o MAC da NIC do host e o host usa um MAC gerado pelo StorageGRID, a menos que um MAC seja especificado na `_NETWORK_MAC` chave. Se um endereço for definido na `_NETWORK_MAC` chave, o host usará o endereço especificado em vez de um gerado. Nesta configuração de chaves, você não deve usar o modo promíscuo.

Se você não quiser usar a clonagem de endereços MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes dos atribuídos pelo hypervisor, verifique se as propriedades de segurança nos níveis de switch virtual e grupo de portas estão definidas como **Accept** para modo promíscuo, alterações de endereço MAC e transmissões forjadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Para ativar a clonagem MAC, consulte o "instruções para criar arquivos de configuração de nó".

Exemplo de clonagem DE MAC

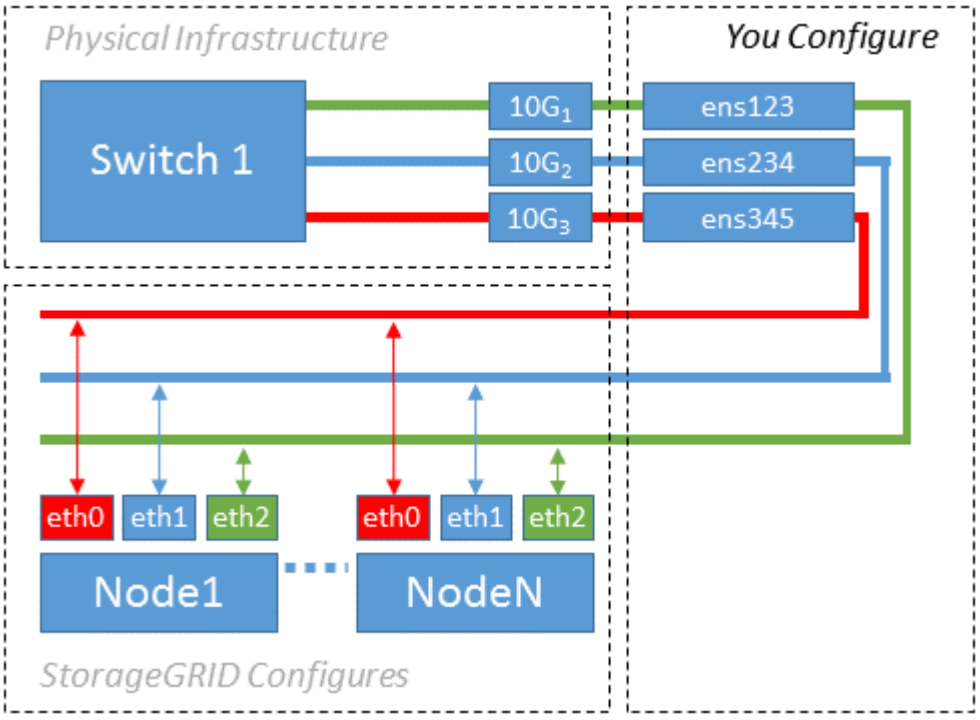
Exemplo de clonagem MAC ativada com um host com endereço MAC de 11:22:33:44:55:66 para a interface ens256 e as seguintes chaves no arquivo de configuração do nó:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Resultado: O MAC do host para ens256 é B2:9c:02:C2:27:10 e o MAC da rede Admin é 11:22:33:44:55:66

Exemplo 1: Mapeamento de 1 para 1 para NICs físicos ou virtuais

O exemplo 1 descreve um mapeamento de interface física simples que requer pouca ou nenhuma configuração do lado do host.



O sistema operacional Linux cria as interfaces ensXYZ automaticamente durante a instalação ou inicialização, ou quando as interfaces são hot-added. Não é necessária nenhuma configuração além de garantir que as interfaces estejam configuradas para serem criadas automaticamente após a inicialização. Você tem que determinar qual ensXYZ corresponde a qual rede StorageGRID (Grade, Administrador ou Cliente) para que você possa fornecer os mapeamentos corretos posteriormente no processo de configuração.

Observe que a figura mostra vários nós de StorageGRID; no entanto, você normalmente usaria essa configuração para VMs de nó único.

Se o Switch 1 for um switch físico, você deve configurar as portas conetadas a interfaces de 10G 3 a 1 a 10G para o modo de acesso e colocá-las nas VLANs apropriadas.

Exemplo 2: VLANs de transporte de ligação LACP

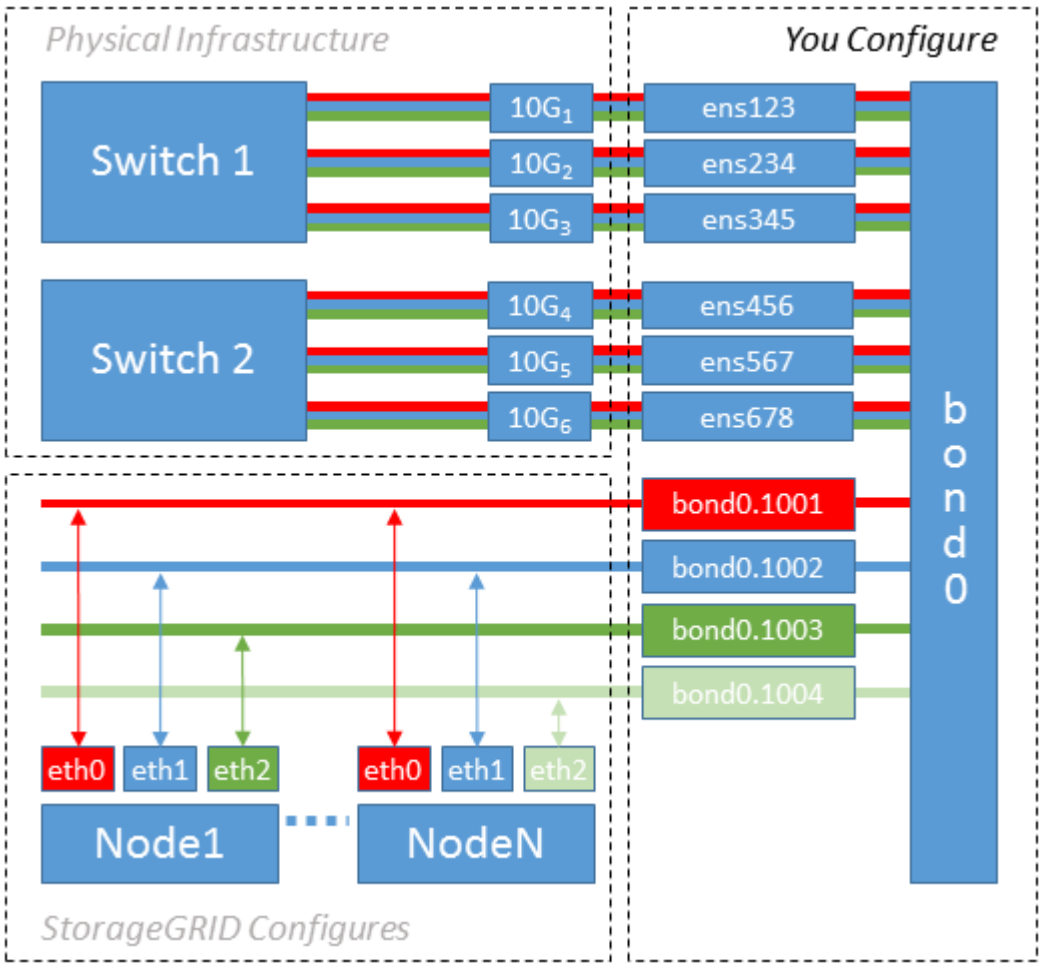
O exemplo 2 assume que você está familiarizado com a ligação de interfaces de rede e com a criação de interfaces VLAN na distribuição Linux que você está usando.

Sobre esta tarefa

O exemplo 2 descreve um esquema genérico, flexível e baseado em VLAN que facilita o compartilhamento de toda a largura de banda de rede disponível em todos os nós em um único host. Este exemplo é particularmente aplicável a hosts de metal nu.

Para entender esse exemplo, suponha que você tenha três sub-redes separadas para redes Grid, Admin e Client em cada data center. As sub-redes estão em VLANs separadas (1001, 1002 e 1003) e são apresentadas ao host em uma porta de tronco ligada ao LACP (bond0). Você configuraria três interfaces VLAN na ligação: bond0,1001, bond0,1002 e bond0,1003.

Se você precisar de VLANs e sub-redes separadas para redes de nós no mesmo host, você pode adicionar interfaces VLAN na ligação e mapeá-las no host (mostrado como bond0,1004 na ilustração).



Passos

1. Agregue todas as interfaces de rede físicas que serão usadas para conetividade de rede StorageGRID em uma única ligação LACP.

   Use o mesmo nome para a ligação em cada host, por exemplo, bond0.

2. Crie interfaces VLAN que usam essa ligação como seu "dispositivo físico" associado, usando a convenção de nomenclatura de interface VLAN padrão `physdev-name.VLAN ID`.

   Observe que as etapas 1 e 2 exigem a configuração apropriada nos switches de borda que terminam as outras extremidades dos links de rede. As portas do switch de borda também devem ser agregadas em um canal de porta LACP, configurado como um tronco, e ter permissão para passar todas as VLANs necessárias.

   Exemplos de arquivos de configuração de interface para este esquema de configuração de rede por host são fornecidos.

Informações relacionadas

"Exemplo /etc/network/interfaces"

Configurar o armazenamento do host

Você deve alocar volumes de storage de bloco a cada host.

Antes de começar

Você revisou os tópicos a seguir, que fornecem informações necessárias para realizar esta tarefa:

- "Requisitos de storage e desempenho"
- "Requisitos de migração de contêiner de nós"

Sobre esta tarefa

Ao alocar LUNs (Block Storage volumes) para hosts, use as tabelas em "requisitos de armazenamento" para determinar o seguinte:

- Número de volumes necessários para cada host (com base no número e nos tipos de nós que serão implantados nesse host)
- Categoria de storage para cada volume (ou seja, dados do sistema ou dados de objeto)
- Tamanho de cada volume

Você usará essas informações, bem como o nome persistente atribuído pelo Linux a cada volume físico quando implantar nós do StorageGRID no host.

> Você não precisa particionar, formatar ou montar qualquer um desses volumes; você só precisa garantir que eles sejam visíveis para os hosts.

> Somente um LUN de dados de objeto é necessário para nós de storage somente de metadados.

Evite usar arquivos de dispositivo especiais "brutos" (`/dev/sdb`, por exemplo) ao compor sua lista de nomes de volume. Esses arquivos podem mudar através das reinicializações do host, o que afetará o funcionamento adequado do sistema. Se você estiver usando iSCSI LUNs e Device Mapper Multipathing, considere usar alias de multipath no `/dev/mapper` diretório, especialmente se a topologia SAN incluir caminhos de rede

redundantes para o armazenamento compartilhado. Em alternativa, pode utilizar as ligações virtuais criadas pelo sistema em `/dev/disk/by-path/` para os nomes de dispositivos persistentes.

Por exemplo:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Os resultados serão diferentes para cada instalação.

Atribua nomes amigáveis a cada um desses volumes de storage de bloco para simplificar a instalação inicial do StorageGRID e os procedimentos de manutenção futuros. Se você estiver usando o driver multipath de mapeamento de dispositivos para acesso redundante a volumes de armazenamento compartilhados, você poderá usar o `alias` campo em `/etc/multipath.conf` seu arquivo.

Por exemplo:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

Usar o campo alias dessa forma faz com que os aliases apareçam como dispositivos de bloco `/dev/mapper` no diretório do host, permitindo que você especifique um nome amigável e facilmente validado sempre que uma operação de configuração ou manutenção exigir a especificação de um volume de armazenamento de bloco.

Se você estiver configurando o armazenamento compartilhado para suportar a migração de nós do StorageGRID e usando multipathing do Mapeador de dispositivos, você poderá criar e instalar um comum `/etc/multipath.conf` em todos os hosts localizados. Apenas certifique-se de usar um volume de armazenamento Docker diferente em cada host. Usar aliases e incluir o nome de host de destino no alias para cada LUN de volume de armazenamento do Docker tornará isso fácil de lembrar e é recomendado.

> O suporte para Docker como o mecanismo de contentor para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contentor em uma versão futura.

Informações relacionadas

- "Requisitos de storage e desempenho"
- "Requisitos de migração de contêiner de nós"

Configure o volume de armazenamento do motor do recipiente

Antes de instalar o mecanismo de contentor (Docker ou Podman), talvez seja necessário formatar o volume de armazenamento e montá-lo.

> O suporte para Docker como o mecanismo de contentor para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contentor em uma versão futura.

Sobre esta tarefa

Você pode ignorar essas etapas se você planeja usar o armazenamento local para o volume de armazenamento do Docker e tem espaço suficiente disponível na partição do host que contém `/var/lib`.

Passos

1. Crie um sistema de arquivos no volume de armazenamento do Docker:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Monte o volume de armazenamento do Docker:

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Adicione uma entrada para docker-storage-volume-volume-device ao /etc/fstab.

   Essa etapa garante que o volume de storage seja remontado automaticamente após a reinicialização do host.

Instale o Docker

O sistema StorageGRID é executado no Linux como uma coleção de contentores Docker. Antes de poder instalar o StorageGRID, você deve instalar o Docker.

> O suporte para Docker como o mecanismo de contentor para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contentor em uma versão futura.

Passos

1. Instale o Docker seguindo as instruções para sua distribuição Linux.

   > Se o Docker não estiver incluído na sua distribuição Linux, você poderá baixá-lo a partir do site do Docker.

2. Certifique-se de que o Docker foi ativado e iniciado executando os dois comandos a seguir:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirme que instalou a versão esperada do Docker inserindo o seguinte:

```
sudo docker version
```

As versões Cliente e servidor devem ser 1.11.0 ou posterior.

Informações relacionadas

"Configurar o armazenamento do host"

Instalar os serviços de host do StorageGRID

Você usa o pacote DEB do StorageGRID para instalar os serviços de host do StorageGRID.

Sobre esta tarefa

Estas instruções descrevem como instalar os serviços de host a partir dos pacotes DEB. Como alternativa, você pode usar os metadados do repositório APT incluídos no arquivo de instalação para instalar os pacotes DEB remotamente. Veja as instruções do repositório APT para o seu sistema operacional Linux.

Passos

1. Copie os pacotes DEB do StorageGRID para cada um de seus hosts ou disponibilize-os no armazenamento compartilhado.

   Por exemplo, coloque-os `/tmp` no diretório, para que você possa usar o comando exemplo na próxima etapa.

2. Faça login em cada host como root ou usando uma conta com permissão sudo e execute os seguintes comandos.

   Você deve instalar o `images` pacote primeiro, e o `service` pacote segundo. Se você colocou os pacotes em um diretório diferente `/tmp`do , modifique o comando para refletir o caminho usado.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```

> O Python 2,7 já deve ser instalado antes que os pacotes StorageGRID possam ser instalados. O `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` comando falhará até que você o tenha feito.

Automatize a instalação (Ubuntu ou Debian)

Você pode automatizar a instalação do serviço de host StorageGRID e a configuração de nós de grade.

Sobre esta tarefa

Automatizar a implantação pode ser útil em qualquer um dos seguintes casos:

- Você já usa uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef, para implantar e configurar hosts físicos ou virtuais.
- Você pretende implantar várias instâncias do StorageGRID.
- Você está implantando uma instância grande e complexa do StorageGRID.

O serviço de host do StorageGRID é instalado por um pacote e impulsionado por arquivos de configuração que podem ser criados interativamente durante uma instalação manual ou preparados com antecedência (ou programaticamente) para permitir a instalação automatizada usando estruturas de orquestração padrão. O StorageGRID fornece scripts Python opcionais para automatizar a configuração de dispositivos StorageGRID e todo o sistema StorageGRID (a "grade"). Você pode usar esses scripts diretamente ou inspecioná-los para saber como usar a API REST de instalação do StorageGRID nas ferramentas de implantação e configuração de grade que você mesmo desenvolve.

Automatize a instalação e a configuração do serviço de host StorageGRID

É possível automatizar a instalação do serviço de host StorageGRID usando estruturas de orquestração padrão, como Ansible, Puppet, Chef, Fabric ou SaltStack.

O serviço de host StorageGRID é empacotado em um DEB e é conduzido por arquivos de configuração que podem ser preparados com antecedência (ou programaticamente) para habilitar a instalação automatizada. Se você já usa uma estrutura de orquestração padrão para instalar e configurar o Ubuntu ou Debian, adicionar StorageGRID aos seus playbooks ou receitas deve ser simples.

Você pode automatizar estas tarefas:

1. Instalando o Linux
2. Configurando o Linux
3. Configuração de interfaces de rede de host para atender aos requisitos do StorageGRID
4. Configuração do storage de host para atender aos requisitos do StorageGRID
5. Instalando o Docker
6. Instalar o serviço de host StorageGRID
7. Criando arquivos de configuração do nó StorageGRID em `/etc/storagegrid/nodes`
8. Validando arquivos de configuração de nó do StorageGRID
9. Iniciando o serviço de host do StorageGRID

Exemplo de função e manual de estratégia do Ansible

Exemplo de função do Ansible e manual de estratégia são fornecidos com o arquivo de instalação `/extras` na pasta. O manual de estratégia do Ansible mostra como a `storagegrid` função prepara os hosts e instala o StorageGRID nos servidores de destino. Você pode personalizar a função ou o manual de estratégia conforme necessário.

Automatize a configuração do StorageGRID

Depois de implantar os nós de grade, você pode automatizar a configuração do sistema StorageGRID.

Antes de começar

- Você sabe a localização dos seguintes arquivos do arquivo de instalação.

Nome do ficheiro	Descrição
configure-StorageGRID.py	Script Python usado para automatizar a configuração
configure-StorageGRID.sample.json	Exemplo de arquivo de configuração para uso com o script
configure-StorageGRID.blank.json	Arquivo de configuração em branco para uso com o script

- Criou um `configure-storagegrid.json` ficheiro de configuração. Para criar este ficheiro, pode modificar o ficheiro de configuração de exemplo (`configure-storagegrid.sample.json`) ou o ficheiro de configuração em branco (`configure-storagegrid.blank.json`).

Sobre esta tarefa

Você pode usar o `configure-storagegrid.py` script Python e o `configure-storagegrid.json` arquivo de configuração para automatizar a configuração do seu sistema StorageGRID.

> Você também pode configurar o sistema usando o Gerenciador de Grade ou a API de Instalação.

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Mude para o diretório onde você extraiu o arquivo de instalação.

   Por exemplo:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   ```
   `platform`onde está `debs`, `rpms`, `vsphere` ou .
   ```

3. Execute o script Python e use o arquivo de configuração que você criou.

   Por exemplo:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Resultado

Um arquivo do Pacote de recuperação `.zip` é gerado durante o processo de configuração e é baixado para o diretório onde você está executando o processo de instalação e configuração. Você deve fazer backup do arquivo do pacote de recuperação para que você possa recuperar o sistema StorageGRID se um ou mais nós de grade falhar. Por exemplo, copie-o para um local de rede seguro e de backup e para um local seguro de armazenamento em nuvem.

> 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.

Se você especificou que senhas aleatórias devem ser geradas, abra o `Passwords.txt` arquivo e procure as senhas necessárias para acessar seu sistema StorageGRID.

```
######################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

O sistema StorageGRID é instalado e configurado quando é apresentada uma mensagem de confirmação.

```
StorageGRID has been configured and installed.
```

Informações relacionadas

"API REST de instalação"

Implantar nós de grade virtual (Ubuntu ou Debian)

Crie arquivos de configuração de nó para implantações Ubuntu ou Debian

Os arquivos de configuração de nó são pequenos arquivos de texto que fornecem as informações que o serviço de host do StorageGRID precisa para iniciar um nó e conectá-lo à rede apropriada e bloquear recursos de armazenamento. Os arquivos de configuração de nós são usados para nós virtuais e não são usados para nós do dispositivo.

Local para arquivos de configuração de nó

Coloque o arquivo de configuração para cada nó do StorageGRID `/etc/storagegrid/nodes` no diretório no host onde o nó será executado. Por exemplo, se você planeja executar um nó de administrador, um nó de gateway e um nó de armazenamento no HostA, você deve colocar três arquivos de configuração de nó no `/etc/storagegrid/nodes` HostA.

Você pode criar os arquivos de configuração diretamente em cada host usando um editor de texto, como vim ou nano, ou você pode criá-los em outro lugar e movê-los para cada host.

Nomenclatura de arquivos de configuração de nó

Os nomes dos arquivos de configuração são significativos. O formato é `node-name.conf`, onde `node-name` é um nome atribuído ao nó. Esse nome aparece no Instalador do StorageGRID e é usado para operações de manutenção de nós, como a migração de nós.

Os nomes dos nós devem seguir estas regras:

- Deve ser único
- Deve começar com uma letra
- Pode conter os carateres De A a Z e de a a z
- Pode conter os números de 0 a 9
- Pode conter um ou mais hífens (-)
- Não deve ter mais de 32 carateres, não incluindo a `.conf` extensão

Quaisquer arquivos `/etc/storagegrid/nodes` que não sigam essas convenções de nomenclatura não serão analisados pelo serviço host.

Se você tiver uma topologia de vários locais planejada para sua grade, um esquema típico de nomes de nós pode ser:

```
site-nodetype-nodenumber.conf
```

Por exemplo, você pode usar `dc1-adm1.conf` para o primeiro nó de administrador no data center 1 e `dc2-sn3.conf` para o terceiro nó de storage no data center 2. No entanto, você pode usar qualquer esquema que desejar, desde que todos os nomes de nós sigam as regras de nomenclatura.

Conteúdo de um arquivo de configuração de nó

Um arquivo de configuração contém pares chave/valor, com uma chave e um valor por linha. Para cada par chave/valor, siga estas regras:

- A chave e o valor devem ser separados por um sinal igual (=) e espaço em branco opcional.
- As teclas não podem conter espaços.
- Os valores podem conter espaços incorporados.
- Qualquer espaço em branco à frente ou à direita é ignorado.

A tabela a seguir define os valores para todas as chaves suportadas. Cada chave tem uma das seguintes designações:

- **Obrigatório**: Necessário para cada nó ou para os tipos de nó especificados
- **Melhor prática**: Opcional, embora recomendado
- **Opcional**: Opcional para todos os nós

Teclas de rede Admin

ADMIN_IP

Valor	Designação
Rede de grade IPv4 endereço do nó de administração principal para a grade à qual esse nó pertence. Use o mesmo valor que você especificou para GRID_NETWORK_IP para o nó de grade com NODE_TYPE e ADMIN_ROLE. Se você omitir esse parâmetro, o nó tentará descobrir um nó Admin primário usando mDNS. "Como os nós de grade descobrem o nó de administração principal" **Nota**: Este valor é ignorado, e pode ser proibido, no nó Admin principal.	Prática recomendada

ADMIN_NETWORK_CONFIG

Valor	Designação
DHCP, ESTÁTICO OU DESATIVADO	Opcional

ADMIN_NETWORK_ESL

Valor	Designação
Lista de sub-redes separadas por vírgulas na notação CIDR à qual esse nó deve se comunicar usando o gateway de rede Admin. Exemplo: `172.16.0.0/21,172.17.0.0/21`	Opcional

ADMIN_NETWORK_GATEWAY

Valor	Designação

Endereço IPv4 do gateway de rede de administração local para este nó. Deve estar na sub-rede definida por ADMIN_network_IP e ADMIN_network_MASK. Este valor é ignorado para redes configuradas por DHCP.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Obrigatório se `ADMIN_NETWORK_ESL` for especificado. Opcional caso contrário.

ADMIN_NETWORK_IP

Valor	Designação

Endereço IPv4 deste nó na rede Admin. Esta chave só é necessária quando ADMIN_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessário quando ADMIN_NETWORK_CONFIG é ESTÁTICO.
	
	Opcional caso contrário.

ADMIN_NETWORK_MAC

Valor	Designação
O endereço MAC da interface de rede de administração no contentor. Este campo é opcional. Se omitido, um endereço MAC será gerado automaticamente. Deve ser 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: `b2:9c:02:c2:27:10`	Opcional

ADMIN_NETWORK_MASK

Valor	Designação

IPv4 máscara de rede para este nó, na rede Admin. Especifique esta chave quando ADMIN_NETWORK_CONFIG estiver ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessário se Admin_network_IP for especificado e ADMIN_network_CONFIG for ESTÁTICO.
	
	Opcional caso contrário.

ADMIN_NETWORK_MTU

Valor	Designação

A unidade de transmissão máxima (MTU) para este nó na rede Admin. Não especifique se ADMIN_NETWORK_CONFIG é DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 é usado.
 	
Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão.
 	
IMPORTANTE: O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.
 	
Exemplos:
 	
`1500`
 	
`8192`
	Opcional

ADMIN_NETWORK_TARGET

Valor	Designação

Nome do dispositivo host que você usará para acesso à rede de administração pelo nó StorageGRID. Apenas são suportados nomes de interface de rede. Normalmente, você usa um nome de interface diferente do que foi especificado para GRID_NETWORK_TARGET ou CLIENT_network_TARGET.
 	
Nota: Não use dispositivos bond ou bridge como destino de rede. Configure uma VLAN (ou outra interface virtual) em cima do dispositivo de ligação ou use um par bridge e Ethernet virtual (vete).
 	
Prática recomendada:Especifique um valor mesmo que este nó não tenha inicialmente um endereço IP de rede Admin. Em seguida, você pode adicionar um endereço IP de rede Admin mais tarde, sem ter que reconfigurar o nó no host.
 	
Exemplos:
 	
`bond0.1002`
 	
`ens256`
	Prática recomendada

ADMIN_NETWORK_TARGET_TYPE

Valor	Designação
Interface (este é o único valor suportado.)	Opcional

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou Falso Defina a chave como "true" para fazer com que o contentor StorageGRID use o endereço MAC da interface de destino do host na rede de administração. **Prática recomendada:** em redes onde o modo promíscuo seria necessário, use a chave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC em vez disso. Para obter mais detalhes sobre clonagem MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Prática recomendada

ADMIN_ROLE

Valor	Designação
Primário ou não primário Esta chave só é necessária quando NODE_TYPE: VM_Admin_Node; não a especifique para outros tipos de nó.	Obrigatório quando NODE_TYPE é VM_Admin_Node Opcional caso contrário.

Bloquear chaves de dispositivo

BLOCK_DEVICE_AUDIT_LOGS

Valor	Designação

Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento persistente de logs de auditoria.
 	
Exemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	Necessário para nós com NODE_TYPE: VM_Admin_Node. Não o especifique para outros tipos de nó.

BLOCK_DEVICE_RANGEDB_NNN

Valor	Designação

Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento de objetos persistente. Esta chave é necessária apenas para nós com NODE_TYPE: VM_Storage_Node; não a especifique para outros tipos de nó.
 	
Somente block_DEVICE_RANGEDB_000 é necessário; o resto é opcional. O dispositivo de bloco especificado para block_DEVICE_RANGEDB_000 deve ter pelo menos 4 TB; os outros podem ser menores.
 	
Não deixe lacunas. Se você especificar block_DEVICE_RANGEDB_005, você também deve especificar BLOCK_DEVICE_RANGEDB_004.
 	
Nota: Para compatibilidade com implantações existentes, chaves de dois dígitos são suportadas para nós atualizados.
 	
Exemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	Obrigatório:
	
	BLOCK_DEVICE_RANGEDB_000
	
	Opcional:
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

BLOCK_DEVICE_TABLES

Valor	Designação

Caminho e nome do arquivo especial do dispositivo de bloco este nó usará para armazenamento persistente de tabelas de banco de dados. Esta chave é necessária apenas para nós com NODE_TYPE: VM_Admin_Node; não a especifique para outros tipos de nó.
 	
Exemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	Obrigatório

BLOCK_DEVICE_VAR_LOCAL

Valor	Designação

Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para seu `/var/local` armazenamento persistente.
 	
Exemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	Obrigatório

Chaves da rede do cliente

CLIENT_NETWORK_CONFIG

Valor	Designação
DHCP, ESTÁTICO OU DESATIVADO	Opcional

CLIENT_NETWORK_GATEWAY

Valor	Designação

Endereço IPv4 do gateway de rede de cliente local para este nó, que deve estar na sub-rede definida por CLIENT_network_IP e CLIENT_network_MASK. Este valor é ignorado para redes configuradas por DHCP.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Opcional

CLIENT_NETWORK_IP

Valor	Designação

Endereço IPv4 deste nó na rede do cliente.
 	
Esta chave só é necessária quando CLIENT_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessário quando CLIENT_NETWORK_CONFIG é ESTÁTICO
	
	Opcional caso contrário.

CLIENT_NETWORK_MAC

Valor	Designação
O endereço MAC da interface de rede do cliente no contentor. Este campo é opcional. Se omitido, um endereço MAC será gerado automaticamente. Deve ser 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: `b2:9c:02:c2:27:20`	Opcional

CLIENT_NETWORK_MASK

Valor	Designação

IPv4 máscara de rede para este nó na rede do cliente.
 	
Especifique esta chave quando CLIENT_NETWORK_CONFIG for STATIC; não a especifique para outros valores.
 	
Exemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessário se CLIENT_network_IP for especificado e CLIENT_network_CONFIG for ESTÁTICO
	
	Opcional caso contrário.

CLIENT_NETWORK_MTU

Valor	Designação

A unidade de transmissão máxima (MTU) para este nó na rede do cliente. Não especifique se CLIENT_NETWORK_CONFIG é DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 é usado.
 	
Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão.
 	
IMPORTANTE: O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.
 	
Exemplos:
 	
`1500`
 	
`8192`
	Opcional

CLIENT_NETWORK_TARGET

Valor	Designação

Nome do dispositivo host que você usará para acesso à rede do cliente pelo nó StorageGRID. Apenas são suportados nomes de interface de rede. Normalmente, você usa um nome de interface diferente do que foi especificado para GRID_Network_TARGET ou ADMIN_network_TARGET.
 	
Nota: Não use dispositivos bond ou bridge como destino de rede. Configure uma VLAN (ou outra interface virtual) em cima do dispositivo de ligação ou use um par bridge e Ethernet virtual (vete).
 	
Prática recomendada: Especifique um valor mesmo que este nó não tenha inicialmente um endereço IP de rede do cliente. Em seguida, você pode adicionar um endereço IP da rede do cliente mais tarde, sem ter que reconfigurar o nó no host.
 	
Exemplos:
 	
`bond0.1003`
 	
`ens423`
	Prática recomendada

CLIENT_NETWORK_TARGET_TYPE

Valor	Designação
Interface (este é apenas o valor suportado.)	Opcional

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou Falso Defina a chave como "true" para fazer com que o contentor StorageGRID use o endereço MAC da interface de destino do host na rede do cliente. **Melhor prática:** em redes onde o modo promíscuo seria necessário, use a chave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC em vez disso. Para obter mais detalhes sobre clonagem MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Prática recomendada

Chaves de rede de grade

GRID_NETWORK_CONFIG

Valor	Designação
ESTÁTICO ou DHCP O padrão é ESTÁTICO se não for especificado.	Prática recomendada

GRID_NETWORK_GATEWAY

Valor	Designação
Endereço IPv4 do gateway de rede local para este nó, que deve estar na sub-rede definida por GRID_Network_IP e GRID_NETWORK_MASK. Este valor é ignorado para redes configuradas por DHCP. Se a rede de Grade for uma única sub-rede sem gateway, use o endereço de gateway padrão para a sub-rede (X.Y.z.1) ou o valor GRID_Network_IP deste nó; qualquer valor simplificará expansões futuras de rede de Grade.	Obrigatório

GRID_NETWORK_IP

Valor	Designação

Endereço IPv4 deste nó na rede de Grade. Esta chave só é necessária quando GRID_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necessário quando GRID_NETWORK_CONFIG é ESTÁTICO
	
	Opcional caso contrário.

GRID_NETWORK_MAC

Valor	Designação
O endereço MAC da interface Grid Network no contentor. Deve ser 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: `b2:9c:02:c2:27:30`	Opcional Se omitido, um endereço MAC será gerado automaticamente.

GRID_NETWORK_MASK

Valor	Designação

IPv4 máscara de rede para este nó na rede de Grade. Especifique esta chave quando GRID_NETWORK_CONFIG estiver ESTÁTICA; não a especifique para outros valores.
 	
Exemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necessário quando GRID_Network_IP é especificado e GRID_NETWORK_CONFIG é ESTÁTICO.
	
	Opcional caso contrário.

GRID_NETWORK_MTU

Valor	Designação

A unidade de transmissão máxima (MTU) para este nó na rede de Grade. Não especifique se GRID_NETWORK_CONFIG é DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 é usado.
 	
Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão.
 	
IMPORTANTE: O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.
 	
IMPORTANTE: Para obter o melhor desempenho da rede, todos os nós devem ser configurados com valores MTU semelhantes em suas interfaces Grid Network. 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.
 	
Exemplos:
 	
`1500`
 	
`8192`
	Opcional

GRID_NETWORK_TARGET

Valor	Designação

Nome do dispositivo host que você usará para acesso à rede de Grade pelo nó StorageGRID. Apenas são suportados nomes de interface de rede. Normalmente, você usa um nome de interface diferente do que foi especificado para ADMIN_NETWORK_TARGET ou CLIENT_network_TARGET.
 	
Nota: Não use dispositivos bond ou bridge como destino de rede. Configure uma VLAN (ou outra interface virtual) em cima do dispositivo de ligação ou use um par bridge e Ethernet virtual (vete).
 	
Exemplos:
 	
`bond0.1001`
 	
`ens192`
	Obrigatório

GRID_NETWORK_TARGET_TYPE

Valor	Designação
Interface (este é o único valor suportado.)	Opcional

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou Falso Defina o valor da chave como "true" para fazer com que o contentor StorageGRID use o endereço MAC da interface de destino do host na rede de Grade. **Melhor prática:** em redes onde o modo promíscuo seria necessário, use a chave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC em vez disso. Para obter mais detalhes sobre clonagem MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Prática recomendada

Chave de senha de instalação (temporária)

CUSTOM_TEMPORARY_PASSWORD_HASH

Valor	Designação
Para o nó de administração principal, defina uma senha temporária padrão para a API de instalação do StorageGRID durante a instalação. **Nota**: Defina uma senha de instalação somente no nó Admin principal. Se você tentar definir uma senha em outro tipo de nó, a validação do arquivo de configuração do nó falhará. Definir este valor não tem efeito quando a instalação estiver concluída. Se esta chave for omitida, por padrão nenhuma senha temporária será definida. Como alternativa, você pode definir uma senha temporária usando a API de instalação do StorageGRID. Deve ser um `crypt()` hash de senha SHA-512 com formato `$6$<salt>$<password hash>` para uma senha de pelo menos 8 e não mais de 32 carateres. Esse hash pode ser gerado usando ferramentas CLI, como o `openssl passwd` comando no modo SHA-512.	Prática recomendada

Chave de interfaces

Interface_TARGET_nnnn

Valor	Designação
Nome e descrição opcional para uma interface extra que você deseja adicionar a este nó. Você pode adicionar várias interfaces extras a cada nó. Para *nnnnn*, especifique um número exclusivo para cada entrada INTERFACE_TARGET que você está adicionando. Para o valor, 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. Exemplo: `INTERFACE_TARGET_0001=ens256, Trunk` 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.	Opcional

Tecla RAM máxima

MÁXIMO_RAM

Valor	Designação

A quantidade máxima de RAM que este nó pode consumir. Se esta chave for omitida, o nó não tem restrições de memória. Ao definir este campo para um nó de nível de produção, especifique um valor que seja pelo menos 24 GB e 16 a 32 GB menor que a RAM total do sistema.
 	
Nota: O valor da RAM afeta o espaço reservado de metadados real de um nó. Consulte "Descrição do que é Metadata Reserved Space".
 	
O formato deste campo é *`numberunit`*, onde *`unit`* pode ser `b`, `k`, , `m` `g` ou .
 	
Exemplos:
 	
`24g`
 	
`38654705664b`
 	
Nota: Se você quiser usar essa opção, você deve habilitar o suporte do kernel para cgroups de memória.
	Opcional

Chaves de tipo de nó

NODE_TYPE (TIPO DE NÓ)

Valor	Designação
Tipo de nó: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway	Obrigatório

TIPO_ARMAZENAMENTO

Valor	Designação
Define o tipo de objetos que um nó de storage contém. Para obter mais informações, "Tipos de nós de storage"consulte . Esta chave é necessária apenas para nós com NODE_TYPE: VM_Storage_Node; não a especifique para outros tipos de nó. Tipos de armazenamento: • combinado • dados • metadados **Nota**: Se o STORAGE_TYPE não for especificado, o tipo Storage Node é definido como combinado (dados e metadados) por padrão.	Opcional

Teclas de remapeamento de portas

PORT_REMAP

Valor	Designação
Remapeia qualquer porta usada por um nó para comunicações internas de nó de grade ou comunicações externas. O remapeamento de portas é necessário se as políticas de rede empresarial restringirem uma ou mais portas usadas pelo StorageGRID, conforme descrito em "Comunicações internas do nó da grade" ou "Comunicações externas". **IMPORTANTE**: Não remapegue as portas que você está planejando usar para configurar pontos de extremidade do balanceador de carga. **Nota**: Se apenas PORT_REMAP estiver definido, o mapeamento especificado será usado para comunicações de entrada e saída. Se Port_REMAP_INBOUND também for especificado, PORT_REMAP se aplica apenas às comunicações de saída. O formato usado é: *`network type/protocol/default port used by grid node/new port`*, Onde *`network type`* está grade, admin ou cliente e *`protocol`* é tcp ou udp. Exemplo: `PORT_REMAP = client/tcp/18082/443` Você também pode remapear várias portas usando uma lista separada por vírgulas. Exemplo: `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	Opcional

PORT_REMAP_INBOUND

Valor	Designação
Remapeia as comunicações de entrada para a porta especificada. Se você especificar PORT_REMAP_INBOUND, mas não especificar um valor para PORT_REMAP, as comunicações de saída para a porta não serão alteradas. **IMPORTANTE**: Não remapegue as portas que você está planejando usar para configurar pontos de extremidade do balanceador de carga. O formato usado é: *`network type/protocol/remapped port /default port used by grid node`*, Onde *`network type`* está grade, admin ou cliente e *`protocol`* é tcp ou udp. Exemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22` Você também pode remapear várias portas de entrada usando uma lista separada por vírgulas. Exemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	Opcional

Como os nós de grade descobrem o nó de administração principal

Os nós de grade se comunicam com o nó de administração principal para configuração e gerenciamento. Cada nó de grade deve saber o endereço IP do nó de administração principal na rede de grade.

Para garantir que um nó de grade possa acessar o nó Admin principal, você pode fazer um dos seguintes procedimentos ao implantar o nó:

- Você pode usar o parâmetro Admin_IP para inserir o endereço IP do nó de administrador principal manualmente.
- Você pode omitir o parâmetro ADMIN_IP para que o nó de grade descubra o valor automaticamente. A deteção automática é especialmente útil quando a rede de Grade usa DHCP para atribuir o endereço IP ao nó Admin principal.

A deteção automática do nó de administração principal é realizada usando um sistema de nome de domínio multicast (mDNS). Quando o nó de administração principal é iniciado pela primeira vez, ele publica seu endereço IP usando mDNS. Outros nós na mesma sub-rede podem então consultar o endereço IP e adquiri-lo automaticamente. No entanto, como o tráfego IP multicast não é normalmente roteável entre sub-redes, os nós em outras sub-redes não podem adquirir o endereço IP do nó de administração principal diretamente.

Se utilizar a deteção automática:

- Você deve incluir a configuração Admin_IP para pelo menos um nó de grade em todas as sub-redes às quais o nó Admin principal não esteja diretamente conetado. Esse nó de grade publicará o endereço IP do nó de administrador principal para outros nós na sub-rede para serem detetados com mDNS.
- Certifique-se de que a sua infra-estrutura de rede suporta a passagem de tráfego IP multi-cast dentro de uma sub-rede.

Exemplo de arquivos de configuração de nó

Você pode usar os arquivos de configuração de nó de exemplo para ajudar a configurar os arquivos de configuração de nó para o seu sistema StorageGRID. Os exemplos mostram arquivos de configuração de nós para todos os tipos de nós de grade.

Para a maioria dos nós, você pode adicionar informações de endereçamento de rede de administrador e cliente (IP, máscara, gateway, etc.) ao configurar a grade usando o Gerenciador de Grade ou a API de instalação. A exceção é o nó de administração principal. Se você quiser navegar até o IP de rede Admin do nó de administração principal para concluir a configuração da grade (porque a rede de grade não está roteada, por exemplo), você deve configurar a conexão de rede Admin para o nó de administração principal em seu arquivo de configuração de nó. Isso é mostrado no exemplo.

Nos exemplos, o destino rede cliente foi configurado como uma prática recomendada, mesmo que a rede cliente esteja desativada por padrão.

Exemplo para nó de administração principal

- Exemplo de nome de arquivo*: `/etc/storagegrid/nodes/dc1-adm1.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Exemplo para nó de storage

- Exemplo de nome do arquivo:* `/etc/storagegrid/nodes/dc1-sn1.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-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
```

Exemplo para Gateway Node

- Exemplo de nome do arquivo:* `/etc/storagegrid/nodes/dc1-gw1.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemplo para um nó de administração não primário

- Exemplo de nome do arquivo:* `/etc/storagegrid/nodes/dc1-adm2.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Valide a configuração do StorageGRID

Depois de criar arquivos de configuração `/etc/storagegrid/nodes` para cada um dos nós do StorageGRID, você deve validar o conteúdo desses arquivos.

Para validar o conteúdo dos arquivos de configuração, execute o seguinte comando em cada host:

```
sudo storagegrid node validate all
```

Se os arquivos estiverem corretos, a saída mostra **PASSADO** para cada arquivo de configuração, como mostrado no exemplo.

Ao usar apenas um LUN em nós somente metadados, você pode receber uma mensagem de aviso que pode ser ignorada.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Para uma instalação automatizada, pode suprimir esta saída utilizando as `-q` opções ou `--quiet` do `storagegrid` comando (por exemplo, `storagegrid --quiet…`). Se você suprimir a saída, o comando terá um valor de saída não zero se quaisquer avisos de configuração ou erros foram detetados.

Se os arquivos de configuração estiverem incorretos, os problemas serão exibidos como **AVISO** e **ERRO**, conforme mostrado no exemplo. Se forem encontrados quaisquer erros de configuração, é necessário corrigi-

los antes de continuar com a instalação.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Inicie o serviço de host do 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.

Passos

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
```

3. Se qualquer nó retornar um status de "não está em execução" ou "parado", execute o seguinte comando:

```
sudo storagegrid node start node-name
```

4. 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
```

Configurar grade e instalação completa (Ubuntu ou Debian)

Navegue até o Gerenciador de Grade

Use o Gerenciador de Grade para definir todas as informações necessárias para configurar o sistema StorageGRID.

Antes de começar

O nó Admin principal deve ser implantado e ter concluído a sequência inicial de inicialização.

Passos

1. Abra o navegador da Web e navegue até:

   `https://primary_admin_node_ip`

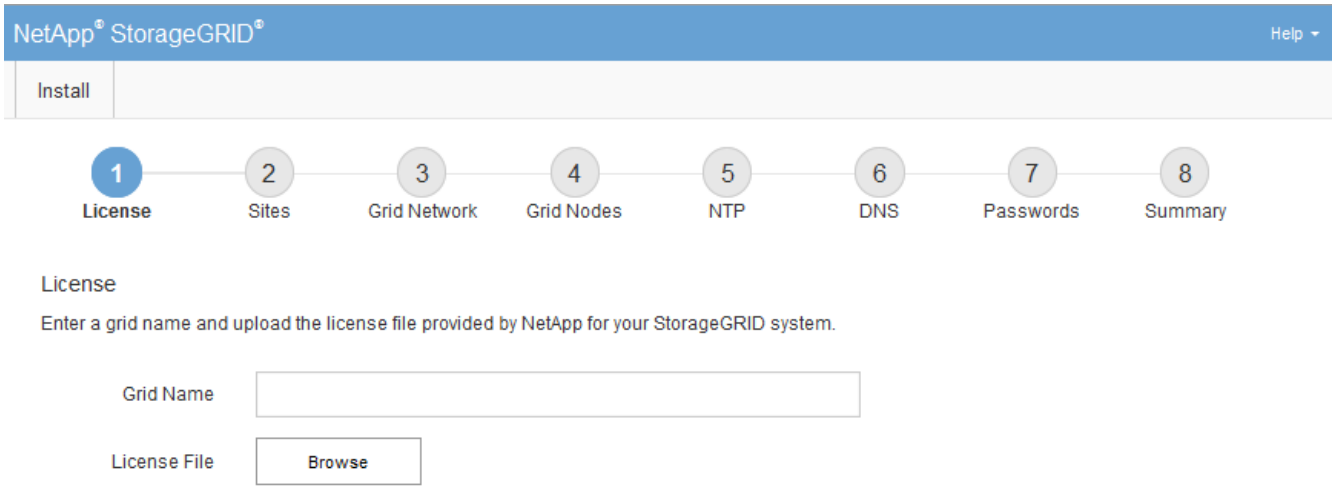
   Como alternativa, você pode acessar o Gerenciador de Grade na porta 8443:

   `https://primary_admin_node_ip:8443`

   Você pode usar o endereço IP do nó de administrador principal IP na rede de grade ou na rede de administração, conforme apropriado para a configuração da rede.

2. Gerencie uma senha temporária do instalador conforme necessário:
   - Se já tiver sido definida uma palavra-passe utilizando um destes métodos, introduza a palavra-passe para prosseguir.
     - Um usuário define a senha ao acessar o instalador anteriormente
     - A senha foi importada automaticamente do arquivo de configuração do nó em `/etc/storagegrid/nodes/<node_name>.conf`
   - Se não tiver sido definida uma palavra-passe, defina opcionalmente uma palavra-passe para proteger o instalador do StorageGRID.
3. Selecione **Instalar um sistema StorageGRID**.

É apresentada a página utilizada para configurar um sistema StorageGRID.



Especifique as informações da licença do StorageGRID

Você deve especificar o nome do seu sistema StorageGRID e fazer o upload do arquivo de licença fornecido pelo NetApp.

Passos

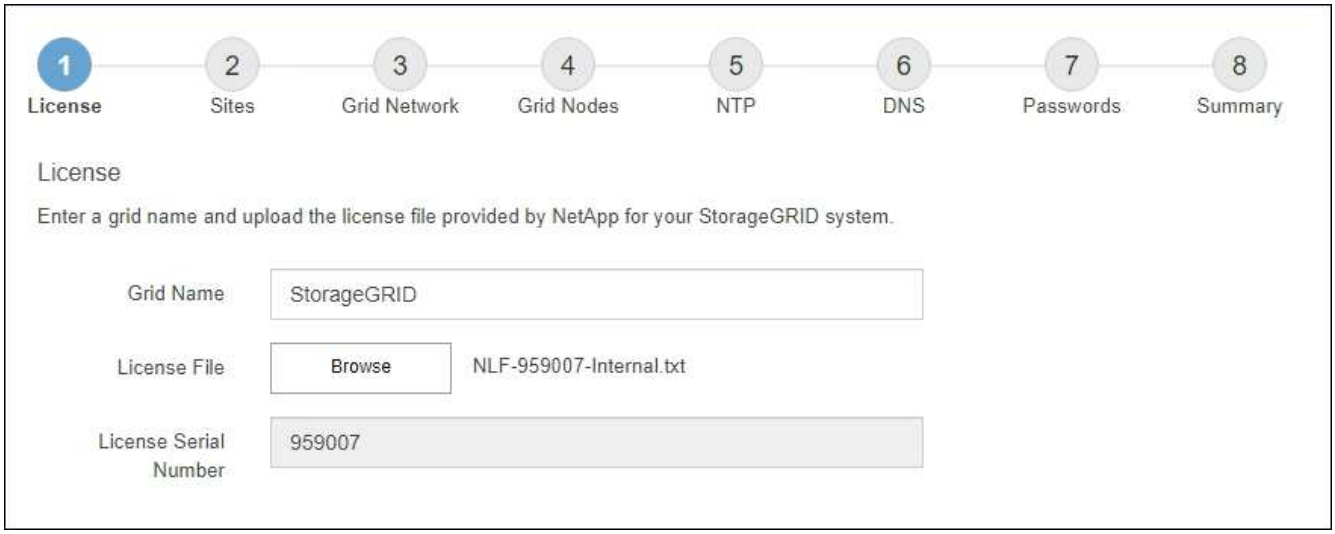
1. Na página Licença, insira um nome significativo para o seu sistema StorageGRID no campo **Nome da Grade**.

   Após a instalação, o nome é exibido na parte superior do menu nós.

2. Selecione **Procurar**, localize o ficheiro de licença NetApp (`NLF-unique-id.txt`) e selecione **abrir**.

   O ficheiro de licença é validado e o número de série é apresentado.

   > O arquivo de instalação do StorageGRID inclui uma licença gratuita que não fornece nenhum direito de suporte para o produto. Você pode atualizar para uma licença que oferece suporte após a instalação.



3. Selecione **seguinte**.

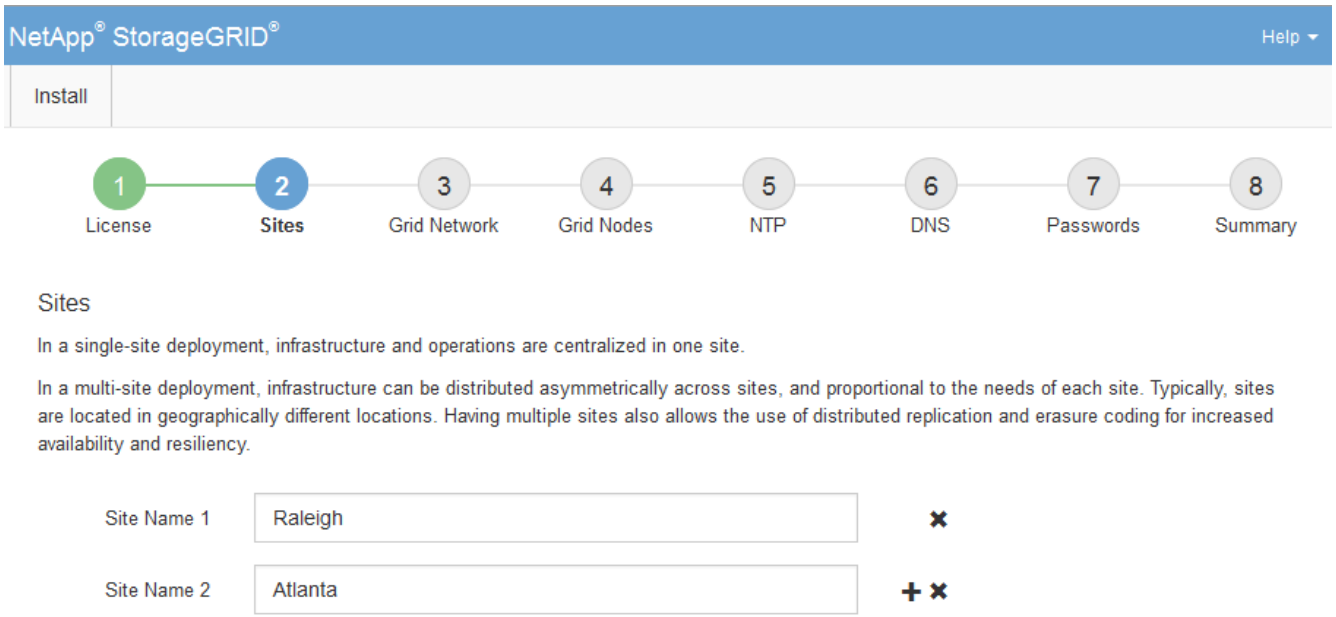
Adicione sites

Você deve criar pelo menos um site quando estiver instalando o StorageGRID. Você pode criar sites adicionais para aumentar a confiabilidade e a capacidade de storage do seu sistema StorageGRID.

Passos

1. Na página Sites, insira o **Nome do Site**.
2. Para adicionar sites adicionais, clique no sinal de adição ao lado da última entrada do site e digite o nome na nova caixa de texto **Nome do site**.

   Adicione tantos locais adicionais quanto necessário para a topologia da grade. Você pode adicionar até 16 sites.



3. Clique em **seguinte**.

Especifique as sub-redes da rede de Grade

Você deve especificar as sub-redes que são usadas na rede de Grade.

Sobre esta tarefa

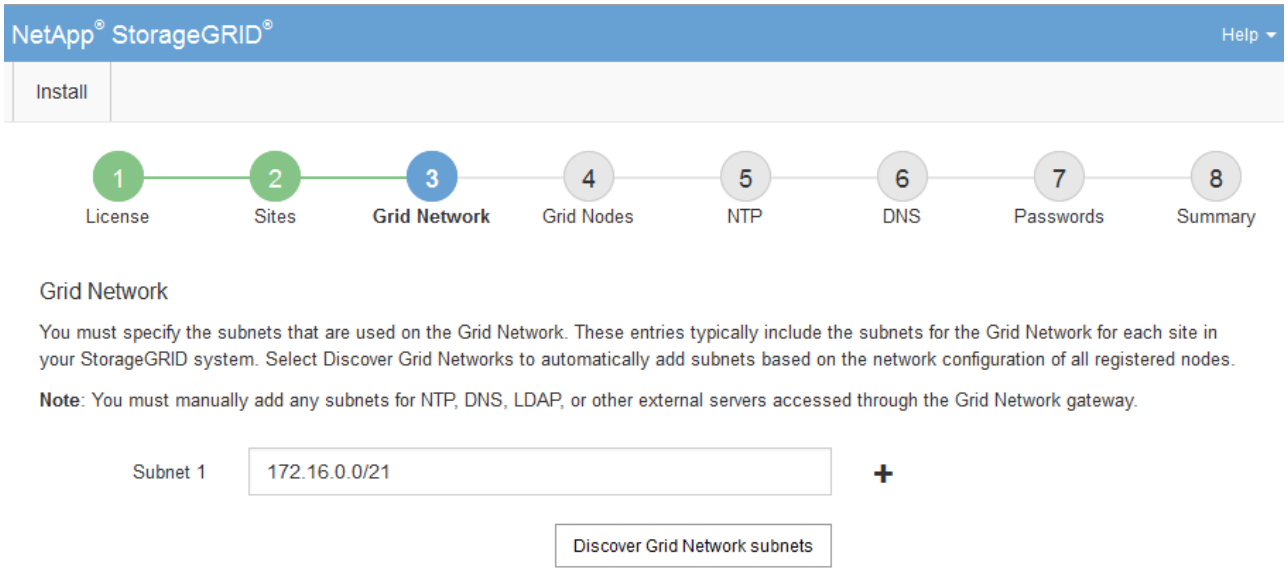
As entradas de sub-rede incluem as sub-redes para a rede de Grade para cada site no seu sistema StorageGRID, juntamente com quaisquer sub-redes que precisam ser acessíveis através da rede de Grade.

Se você tiver várias sub-redes de grade, o gateway de rede de grade é necessário. Todas as sub-redes de grade especificadas devem ser acessíveis através deste gateway.

Passos

1. Especifique o endereço de rede CIDR para pelo menos uma rede de Grade na caixa de texto **Subnet 1**.
2. Clique no sinal de mais ao lado da última entrada para adicionar uma entrada de rede adicional. Você deve especificar todas as sub-redes para todos os sites na rede de Grade.

- Se você já implantou pelo menos um nó, clique em **descobrir sub-redes de redes de Grade** para preencher automaticamente a Lista de sub-redes de rede de Grade com as sub-redes relatadas pelos nós de grade que se registraram no Gerenciador de Grade.
- Você deve adicionar manualmente quaisquer sub-redes para NTP, DNS, LDAP ou outros servidores externos acessados através do gateway de rede de Grade.



3. Clique em **seguinte**.

Aprovar nós de grade pendentes

Você deve aprovar cada nó de grade antes que ele possa ingressar no sistema StorageGRID.

Antes de começar

Você implantou todos os nós de grade de dispositivos virtuais e StorageGRID.

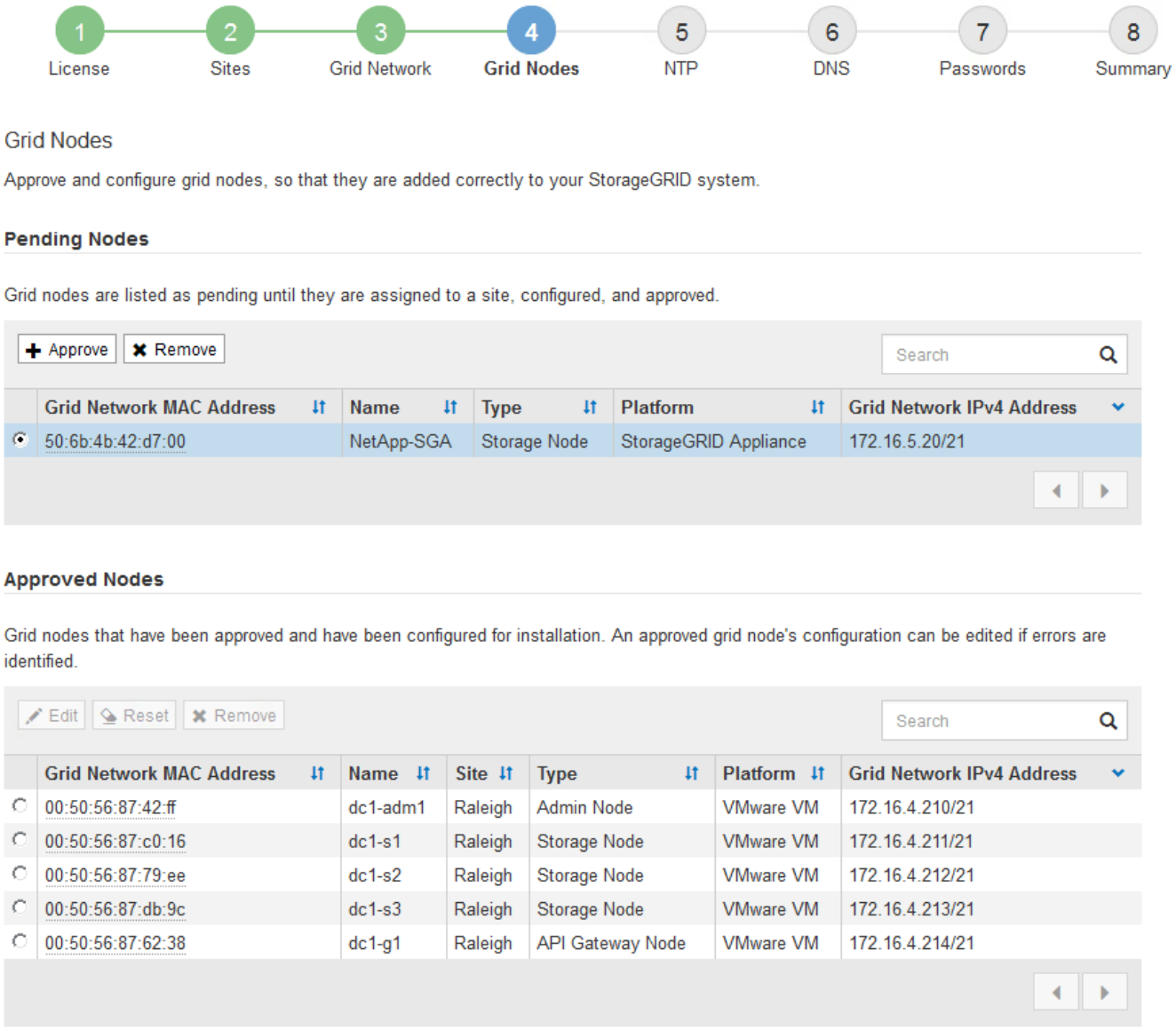
> É mais eficiente executar uma única instalação de todos os nós, em vez de instalar alguns nós agora e alguns nós depois.

Passos

1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade implantados.

> Se um nó de grade estiver ausente, confirme que ele foi implantado com sucesso e que tem o IP de rede de grade correto do nó de administrador principal definido para ADMIN_IP.

2. Selecione o botão de opção ao lado de um nó pendente que você deseja aprovar.



3. Clique em **Approve**.
4. Em Configurações gerais, modifique as configurações para as seguintes propriedades, conforme necessário:
   - **Site**: O nome do sistema do site para este nó de grade.
   - **Nome**: O nome do sistema para o nó. O nome padrão é o nome que você especificou quando configurou o nó.

     Os nomes de sistema são necessários para operações internas do StorageGRID e não podem ser alterados após a conclusão da instalação. No entanto, durante esta etapa do processo de instalação, você pode alterar os nomes do sistema conforme necessário.

   - **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.

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.

- * Tipo de armazenamento* (somente nós de armazenamento): Especifique que um novo nó de armazenamento seja usado exclusivamente para dados, somente metadados ou ambos. As opções são **dados e metadados** ("combinados"), **somente dados** e **somente metadados**.

  "Tipos de nós de storage"Consulte para obter informações sobre os requisitos para esses tipos de nós.

- **ADC Service** (somente nós de armazenamento): Selecione **Automático** para permitir que o sistema determine se o nó requer 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. Não é possível adicionar o serviço ADC a um nó depois que ele é implantado.

5. Na rede de Grade, modifique as configurações para as seguintes propriedades, conforme necessário:

   - **Endereço IPv4 (CIDR)**: O endereço de rede CIDR para a interface Grid Network (eth0 dentro do contentor). Por exemplo: 192.168.1.234/21
   - **Gateway**: O gateway Grid Network. Por exemplo: 192.168.0.1

     O gateway é necessário se houver várias sub-redes de grade.

   Se você selecionou DHCP para a configuração da rede de Grade e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

6. Se pretender configurar a rede de administração para o nó da grelha, adicione ou atualize as definições na secção rede de administração, conforme necessário.

   Insira as sub-redes de destino das rotas fora desta interface na caixa de texto **sub-redes (CIDR)**. Se houver várias sub-redes Admin, o gateway Admin é necessário.

   Se você selecionou DHCP para a configuração da rede Admin e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

   Appliances: para um appliance StorageGRID, se a rede de administração não tiver sido configurada durante a instalação inicial usando o Instalador de appliance StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

   a. Reinicie o aparelho: No Instalador de dispositivos, selecione **Avançado** > **Reiniciar**.

      A reinicialização pode levar vários minutos.

   b. Selecione **Configure Networking** > **Link Configuration** e ative as redes apropriadas.
   c. Selecione **Configurar rede** > **Configuração IP** e configure as redes ativadas.
   d. Volte à página inicial e clique em **Iniciar instalação**.

e. No Gerenciador de Grade: Se o nó estiver listado na tabela de nós aprovados, remova o nó.

f. Remova o nó da tabela nós pendentes.

g. Aguarde que o nó reapareça na lista de nós pendentes.

h. Confirme se você pode configurar as redes apropriadas. Eles já devem ser preenchidos com as informações fornecidas na página Configuração IP do Instalador de dispositivos.

   Para obter informações adicionais, consulte o "Início rápido para instalação de hardware" para localizar as instruções do seu aparelho.

7. Se pretender configurar a rede do cliente para o nó da grelha, adicione ou atualize as definições na secção rede do cliente, conforme necessário. Se a rede do cliente estiver configurada, o gateway é necessário e ele se torna o gateway padrão para o nó após a instalação.

   > Se você selecionou DHCP para a configuração da rede do cliente e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

   Appliances: para um appliance StorageGRID, se a rede cliente não tiver sido configurada durante a instalação inicial usando o Instalador de appliance StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

   a. Reinicie o aparelho: No Instalador de dispositivos, selecione **Avançado** > **Reiniciar**.

      A reinicialização pode levar vários minutos.

   b. Selecione **Configure Networking** > **Link Configuration** e ative as redes apropriadas.

   c. Selecione **Configurar rede** > **Configuração IP** e configure as redes ativadas.

   d. Volte à página inicial e clique em **Iniciar instalação**.

   e. No Gerenciador de Grade: Se o nó estiver listado na tabela de nós aprovados, remova o nó.

   f. Remova o nó da tabela nós pendentes.

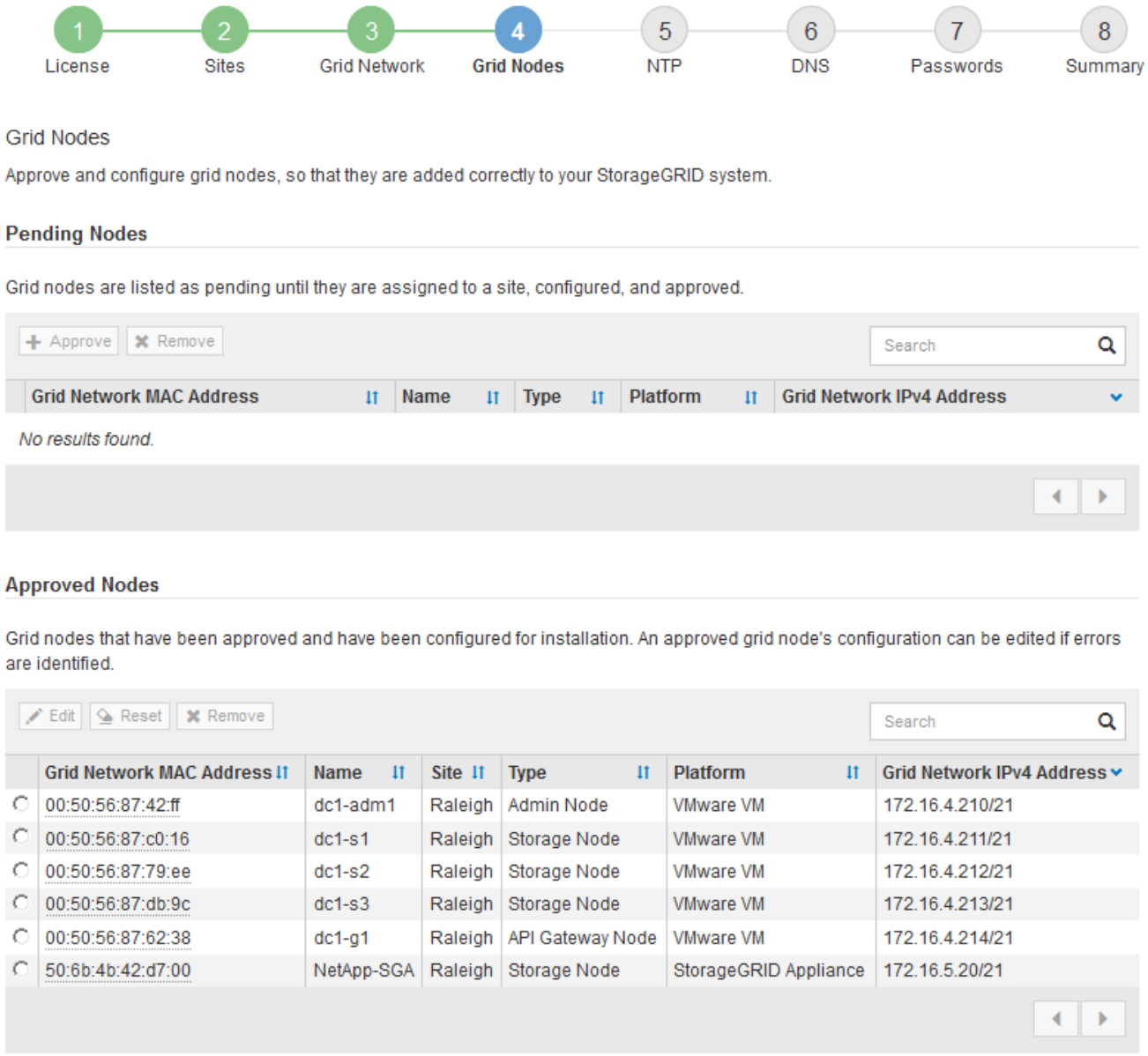
   g. Aguarde que o nó reapareça na lista de nós pendentes.

   h. Confirme se você pode configurar as redes apropriadas. Eles já devem ser preenchidos com as informações fornecidas na página Configuração IP do Instalador de dispositivos.

      Para saber como instalar dispositivos StorageGRID, consulte "Início rápido para instalação de hardware" para localizar as instruções do seu aparelho.

8. Clique em **Salvar**.

   A entrada do nó de grade se move para a lista de nós aprovados.



9. Repita estas etapas para cada nó de grade pendente que você deseja aprovar.

   Você deve aprovar todos os nós que deseja na grade. No entanto, você pode retornar a esta página a qualquer momento antes de clicar em **Instalar** na página Resumo. Você pode modificar as propriedades de um nó de grade aprovado selecionando seu botão de opção e clicando em **Editar**.

10. Quando terminar de aprovar nós de grade, clique em **Next**.

Especifique as informações do servidor Network Time Protocol

Você deve especificar as informações de configuração do protocolo de tempo de rede (NTP) para o sistema StorageGRID, para que as operações executadas em servidores separados possam ser mantidas sincronizadas.

Sobre esta tarefa

Você deve especificar endereços IPv4 para os servidores NTP.

Tem de especificar servidores NTP externos. Os servidores NTP especificados devem usar o protocolo NTP.

Você deve especificar quatro referências de servidor NTP do estrato 3 ou melhor para evitar problemas com a deriva de tempo.

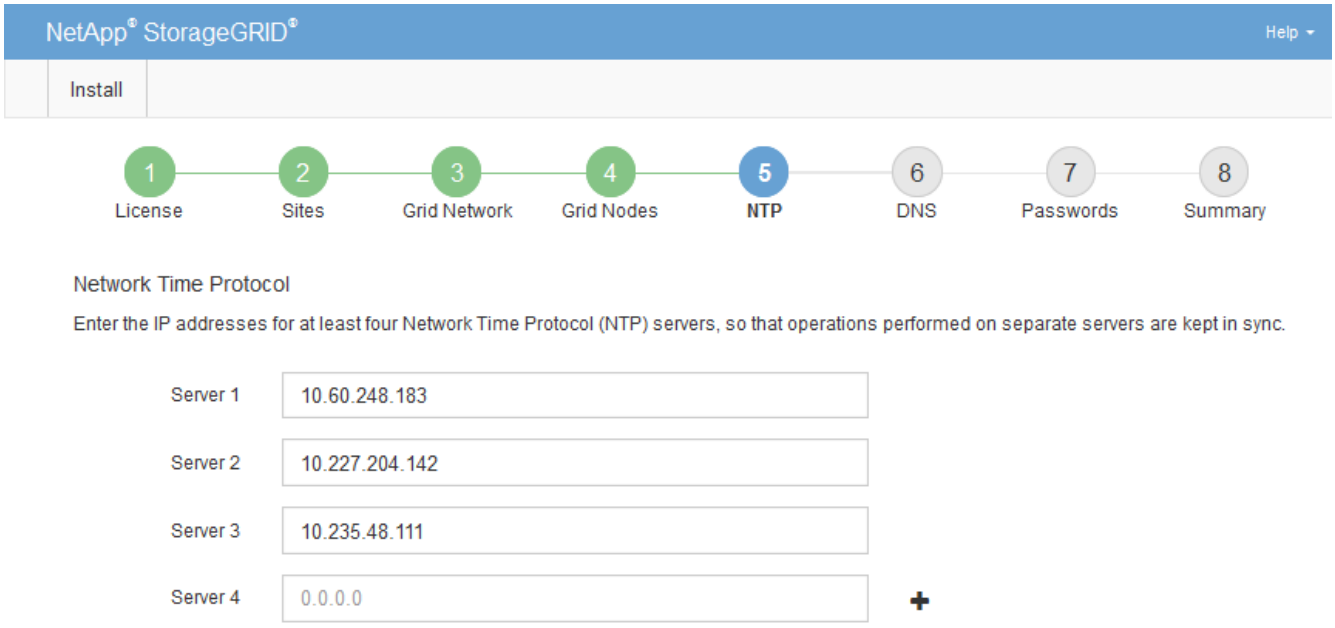
> Ao especificar a fonte NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft 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"

Os servidores NTP externos são usados pelos nós aos quais você atribuiu funções primárias NTP anteriormente.

> 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.

Passos

1. Especifique os endereços IPv4 para pelo menos quatro servidores NTP nas caixas de texto **Server 1** para **Server 4**.
2. Se necessário, selecione o sinal de adição ao lado da última entrada para adicionar entradas adicionais do servidor.



3. Selecione **seguinte**.

Informações relacionadas

"Diretrizes de rede"

Especifique as informações do servidor DNS

Você deve especificar informações de DNS para seu sistema StorageGRID, para que você possa acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

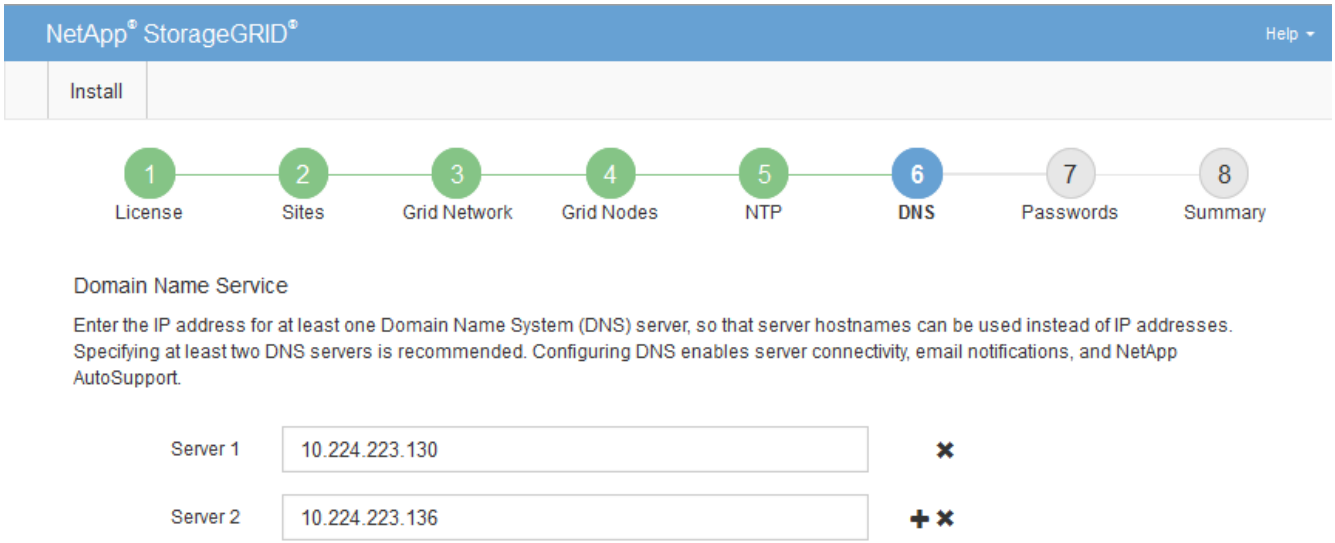
Especificar "Informações do servidor DNS" permite que você use nomes de host de nome de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações de e-mail e AutoSupport.

Para garantir o funcionamento correto, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três serão usados por causa das limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, pode "Personalize a lista de servidores DNS"usar um conjunto diferente de até três servidores DNS para nós individuais (normalmente todos os nós em um site).

Se possível, use servidores DNS que cada site pode acessar localmente para garantir que um site islanded possa resolver os FQDNs para destinos externos.

Passos

1. Especifique o endereço IPv4 para pelo menos um servidor DNS na caixa de texto **Server 1**.
2. Se necessário, selecione o sinal de adição ao lado da última entrada para adicionar entradas adicionais do servidor.



   A prática recomendada é especificar pelo menos dois servidores DNS. Você pode especificar até seis servidores DNS.

3. Selecione **seguinte**.

Especifique as senhas do sistema StorageGRID

Como parte da instalação do sistema StorageGRID, você precisa inserir as senhas a serem usadas para proteger o sistema e executar tarefas de manutenção.

Sobre esta tarefa

Use a página Instalar senhas para especificar a senha de provisionamento e a senha de usuário raiz de gerenciamento de grade.

- A senha de provisionamento é usada como uma chave de criptografia e não é armazenada pelo sistema StorageGRID.
- Você deve ter a senha de provisionamento para procedimentos de instalação, expansão e manutenção, incluindo o download do Pacote de recuperação. Portanto, é importante que você armazene a senha de provisionamento em um local seguro.
- Você pode alterar a senha de provisionamento do Gerenciador de Grade se tiver a senha atual.
- A senha do usuário raiz de gerenciamento de grade pode ser alterada usando o Gerenciador de Grade.
- As senhas do console de linha de comando e SSH geradas aleatoriamente são armazenadas no `Passwords.txt` arquivo no Pacote de recuperação.

Passos

1. Em **frase-passe de aprovisionamento**, introduza a frase-passe de aprovisionamento que será necessária para efetuar alterações na topologia de grelha do seu sistema StorageGRID.

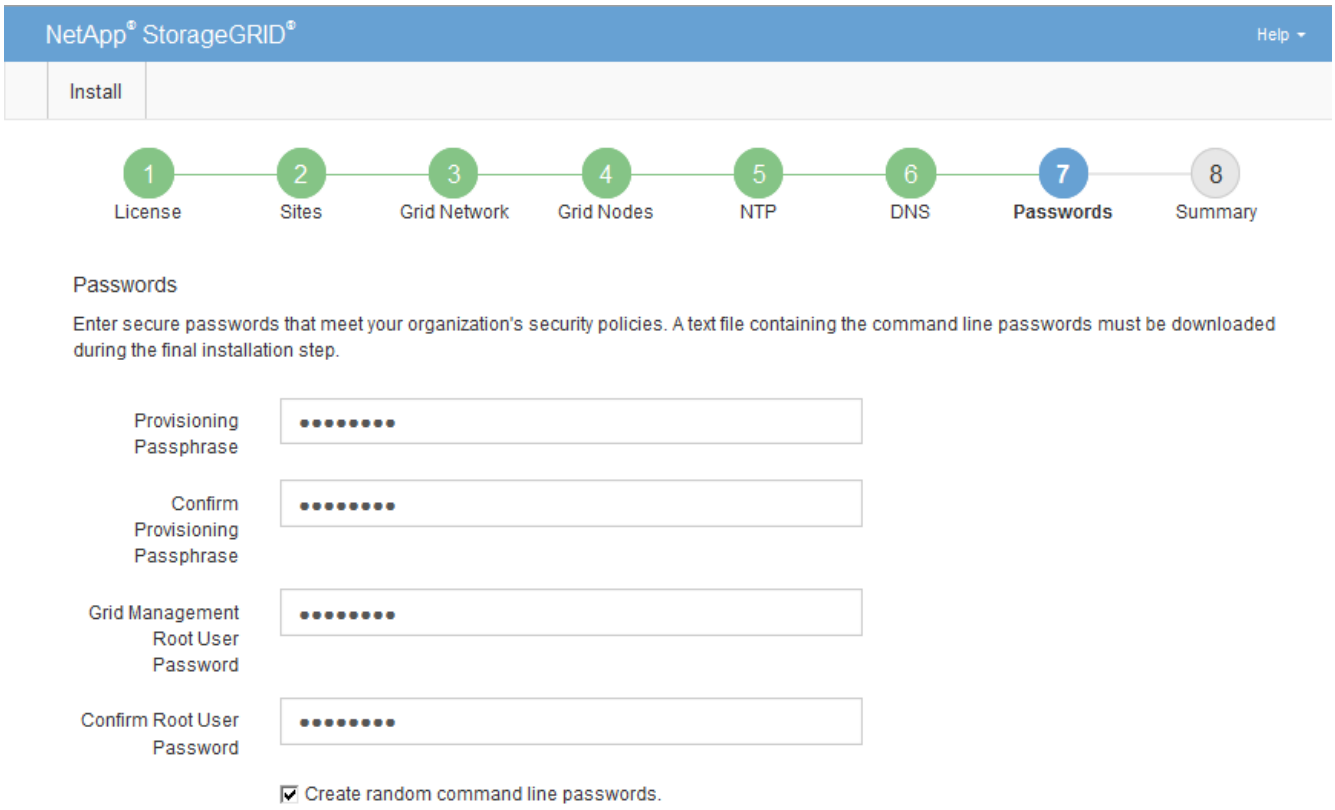
   Armazene a senha de provisionamento em um local seguro.

   > ⓘ Se após a conclusão da instalação e você quiser alterar a senha de provisionamento mais tarde, você pode usar o Gerenciador de Grade. Selecione **CONFIGURATION** > **access control**> **Grid passwords**.

2. Em **Confirm Provisioning Passphrase** (confirmar frase-passe de aprovisionamento), volte a introduzir a frase-passe de aprovisionamento para a confirmar.
3. Em **Grid Management Root User Password**, insira a senha a ser usada para acessar o Grid Manager como usuário "root".

   Guarde a palavra-passe num local seguro.

4. Em **Confirm root User Password**, digite novamente a senha do Grid Manager para confirmá-la.



5. Se você estiver instalando uma grade para fins de prova de conceito ou demonstração, desmarque a caixa de seleção **criar senhas de linha de comando aleatórias**.

   Para implantações de produção, senhas aleatórias devem sempre ser usadas por razões de segurança. Limpar **criar senhas de linha de comando aleatórias** somente para grades de demonstração se você quiser usar senhas padrão para acessar nós de grade da linha de comando usando a conta "root" ou "admin".

   > Você será solicitado a baixar o arquivo do pacote de recuperação (`sgws-recovery-package-id-revision.zip`) depois de clicar em **Instalar** na página Resumo. Você deve "transfira este ficheiro"concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas `Passwords.txt` no arquivo, contido no arquivo Pacote de recuperação.

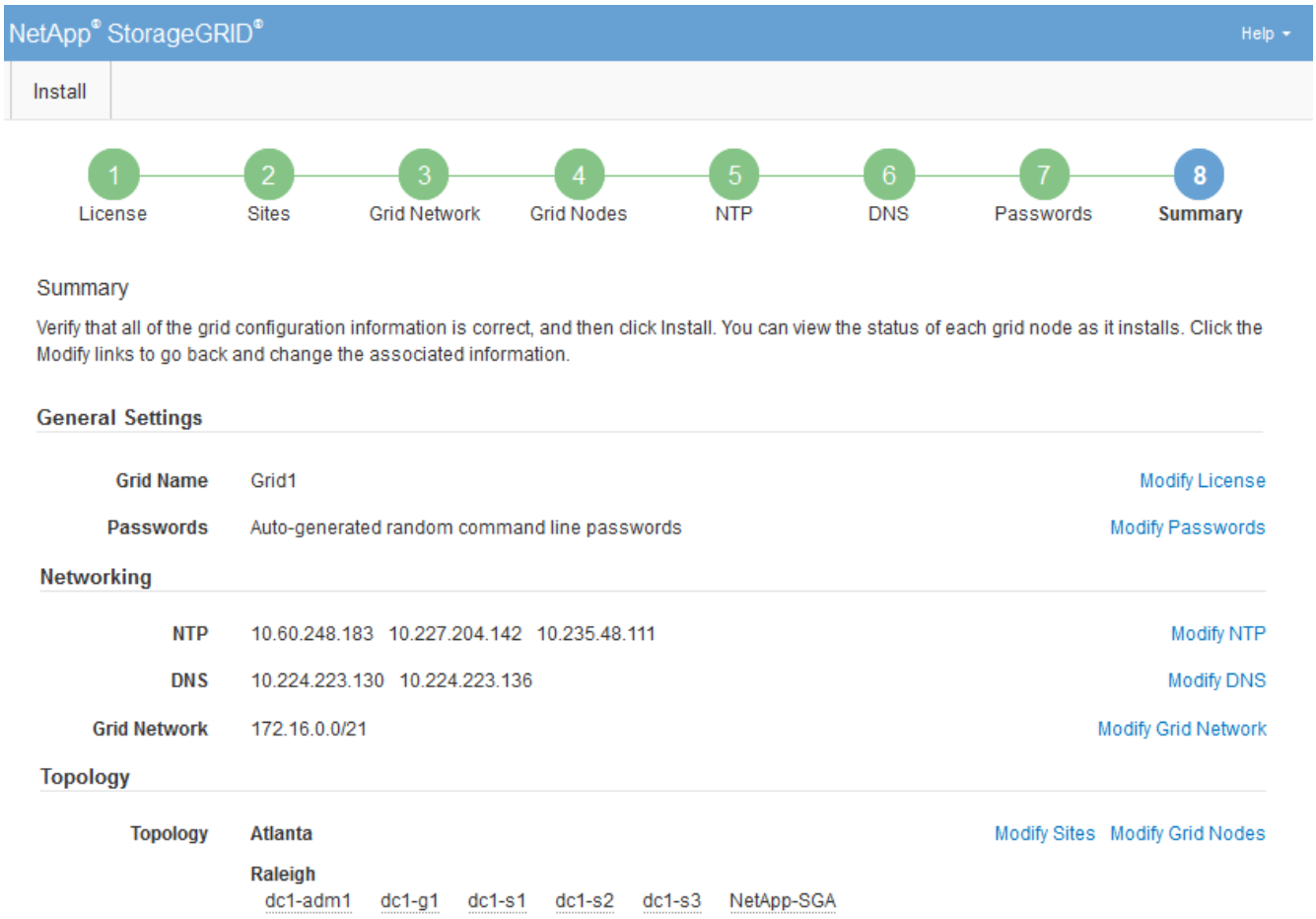
6. Clique em **seguinte**.

Revise sua configuração e conclua a instalação

Você deve analisar cuidadosamente as informações de configuração inseridas para garantir que a instalação seja concluída com êxito.

Passos

1. Veja a página **Summary**.



2. Verifique se todas as informações de configuração da grade estão corretas. Use os links Modificar na página Resumo para voltar e corrigir quaisquer erros.
3. Clique em **Instalar**.

> Se um nó estiver configurado para usar a rede do cliente, o gateway padrão para esse nó alterna da rede da grade para a rede do cliente quando você clica em **Instalar**. Se você perder a conetividade, deve garantir que está acessando o nó de administração principal por meio de uma sub-rede acessível. "Diretrizes de rede"Consulte para obter detalhes.

4. Clique em **Download Recovery Package**.

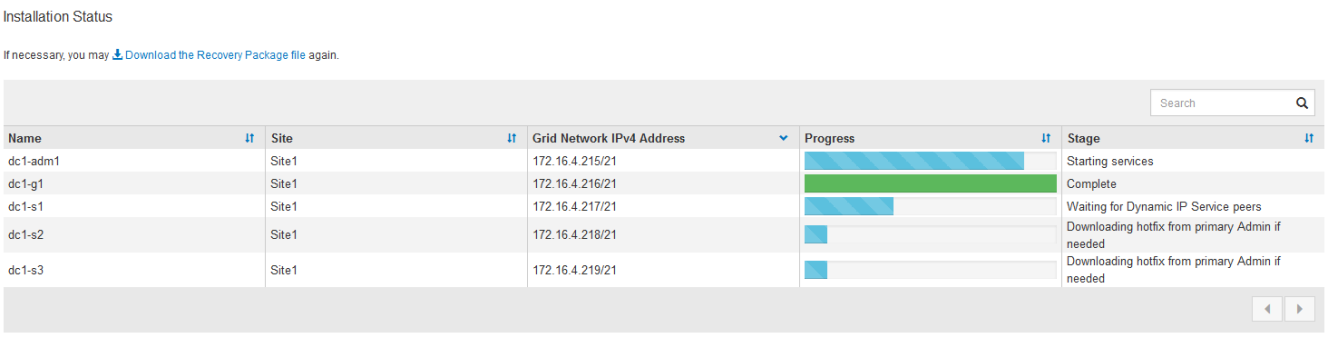
   Quando a instalação progride até o ponto em que a topologia da grade é definida, você será solicitado a baixar o arquivo do Pacote de recuperação (`.zip`) e confirmar que você pode acessar com êxito o conteúdo desse arquivo. Você deve baixar o arquivo do pacote de recuperação para que você possa recuperar o sistema StorageGRID se um ou mais nós de grade falharem. A instalação continua em segundo plano, mas você não pode concluir a instalação e acessar o sistema StorageGRID até baixar e verificar esse arquivo.

5. Verifique se você pode extrair o conteúdo do `.zip` arquivo e salvá-lo em 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.

6. Marque a caixa de seleção **Eu baixei e verifiquei com êxito o arquivo do pacote de recuperação** e clique em **Avançar**.

   Se a instalação ainda estiver em andamento, a página de status será exibida. Esta página indica o progresso da instalação para cada nó de grade.



   Quando o estágio completo é alcançado para todos os nós de grade, a página de login do Gerenciador de Grade é exibida.

7. Inicie sessão no Grid Manager utilizando o utilizador "root" e a palavra-passe especificada durante a instalação.

Diretrizes de pós-instalação

Depois de concluir a implantação e a configuração do nó de grade, siga estas diretrizes para endereçamento DHCP e alterações na configuração da rede.

- Se o DHCP foi usado para atribuir endereços IP, configure uma reserva DHCP para cada endereço IP nas redes que estão sendo usadas.

  Só pode configurar o DHCP durante a fase de implementação. Não é possível configurar o DHCP durante a configuração.

  > Os nós reiniciam quando a configuração da rede de Grade é alterada pelo DHCP, o que pode causar interrupções se uma alteração de DHCP afetar vários nós ao mesmo tempo.

- Você deve usar os procedimentos alterar IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. "Configurar endereços IP"Consulte .
- Se você fizer alterações na configuração de rede, incluindo alterações de roteamento e gateway, a conetividade do cliente para o nó de administração principal e outros nós de grade pode ser perdida. Dependendo das alterações de rede aplicadas, talvez seja necessário restabelecer essas conexões.

API REST de instalação

O StorageGRID fornece a API de instalação do StorageGRID para executar tarefas de instalação.

A API usa a plataforma de API de código aberto Swagger para fornecer a documentação da API. O Swagger permite que desenvolvedores e não desenvolvedores interajam com a API em uma interface de usuário que ilustra como a API responde a parâmetros e opções. Esta documentação pressupõe que você esteja familiarizado com as tecnologias da Web padrão e o formato de dados JSON.

Todas as operações de API executadas usando a página da Documentação da API são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Cada comando REST API inclui o URL da API, uma ação HTTP, quaisquer parâmetros de URL necessários ou opcionais e uma resposta de API esperada.

API de instalação do StorageGRID

A API de instalação do StorageGRID só está disponível quando você estiver configurando inicialmente o sistema StorageGRID e se precisar executar uma recuperação do nó de administração principal. A API de instalação pode ser acessada por HTTPS a partir do Gerenciador de Grade.

Para acessar a documentação da API, vá para a página da Web de instalação no nó de administração principal e selecione **Ajuda** > **Documentação da API** na barra de menus.

A API de instalação do StorageGRID inclui as seguintes seções:

- **Config** — operações relacionadas à versão do produto e versões da API. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **Grid** — operações de configuração em nível de grade. Você pode obter e atualizar configurações de grade, incluindo detalhes de grade, sub-redes de rede de grade, senhas de grade e endereços IP de servidor NTP e DNS.
- **Nodes** — operações de configuração em nível de nó. Você pode recuperar uma lista de nós de grade, excluir um nó de grade, configurar um nó de grade, exibir um nó de grade e redefinir a configuração de um nó de grade.
- **Provisão** — operações de provisionamento. Você pode iniciar a operação de provisionamento e exibir o status da operação de provisionamento.
- **Recovery** — operações de recuperação do nó de administração principal. Você pode redefinir informações, carregar o pacote de recuperação, iniciar a recuperação e exibir o status da operação de recuperação.
- **Recovery-package** — operações para baixar o Recovery Package.
- **Sites** — operações de configuração no nível do local. Você pode criar, exibir, excluir e modificar um site.
- **Temporary-password** — operações na senha temporária para proteger a mgmt-api durante a instalação.

Informações relacionadas

"Automatizando a instalação"

Onde ir a seguir

Depois de concluir uma instalação, execute as tarefas de integração e configuração necessárias. Você pode executar as tarefas opcionais conforme necessário.

Tarefas necessárias

- "Crie uma conta de locatário" Para o protocolo cliente S3 que será utilizado para armazenar objetos no seu sistema StorageGRID.
- "Controle o acesso ao sistema" configurando grupos e contas de usuário. Opcionalmente, você pode "configure uma fonte de identidade federada" (como ative Directory ou OpenLDAP), para que você possa

importar grupos de administração e usuários. Ou, você pode "crie grupos locais e usuários".

- Integre e teste os "S3 API" aplicativos cliente que você usará para carregar objetos para seu sistema StorageGRID.
- "Configure as regras de gerenciamento do ciclo de vida das informações (ILM) e a política ILM" você deseja usar para proteger os dados do objeto.
- Se a instalação incluir nós de storage do dispositivo, use o SANtricity os para concluir as seguintes tarefas:
  - Ligue a cada dispositivo StorageGRID.
  - Verifique a receção dos dados do AutoSupport.

```
https://docs.netapp.com/us-en/storagegrid-
appliances/installconfig/configuring-hardware.html["Configure o
hardware"^]Consulte .
```

- Analise e siga o "Diretrizes de fortalecimento do sistema StorageGRID" para eliminar os riscos de segurança.
- "Configurar notificações por e-mail para alertas do sistema".

Tarefas opcionais

- "Atualize os endereços IP do nó da grade" Se eles foram alterados desde que você planejou sua implantação e gerou o Pacote de recuperação.
- "Configurar a criptografia de armazenamento", se necessário.
- "Configurar a compressão de armazenamento" para reduzir o tamanho dos objetos armazenados, se necessário.
- "Configurar interfaces VLAN" para isolar e particionar o tráfego de rede, se necessário.
- "Configurar grupos de alta disponibilidade" Para melhorar a disponibilidade de conexão para os clientes Grid Manager, Tenant Manager e S3, se necessário.
- "Configurar pontos de extremidade do balanceador de carga" Para conetividade de cliente S3, se necessário.

Solucionar problemas de instalação

Se ocorrerem problemas durante a instalação do sistema StorageGRID, pode aceder aos ficheiros de registo de instalação. O suporte técnico também pode precisar usar os arquivos de log de instalação para resolver problemas.

Os seguintes arquivos de log de instalação estão disponíveis no contentor que está executando cada nó:

- `/var/local/log/install.log` (encontrado em todos os nós da grade)
- `/var/local/log/gdu-server.log` (Encontrado no nó de administração principal)

Os seguintes arquivos de log de instalação estão disponíveis no host:

- `/var/log/storagegrid/daemon.log`

- `/var/log/storagegrid/nodes/<node-name>.log`

Para saber como acessar os arquivos de log, "Colete arquivos de log e dados do sistema"consulte .

Informações relacionadas

"Solucionar problemas de um sistema StorageGRID"

Exemplo /etc/network/interfaces

O `/etc/network/interfaces` arquivo inclui três seções, que definem as interfaces físicas, a interface de ligação e as interfaces VLAN. Você pode combinar as três seções de exemplo em um único arquivo, que agregará quatro interfaces físicas do Linux em uma única ligação LACP e, em seguida, estabelecer três interfaces VLAN que subtendem a ligação para uso como interfaces de rede StorageGRID, Admin e rede Cliente.

Interfaces físicas

Observe que os switches nas outras extremidades dos links também devem tratar as quatro portas como um único tronco LACP ou canal de porta, e devem passar pelo menos as três VLANs referenciadas com tags.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Interface Bond

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

Interfaces VLAN

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Instale o StorageGRID no VMware

Início rápido para instalar o StorageGRID no VMware

Siga estas etapas de alto nível para instalar um nó do VMware StorageGRID.

1. **Preparação**
   - Saiba mais "Topologia de rede e arquitetura StorageGRID"sobre .
   - Saiba mais sobre as especificidades "Rede StorageGRID"do .
   - Reúna e prepare o "Informações e materiais necessários".
   - Instalar e configurar "VMware vSphere Hypervisor, vCenter e os hosts ESX"o .
   - Prepare o "CPU e RAM"necessário .
   - Fornecer para "requisitos de storage e desempenho".
2. **Implantação**

Implante nós de grade. Quando você implementa nós de grade, eles são criados como parte do sistema StorageGRID e conetados a uma ou mais redes.

- Use o VMware vSphere Web Client, um arquivo .vmdk e um conjunto de modelos de arquivo .ovf "Implante os nós baseados em software como máquinas virtuais (VMs)"nos servidores preparados na etapa 1.
- Para implantar os nós de dispositivos StorageGRID, siga o "Início rápido para instalação de hardware".

Configuração

Quando todos os nós tiverem sido implantados, use o Gerenciador de Grade para "configure a grade e conclua a instalação".

Automatize a instalação

Para economizar tempo e fornecer consistência, você pode automatizar a implantação e configuração de nós de grade e a configuração do sistema StorageGRID.

- "Automatize a implantação do nó de grade usando o VMware vSphere".
- Depois de implantar nós de grade, "Automatize a configuração do sistema StorageGRID" usando o script de configuração Python fornecido no arquivo de instalação.
- "Automatize a instalação e a configuração dos nós de grade do dispositivo"
- Se você é um desenvolvedor avançado de implantações do StorageGRID, automatize a instalação de nós de grade usando o "API REST de instalação".

Planeje e prepare-se para a instalação no VMware

Informações e materiais necessários

Antes de instalar o StorageGRID, reúna e prepare as informações e materiais necessários.

Informações necessárias

Plano de rede

Quais redes você pretende anexar a cada nó do StorageGRID. O StorageGRID suporta várias redes para separação de tráfego, segurança e conveniência administrativa.

Consulte o StorageGRID "Diretrizes de rede".

Informações de rede

Endereços IP para atribuir a cada nó de grade e aos endereços IP dos servidores DNS e NTP.

Servidores para nós de grade

Identifique um conjunto de servidores (físicos, virtuais ou ambos) que, no agregado, fornecem recursos suficientes para suportar o número e o tipo de nós do StorageGRID que você planeja implantar.

Se a instalação do StorageGRID não usar nós de armazenamento do StorageGRID Appliance (hardware), você deve usar o armazenamento RAID de hardware com cache de gravação (BBWC) com bateria. O StorageGRID não suporta o uso de redes de área de armazenamento virtual (VSANs), RAID de software ou nenhuma proteção RAID.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Materiais necessários

Licença NetApp StorageGRID

Você deve ter uma licença NetApp válida e assinada digitalmente.

Uma licença de não produção, que pode ser usada para testar e testar grades de prova de conceito, está incluída no arquivo de instalação do StorageGRID.

Arquivo de instalação do StorageGRID

"Baixe o arquivo de instalação do StorageGRID e extraia os arquivos".

Serviço de laptop

O sistema StorageGRID é instalado através de um computador portátil de serviço.

O computador portátil de serviço deve ter:

- Porta de rede
- Cliente SSH (por exemplo, PuTTY)
- "Navegador da Web suportado"

Documentação do StorageGRID

- "Notas de lançamento"
- "Instruções para administrar o StorageGRID"

Baixe e extraia os arquivos de instalação do StorageGRID

Você deve baixar os arquivos de instalação do StorageGRID e extrair os arquivos. Opcionalmente, você pode verificar manualmente os arquivos no pacote de instalação.

Passos

1. Vá para "Página de downloads do NetApp para StorageGRID" .
2. Selecione o botão para baixar a versão mais recente ou selecione outra versão no menu suspenso e selecione **Go**.
3. Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.
4. Se for apresentada uma instrução Caution/MustRead, leia-a e selecione a caixa de verificação.

Você deve aplicar os hotfixes necessários depois de instalar a versão do StorageGRID. Para obter mais informações, consulte a. "procedimento de hotfix nas instruções de recuperação e manutenção"

5. Leia o Contrato de Licença de Utilizador final, selecione a caixa de verificação e, em seguida, selecione **Accept & continue**.
6. Na coluna **Instalar StorageGRID**, selecione o arquivo de instalação .tgz ou .zip para VMware.

   Use o `.zip` arquivo se você estiver executando o Windows no laptop de serviço.

7. Salve o arquivo de instalação.
8. se você precisar verificar o arquivo de instalação:
   a. Baixe o pacote de verificação de assinatura de código StorageGRID. O nome do arquivo deste pacote usa o formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`, onde `<version-number>` está a versão do software StorageGRID.
   b. Siga os passos para "verifique manualmente os arquivos de instalação".
9. Extraia os arquivos do arquivo de instalação.
10. Escolha os arquivos que você precisa.

    Os arquivos de que você precisa dependem da topologia de grade planejada e de como implantar o sistema StorageGRID.

Os caminhos listados na tabela são relativos ao diretório de nível superior instalado pelo arquivo de instalação extraído.

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 do Gateway.

Caminho e nome do arquivo	Descrição
	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 `deploy-vsphere-ovftool.sh` 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 entrar na API de Gerenciamento de Grade quando o logon único (SSO) está ativado. Você também pode usar este script para integração Ping federate.
	Um exemplo de arquivo de configuração para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.

Caminho e nome do arquivo	Descrição
	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.

Verificar manualmente os arquivos de instalação (opcional)

Se necessário, você pode verificar manualmente os arquivos no arquivo de instalação do StorageGRID.

Antes de começar

Você tem "download do pacote de verificação"do "Página de downloads do NetApp para StorageGRID".

Passos

1. Extraia os artefatos do pacote de verificação:

   ```
   tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
   ```

2. Certifique-se de que estes artefactos foram extraídos:
   - Folha de certificado: `Leaf-Cert.pem`
   - Cadeia de certificados: `CA-Int-Cert.pem`
   - Cadeia de resposta do carimbo de hora: `TS-Cert.pem`
   - Ficheiro checksum: `sha256sum`
   - Assinatura do checksum: `sha256sum.sig`
   - Ficheiro de resposta do carimbo de hora: `sha256sum.sig.tsr`
3. Utilize a corrente para verificar se o certificado de lâminas é válido.

   Exemplo: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

   Saída esperada: `Leaf-Cert.pem: OK`

4. Se a etapa *2* falhou devido a um certificado de folha expirado, use o `tsr` arquivo para verificar.

   Exemplo: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

   Saída esperada inclui: `Verification: OK`

5. Crie um arquivo de chave pública a partir do certificado Leaf.

   Exemplo: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Saída esperada: *None*

6. Use a chave pública para verificar o `sha256sum` arquivo contra `sha256sum.sig`.

   Exemplo: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

   Saída esperada: `Verified OK`

7. Verifique o `sha256sum` conteúdo do arquivo em relação às somas de verificação recém-criadas.

   Exemplo: `sha256sum -c sha256sum`

   Saída esperada: *<filename>*`: OK`
   <filename> É o nome do arquivo que você baixou.

8. "Conclua as etapas restantes" para extrair e escolher os arquivos de instalação apropriados.

Requisitos de software para VMware

Você pode usar uma máquina virtual para hospedar qualquer tipo de nó StorageGRID. Você precisa de uma máquina virtual para cada nó de grade.

VMware vSphere Hypervisor

Você deve instalar o VMware vSphere Hypervisor em um servidor físico preparado. O hardware deve ser configurado corretamente (incluindo versões de firmware e configurações de BIOS) antes de instalar o software VMware.

- Configure a rede no hypervisor conforme necessário para suportar a rede para o sistema StorageGRID que você está instalando.

  "Diretrizes de rede"

- Certifique-se de que o datastore seja grande o suficiente para as máquinas virtuais e os discos virtuais necessários para hospedar os nós da grade.
- Se você criar mais de um datastore, nomeie cada datastore para que possa identificar facilmente qual datastore usar para cada nó de grade ao criar máquinas virtuais.

Requisitos de configuração do host ESX

> Você deve configurar corretamente o protocolo NTP (Network Time Protocol) em cada host ESX. Se o tempo do host estiver incorreto, podem ocorrer efeitos negativos, incluindo perda de dados.

Requisitos de configuração da VMware

Você deve instalar e configurar o VMware vSphere e o vCenter antes de implantar os nós do StorageGRID.

Para versões com suporte do software VMware vSphere Hypervisor e VMware vCenter Server, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Para obter as etapas necessárias para instalar esses produtos VMware, consulte a documentação da

VMware.

Requisitos de CPU e RAM

Antes de instalar o software StorageGRID, verifique e configure o hardware para que ele esteja pronto para suportar o sistema StorageGRID.

Cada nó do StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Depende do total de RAM disponível e da quantidade de software que não seja StorageGRID executado no sistema
  - Geralmente, pelo menos 24 GB por nó e 2 a 16 GB menos do que a RAM total do sistema
  - Um mínimo de 64 GB para cada locatário que terá aproximadamente 5.000 buckets

A VMware oferece suporte a um nó por máquina virtual. Certifique-se de que o nó StorageGRID não exceda a RAM física disponível. Cada máquina virtual deve ser dedicada à execução do StorageGRID.

> Monitore regularmente o uso da CPU e da memória para garantir que esses recursos continuem a acomodar sua carga de trabalho. Por exemplo, duplicar a alocação de RAM e CPU para nós de storage virtual forneceria recursos semelhantes aos fornecidos para nós de dispositivos StorageGRID. Além disso, se a quantidade de metadados por nó exceder 500 GB, considere aumentar a RAM por nó para 48 GB ou mais. Para obter informações sobre como gerenciar o armazenamento de metadados de objetos, aumentar a configuração espaço reservado de metadados e monitorar o uso da CPU e da memória, consulte as instruções para "administrar", "monitorização"e "a atualizar"StorageGRID.

Se o hyperthreading estiver habilitado nos hosts físicos subjacentes, você poderá fornecer 8 núcleos virtuais (4 núcleos físicos) por nó. Se o hyperthreading não estiver habilitado nos hosts físicos subjacentes, você deverá fornecer 8 núcleos físicos por nó.

Se você estiver usando máquinas virtuais como hosts e tiver controle sobre o tamanho e o número de VMs, use uma única VM para cada nó do StorageGRID e dimensione a VM de acordo.

Consulte também "Requisitos de storage e desempenho".

Requisitos de storage e desempenho

Você precisa entender os requisitos de storage e desempenho para nós do StorageGRID hospedados por máquinas virtuais, para que você possa fornecer espaço suficiente para dar suporte à configuração inicial e à expansão futura de storage.

Requisitos de desempenho

O desempenho do volume do sistema operacional e do primeiro volume de storage impactam significativamente o desempenho geral do sistema. Certifique-se de que eles forneçam desempenho de disco adequado em termos de latência, IOPS e taxa de transferência.

Todos os nós do StorageGRID exigem que a unidade de sistema operacional e todos os volumes de storage tenham o armazenamento em cache de gravação ativado. O cache deve estar em uma Mídia protegida ou persistente.

Requisitos para máquinas virtuais que usam armazenamento NetApp ONTAP

Se você estiver implantando um nó StorageGRID como uma máquina virtual com armazenamento atribuído a partir de um sistema NetApp ONTAP, você confirmou que o volume não tem uma política de disposição em camadas do FabricPool ativada. Por exemplo, se um nó do StorageGRID estiver sendo executado como uma máquina virtual em um host VMware, verifique se o volume que faz o backup do datastore para o nó 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.

Número de máquinas virtuais necessárias

Cada local do StorageGRID requer um mínimo de três nós de storage.

Requisitos de storage por tipo de nó

Em um ambiente de produção, as máquinas virtuais para nós de StorageGRID precisam atender a requisitos diferentes, dependendo dos tipos de nós.

> Snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte "recuperação do nó de grade"os procedimentos para cada tipo de nó.

Tipo nó	Armazenamento
Nó de administração	LUN DE 100 GB PARA OS LUN de 200 GB para tabelas Admin Node LUN de 200 GB para log de auditoria do nó de administrador
Nó de storage	LUN DE 100 GB PARA OS 3 LUNs para cada nó de storage nesse host **Nota**: Um nó de armazenamento pode ter 1 a 16 LUNs de armazenamento; pelo menos 3 LUNs de armazenamento são recomendados. Tamanho mínimo por LUN: 4 TB Tamanho máximo de LUN testado: 39 TB.

Tipo nó	Armazenamento
Nó de storage (somente metadados)	LUN DE 100 GB PARA OS 1 LUN Tamanho mínimo por LUN: 4 TB **Nota**: Não há tamanho máximo para o único LUN. A capacidade excedente é economizada para uso futuro. **Nota**: Somente um rangedb é necessário para nós de storage somente metadados.
Nó de gateway	LUN DE 100 GB PARA OS

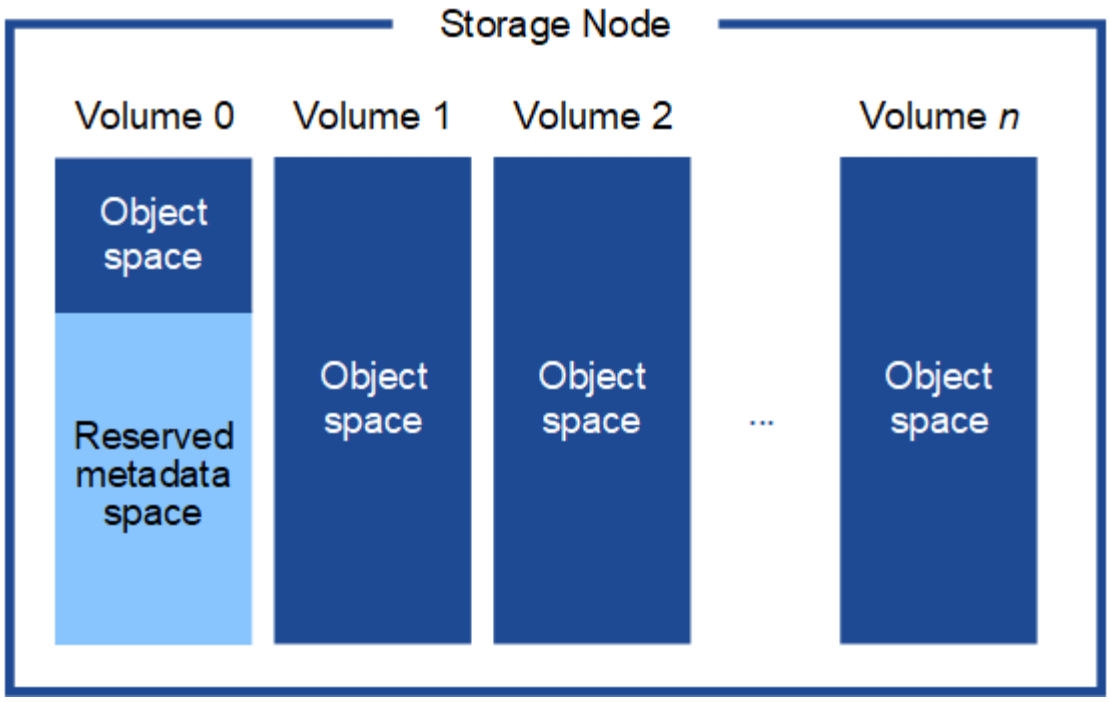
Dependendo do nível de auditoria configurado, do tamanho das entradas do usuário, como o nome da chave do objeto S3 e da quantidade de dados de log de auditoria que você precisa preservar, talvez seja necessário aumentar o tamanho do LUN de log de auditoria em cada nó Admin. Geralmente, uma grade gera aproximadamente 1 KB de dados de auditoria por operação S3, o que significaria que um LUN de 200 GB suportaria 70 milhões de operações por dia ou 800 operações por segundo por dois a três dias.

Requisitos de storage para nós de storage

Um nó de storage baseado em software pode ter 1 a 16 volumes de armazenamento—3 ou mais volumes de armazenamento são recomendados. Cada volume de armazenamento deve ser de 4 TB ou maior.

Um nó de storage de dispositivo pode ter até 48 volumes de storage.

Como mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de storage 0 de cada nó de storage. Qualquer espaço restante no volume de armazenamento 0 e quaisquer outros volumes de armazenamento no nó de armazenamento são usados exclusivamente para dados de objeto.



Para fornecer redundância e proteger os metadados de objetos contra perda, o StorageGRID armazena três cópias dos metadados de todos os objetos no sistema em cada local. As três cópias dos metadados de objetos são distribuídas uniformemente por todos os nós de storage em cada local.

Ao instalar uma grade com nós de storage somente de metadados, a grade também deve conter um número mínimo de nós para storage de objetos. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

- Para uma grade de um único local, pelo menos dois nós de storage são configurados para objetos e metadados.
- Para uma grade de vários locais, pelo menos um nó de storage por local é configurado para objetos e metadados.

Ao atribuir espaço ao volume 0 de um novo nó de storage, você deve garantir que haja espaço adequado para a parte desse nó de todos os metadados de objetos.

- No mínimo, você deve atribuir pelo menos 4 TB ao volume 0.

> Se você usar apenas um volume de armazenamento para um nó de armazenamento e atribuir 4 TB ou menos ao volume, o nó de armazenamento poderá entrar no estado somente leitura de armazenamento na inicialização e armazenar somente metadados de objetos.

> Se você atribuir menos de 500 GB ao volume 0 (somente uso não-produção), 10% da capacidade do volume de armazenamento será reservada para metadados.

- Se você estiver instalando um novo sistema (StorageGRID 11,6 ou superior) e cada nó de armazenamento tiver 128 GB ou mais de RAM, atribua 8 TB ou mais ao volume 0. O uso de um valor maior para o volume 0 pode aumentar o espaço permitido para metadados em cada nó de storage.
- Ao configurar diferentes nós de storage para um local, use a mesma configuração para o volume 0, se possível. Se um local contiver nós de storage de tamanhos diferentes, o nó de storage com o menor

volume 0 determinará a capacidade de metadados desse local.

Para obter mais detalhes, "Gerenciar o storage de metadados de objetos"visite .

Automatizar a instalação (VMware)

Você pode usar a ferramenta VMware OVF para automatizar a implantação de nós de grade. Também é possível automatizar a configuração do StorageGRID.

Automatize a implantação do nó de grade

Use a ferramenta VMware OVF para automatizar a implantação de nós de grade.

Antes de começar

- Você tem acesso a um sistema Linux/Unix com o Bash 3,2 ou posterior.
- Você tem o VMware vSphere com vCenter
- Você tem o VMware OVF Tool 4,1 instalado e configurado corretamente.
- Você sabe o nome de usuário e a senha para acessar o VMware vSphere usando a ferramenta OVF
- Você tem as permissões suficientes para implantar VMs de arquivos OVF e ativá-las e permissões para criar volumes adicionais para serem anexados às VMs. Consulte `ovftool` a documentação para obter detalhes.
- Você conhece o URL da infraestrutura virtual (VI) para o local no vSphere onde deseja implantar as máquinas virtuais do StorageGRID. Esse URL normalmente será um vApp ou pool de recursos. Por exemplo: `vi://vcenter.example.com/vi/sgws`

> Você pode usar o utilitário VMware `ovftool` para determinar esse valor (consulte `ovftool` a documentação para obter detalhes).

> Se você estiver implantando em um vApp, as máquinas virtuais não serão iniciadas automaticamente pela primeira vez e você deverá ligá-las manualmente.

- Você coletou todas as informações necessárias para o arquivo de configuração de implantação. Consulte "Colete informações sobre seu ambiente de implantação" para obter informações.
- Você tem acesso aos seguintes arquivos do arquivo de instalação do VMware para StorageGRID:

Nome do ficheiro	Descrição
NetApp-SG-version-SHA.vmdk	O arquivo de disco da máquina virtual que é usado como um modelo para criar máquinas virtuais de nó de grade. **Nota:** este ficheiro tem de estar na mesma pasta que os `.ovf` ficheiros e `.mf`.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	O arquivo de modelo Open Virtualization Format (`.ovf`) e o arquivo de manifesto (`.mf`) para implantar o nó de administração principal.

Nome do ficheiro	Descrição
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de administração não primários.
vsphere-gateway.ovf vsphere-gateway.mf	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós do Gateway.
vsphere-storage.ovf vsphere-storage.mf	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de storage baseados em máquina virtual.
deploy-vsphere-ovftool.sh	O script de shell Bash usado para automatizar a implantação de nós de grade virtual.
deploy-vsphere-ovftool-sample.ini	O exemplo de arquivo de configuração para uso com o `deploy-vsphere-ovftool.sh` script.

Defina o arquivo de configuração para sua implantação

Você especifica as informações necessárias para implantar nós de grade virtual para o StorageGRID em um arquivo de configuração, que é usado pelo `deploy-vsphere-ovftool.sh` script Bash. Você pode modificar um exemplo de arquivo de configuração, para que você não precise criar o arquivo do zero.

Passos

1. Faça uma cópia do arquivo de configuração de exemplo (`deploy-vsphere-ovftool.sample.ini`). Salve o novo arquivo como `deploy-vsphere-ovftool.ini` no mesmo diretório do `deploy-vsphere-ovftool.sh`.
2. Abra `deploy-vsphere-ovftool.ini`o .
3. Insira todas as informações necessárias para implantar os nós de grade virtual da VMware.

   Consulte Definições do ficheiro de configuração para obter informações.

4. Quando tiver introduzido e verificado todas as informações necessárias, guarde e feche o ficheiro.

Definições do ficheiro de configuração

O `deploy-vsphere-ovftool.ini` arquivo de configuração contém as configurações necessárias para implantar nós de grade virtual.

O arquivo de configuração primeiro lista os parâmetros globais e, em seguida, lista os parâmetros específicos do nó em seções definidas pelo nome do nó. Quando o arquivo é usado:

- *Parâmetros globais* são aplicados a todos os nós de grade.
- *Parâmetros específicos do nó* substituem os parâmetros globais.

Parâmetros globais

Os parâmetros globais são aplicados a todos os nós da grade, a menos que sejam substituídos por configurações em seções individuais. Coloque os parâmetros que se aplicam a vários nós na seção parâmetro global e, em seguida, substitua essas configurações conforme necessário nas seções para nós individuais.

- **OVFTOOL_ARGUMENTS**: Você pode especificar OVFTOOL_ARGUMENTS como configurações globais, ou você pode aplicar argumentos individualmente a nós específicos. Por exemplo:

```
OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
--datastore='datastore_name'
```

  Você pode usar as `--powerOffTarget` opções e `--overwrite` para desligar e substituir máquinas virtuais existentes.

  > Você deve implantar nós em diferentes datastores e especificar OVFTOOL_ARGUMENTS para cada nó, em vez de globalmente.

- **SOURCE**: O caminho para o (`.vmdk`arquivo de modelo de máquina virtual StorageGRID) e `.ovf` os arquivos e `.mf` para nós de grade individuais. O padrão é o diretório atual.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **TARGET**: O URL da infraestrutura virtual (vi) do VMware vSphere para o local onde o StorageGRID será implantado. Por exemplo:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_Network_CONFIG**: O método usado para adquirir endereços IP, ESTÁTICOS ou DHCP. O padrão é ESTÁTICO. Se todos ou a maioria dos nós usarem o mesmo método para adquirir endereços IP, você pode especificar esse método aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_Network_TARGET**: O nome de uma rede VMware existente a ser usada para a rede Grid. Se todos ou a maioria dos nós usarem o mesmo nome de rede, você pode especificá-lo aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_Network_mask**: A máscara de rede para a rede de Grade. Se todos ou a maioria dos nós usarem a mesma máscara de rede, você pode especificá-la aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_Network_GATEWAY**: O gateway de rede para a rede Grid. Se todos ou a maioria dos nós usarem o mesmo gateway de rede, você pode especificá-lo aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU**: OPCIONAL. A unidade de transmissão máxima (MTU) na rede de Grade. Se especificado, o valor deve estar entre 1280 e 9216. Por exemplo:

```
GRID_NETWORK_MTU = 9000
```

  Se omitido, 1400 é usado.

  Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão.

  > O valor MTU da rede deve corresponder ao valor configurado na porta do switch virtual no vSphere ao qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

  > 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.

- **ADMIN_network_CONFIG**: O método usado para adquirir endereços IP, DESATIVADOS, ESTÁTICOS ou DHCP. A predefinição é desativada. Se todos ou a maioria dos nós usarem o mesmo método para adquirir endereços IP, você pode especificar esse método aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **Admin_network_TARGET**: O nome de uma rede VMware existente a ser usada para a rede Admin. Esta definição é necessária, a menos que a rede de administração esteja desativada. Se todos ou a maioria dos nós usarem o mesmo nome de rede, você pode especificá-lo aqui. Ao contrário da rede de Grade, todos os nós não precisam ser conetados à mesma rede de administração. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_network_mask**: A máscara de rede para a rede Admin. Esta definição é necessária se estiver a utilizar endereçamento IP estático. Se todos ou a maioria dos nós usarem a mesma máscara de rede, você pode especificá-la aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_Network_GATEWAY**: O gateway de rede para a rede Admin. Essa configuração é necessária se você estiver usando endereçamento IP estático e especificar sub-redes externas na configuração ADMIN_NETWORK_ESL. (Isto é, não é necessário se ADMIN_NETWORK_ESL estiver vazio.) Se todos ou a maioria dos nós usarem o mesmo gateway de rede, você pode especificá-lo aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **Admin_network_ESL**: A lista de sub-redes externas (rotas) para a rede Admin, especificada como uma lista separada por vírgulas de destinos de rota CIDR. Se todos ou a maioria dos nós usarem a mesma lista de sub-rede externa, você pode especificá-la aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU**: OPCIONAL. A unidade de transmissão máxima (MTU) na rede de administração. Não especifique se ADMIN_NETWORK_CONFIG é DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1400 é usado. Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. Se todos ou a maioria dos nós usarem a mesma MTU para a rede Admin, você pode especificá-la aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_network_CONFIG**: O método usado para adquirir endereços IP, DESATIVADOS, ESTÁTICOS ou DHCP. A predefinição é desativada. Se todos ou a maioria dos nós usarem o mesmo método para adquirir endereços IP, você pode especificar esse método aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_network_TARGET**: O nome de uma rede VMware existente a ser usada para a rede cliente. Esta definição é necessária, a menos que a rede do cliente esteja desativada. Se todos ou a maioria dos nós usarem o mesmo nome de rede, você pode especificá-lo aqui. Ao contrário da rede de Grade, todos os nós não precisam ser conetados à mesma rede de Cliente. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_network_mask**: A máscara de rede para a rede do cliente. Esta definição é necessária se estiver a utilizar endereçamento IP estático. Se todos ou a maioria dos nós usarem a mesma máscara de rede, você pode especificá-la aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_Network_GATEWAY**: O gateway de rede para a rede do cliente. Esta definição é necessária se estiver a utilizar endereçamento IP estático. Se todos ou a maioria dos nós usarem o mesmo gateway de rede, você pode especificá-lo aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU**: OPCIONAL. A unidade de transmissão máxima (MTU) na rede de clientes. Não especifique se CLIENT_NETWORK_CONFIG é DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1400 é usado. Se você quiser usar quadros jumbo, defina o MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. Se todos ou a maioria dos nós usarem a mesma MTU para a rede do cliente, você pode especificá-la aqui. Em seguida, você pode substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_MTU = 8192
```

- **Port_REMAP**: Remapeia qualquer porta usada por um nó para comunicações internas de nó de grade ou comunicações externas. O remapeamento de portas é necessário se as políticas de rede empresarial restringirem uma ou mais portas usadas pelo StorageGRID. Para obter a lista de portas usadas pelo StorageGRID, consulte comunicações internas de nó de grade e comunicações externas no "Diretrizes de rede".

  > Não remapegue novamente as portas que você está planejando usar para configurar pontos de extremidade do balanceador de carga.

  > Se apenas Port_REMAP estiver definido, o mapeamento que você especificar será usado para comunicações de entrada e saída. Se Port_REMAP_INBOUND também for especificado, PORT_REMAP se aplica apenas às comunicações de saída.

  O formato usado é: *`network type/protocol/default port used by grid node/new port`*, Onde o tipo de rede é grade, admin ou cliente e o protocolo é tcp ou udp.

  Por exemplo:

```
PORT_REMAP = client/tcp/18082/443
```

Se usado sozinho, esta configuração de exemplo mapeia simetricamente as comunicações de entrada e saída para o nó de grade da porta 18082 para a porta 443. Se usado em conjunto com PORT_REMAP_INBOUND, esta configuração de exemplo mapeia as comunicações de saída da porta 18082 para a porta 443.

Você também pode remapear várias portas usando uma lista separada por vírgulas.

Por exemplo:

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- **Port_REMAP_INBOUND**: Remapeia as comunicações de entrada para a porta especificada. Se você especificar PORT_REMAP_INBOUND, mas não especificar um valor para PORT_REMAP, as comunicações de saída para a porta não serão alteradas.

> Não remapegue novamente as portas que você está planejando usar para configurar pontos de extremidade do balanceador de carga.

O formato usado é: *`network type/protocol/_default port used by grid node/new port`*, Onde o tipo de rede é grade, admin ou cliente e o protocolo é tcp ou udp.

Por exemplo:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

Este exemplo leva o tráfego que é enviado para a porta 443 para passar um firewall interno e direciona-o para a porta 18082, onde o nó de grade está ouvindo solicitações S3.

Você também pode remapear várias portas de entrada usando uma lista separada por vírgulas.

Por exemplo:

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- **TEMPORARY_PASSWORD_TYPE**: O tipo de senha de instalação temporária a ser usada ao acessar o console da VM ou a API de instalação do StorageGRID, ou usando SSH, antes que o nó se una à grade.

> Se todos ou a maioria dos nós usarem o mesmo tipo de senha de instalação temporária, especifique o tipo na seção parâmetro global. Em seguida, opcionalmente, use uma configuração diferente para um nó individual. Por exemplo, se você selecionar **usar Senha personalizada** globalmente, você pode usar **CUSTOM_TEMPORARY_password <password>** para definir a senha para cada nó.

TEMPORARY_PASSWORD_TYPE pode ser um dos seguintes:

- **Use node name**: O nome do nó é usado como a senha de instalação temporária e fornece acesso ao console da VM, à API de instalação do StorageGRID e ao SSH.
- **Desativar senha**: Nenhuma senha de instalação temporária será usada. Se precisar acessar a VM para depurar problemas de instalação, "Solucionar problemas de instalação"consulte .
- **Use a senha personalizada**: O valor fornecido com o <password>* é usado como a senha de instalação temporária e fornece acesso ao console da VM, à API de instalação do StorageGRID e ao SSH.

> Opcionalmente, você pode omitir o parâmetro **TEMPORARY_PASSWORD_TYPE** e especificar somente **CUSTOM_TEMPORARY_password_<password>**.

- **CUSTOM_TEMPORARY_password: <password>** Opcional. A senha temporária a ser usada durante a instalação ao acessar o console da VM, a API de instalação do StorageGRID e o SSH. Ignorado se **TEMPORARY_PASSWORD_TYPE** estiver definido como **Use node name** ou **Disable password**.

Parâmetros específicos do nó

Cada nó está em sua própria seção do arquivo de configuração. Cada nó requer as seguintes configurações:

- O cabeçalho da seção define o nome do nó que será exibido no Gerenciador de Grade. Você pode substituir esse valor especificando o parâmetro opcional NODE_NAME para o nó.
- **NODE_TYPE**: VM_Admin_Node, VM_Storage_Node ou VM_API_Gateway_Node
- **STORAGE_TYPE**: Combinado, dados ou metadados. Esse parâmetro opcional para nós de storage é padrão combinado (dados e metadados), se não for especificado. Para obter mais informações, "Tipos de nós de storage"consulte .
- **GRID_Network_IP**: O endereço IP do nó na rede de Grade.
- **Admin_network_IP**: O endereço IP do nó na rede Admin. Necessário somente se o nó estiver conetado à rede Admin e ADMIN_network_CONFIG estiver definido como ESTÁTICO.
- **CLIENT_Network_IP**: O endereço IP do nó na rede do cliente. Necessário somente se o nó estiver conetado à rede cliente e CLIENT_network_CONFIG para este nó estiver definido como ESTÁTICO.
- **ADMIN_IP**: O endereço IP do nó Admin principal na rede de Grade. Use o valor que você especificar como GRID_NETWORK_IP para o nó Admin principal. Se você omitir esse parâmetro, o nó tentará descobrir o IP do nó Admin primário usando mDNS. Para obter mais informações, "Como os nós de grade descobrem o nó de administração principal"consulte .

> O parâmetro Admin_IP é ignorado para o nó Admin principal.

- Quaisquer parâmetros que não foram definidos globalmente. Por exemplo, se um nó estiver conetado à rede Admin e você não tiver especificado os parâmetros ADMIN_NETWORK globalmente, você deverá especificá-los para o nó.

Nó de administração principal

As seguintes configurações adicionais são necessárias para o nó de administração principal:

- **NODE_TYPE**: VM_Admin_Node
- **ADMIN_ROLE**: Primário

Esta entrada de exemplo é para um nó de administração principal que está nas três redes:

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node
  TEMPORARY_PASSWORD_TYPE = Use custom password
  CUSTOM_TEMPORARY_PASSWORD = Passw0rd

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

A seguinte configuração adicional é opcional para o nó de administração principal:

- **DISK**: Por padrão, os nós Admin recebem dois discos rígidos adicionais de 200 GB para auditoria e uso de banco de dados. Você pode aumentar essas configurações usando o parâmetro DISCO. Por exemplo:

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  Para nós de administração, AS INSTÂNCIAS devem sempre ser iguais a 2.

Nó de storage

A seguinte configuração adicional é necessária para nós de storage:

- **NODE_TYPE**: VM_Storage_Node

  Esta entrada de exemplo é para um nó de armazenamento que está nas redes Grid e Admin, mas não na rede Cliente. Esse nó usa a configuração Admin_IP para especificar o endereço IP do nó de administrador principal na rede de grade.

  ```
  [DC1-S1]
    NODE_TYPE = VM_Storage_Node

    GRID_NETWORK_IP = 10.1.0.3
    ADMIN_NETWORK_IP = 10.3.0.3

    ADMIN_IP = 10.1.0.2
  ```

  Esta segunda entrada de exemplo é para um nó de armazenamento em uma rede de cliente onde a política de rede empresarial do cliente afirma que um aplicativo cliente S3 só é permitido acessar o nó de armazenamento usando a porta 80 ou 443. O exemplo de arquivo de configuração usa port_REMAP para habilitar o nó de armazenamento para enviar e receber mensagens S3 na porta 443.

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

O último exemplo cria um remapeamento simétrico para o tráfego ssh da porta 22 para a porta 3022, mas define explicitamente os valores para o tráfego de entrada e de saída.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

As seguintes configurações adicionais são opcionais para nós de storage:

- **DISK**: Por padrão, os nós de storage recebem três discos de 4 TB para uso em RangeDB. Você pode aumentar essas configurações com o parâmetro DISCO. Por exemplo:

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **STORAGE_TYPE**: Por padrão, todos os novos nós de armazenamento são configurados para armazenar dados de objeto e metadados, conhecidos como *Combined* Storage Node. Você pode alterar o tipo nó de armazenamento para armazenar apenas dados ou metadados com o parâmetro storage_TYPE. Por exemplo:

```
STORAGE_TYPE = data
```

Nó de gateway

A seguinte configuração adicional é necessária para os nós de Gateway:

- **NODE_TYPE**: VM_API_GATEWAY

Esta entrada de exemplo é para um exemplo de Gateway Node em todas as três redes. Neste exemplo, não foram especificados parâmetros de rede do cliente na secção global do ficheiro de configuração, pelo que têm de ser especificados para o nó:

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG Client Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

Nó de administração não primário

As seguintes configurações adicionais são necessárias para nós de administração não primários:

- **NODE_TYPE**: VM_Admin_Node
- **ADMIN_ROLE**: Não-primário

Esta entrada de exemplo é para um nó de administração não primário que não esteja na rede de cliente:

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG Grid Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

A seguinte configuração adicional é opcional para nós de administração não primários:

- **DISK**: Por padrão, os nós Admin recebem dois discos rígidos adicionais de 200 GB para auditoria e uso de banco de dados. Você pode aumentar essas configurações usando o parâmetro DISCO. Por exemplo:

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  Para nós de administração, AS INSTÂNCIAS devem sempre ser iguais a 2.

Execute o script Bash

Você pode usar o `deploy-vsphere-ovftool.sh` script Bash e o arquivo de configuração deploy-vsphere-

ovftool.ini modificado para automatizar a implantação de nós do StorageGRID no VMware vSphere.

Antes de começar

Você criou um arquivo de configuração deploy-vsphere-ovftool.ini para o seu ambiente.

Você pode usar a ajuda disponível com o script Bash inserindo os comandos de ajuda (`-h/--help`). Por exemplo:

```
./deploy-vsphere-ovftool.sh -h
```

ou

```
./deploy-vsphere-ovftool.sh --help
```

Passos

1. Faça login na máquina Linux que você está usando para executar o script Bash.
2. Mude para o diretório onde você extraiu o arquivo de instalação.

   Por exemplo:

   ```
   cd StorageGRID-Webscale-version/vsphere
   ```

3. Para implantar todos os nós de grade, execute o script Bash com as opções apropriadas para o seu ambiente.

   Por exemplo:

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
   vsphere-ovftool.ini
   ```

4. Se um nó de grade não conseguir implantar por causa de um erro, resolva o erro e execute novamente o script Bash apenas para esse nó.

   Por exemplo:

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
   -node="DC1-S3" ./deploy-vsphere-ovftool.ini
   ```

A implantação é concluída quando o status de cada nó é "passado".

```
Deployment Summary
+-----------------------------+----------+----------------------+
| node                        | attempts | status               |
+-----------------------------+----------+----------------------+
| DC1-ADM1                    |        1 | Passed               |
| DC1-G1                      |        1 | Passed               |
| DC1-S1                      |        1 | Passed               |
| DC1-S2                      |        1 | Passed               |
| DC1-S3                      |        1 | Passed               |
+-----------------------------+----------+----------------------+
```

Automatize a configuração do StorageGRID

Depois de implantar os nós de grade, você pode automatizar a configuração do sistema StorageGRID.

Antes de começar

- Você sabe a localização dos seguintes arquivos do arquivo de instalação.

Nome do ficheiro	Descrição
configure-StorageGRID.py	Script Python usado para automatizar a configuração
configure-StorageGRID.sample.json	Exemplo de arquivo de configuração para uso com o script
configure-StorageGRID.blank.json	Arquivo de configuração em branco para uso com o script

- Criou um `configure-storagegrid.json` ficheiro de configuração. Para criar este ficheiro, pode modificar o ficheiro de configuração de exemplo (`configure-storagegrid.sample.json`) ou o ficheiro de configuração em branco (`configure-storagegrid.blank.json`).

  Você pode usar o `configure-storagegrid.py` script Python e o `configure-storagegrid.json` arquivo de configuração de grade para automatizar a configuração do seu sistema StorageGRID.

  > Você também pode configurar o sistema usando o Gerenciador de Grade ou a API de Instalação.

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Mude para o diretório onde você extraiu o arquivo de instalação.

   Por exemplo:

```
cd StorageGRID-Webscale-version/platform
```

```
`platform`onde está debs, rpms ou vsphere.
```

3. Execute o script Python e use o arquivo de configuração que você criou.

   Por exemplo:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Resultado

Um arquivo do Pacote de recuperação `.zip` é gerado durante o processo de configuração e é baixado para o diretório onde você está executando o processo de instalação e configuração. Você deve fazer backup do arquivo do pacote de recuperação para que você possa recuperar o sistema StorageGRID se um ou mais nós de grade falhar. Por exemplo, copie-o para um local de rede seguro e de backup e para um local seguro de armazenamento em nuvem.

> 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.

Se você especificou que senhas aleatórias devem ser geradas, abra o `Passwords.txt` arquivo e procure as senhas necessárias para acessar seu sistema StorageGRID.

```
######################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

O sistema StorageGRID é instalado e configurado quando é apresentada uma mensagem de confirmação.

```
StorageGRID has been configured and installed.
```

Informações relacionadas

- "Navegue até o Gerenciador de Grade"
- "API REST de instalação"

Implantar nós de grade de máquina virtual (VMware)

Colete informações sobre seu ambiente de implantação

Antes de implantar nós de grade, você deve coletar informações sobre a configuração de rede e o ambiente VMware.

> É mais eficiente executar uma única instalação de todos os nós, em vez de instalar alguns nós agora e alguns nós depois.

Informações da VMware

Você deve acessar o ambiente de implantação e coletar informações sobre o ambiente VMware, as redes criadas para as redes Grid, Admin e Client e os tipos de volume de armazenamento que você planeja usar para os nós de armazenamento.

Você deve coletar informações sobre seu ambiente VMware, incluindo o seguinte:

- O nome de usuário e a senha de uma conta do VMware vSphere que tem permissões apropriadas para concluir a implantação.
- Informações de configuração de host, datastore e rede para cada máquina virtual de nó StorageGRID.

> O VMware Live vMotion faz com que o tempo do relógio da máquina virtual salte e não é suportado para nós de grade de qualquer tipo. Embora raros, tempos de clock incorretos podem resultar em perda de dados ou atualizações de configuração.

Informações da rede de grelha

Você deve coletar informações sobre a rede da VMware criada para a rede de grade do StorageGRID (obrigatório), incluindo:

- O nome da rede.
- O método utilizado para atribuir endereços IP, estáticos ou DHCP.
  - Se você estiver usando endereços IP estáticos, os detalhes de rede necessários para cada nó de grade (endereço IP, gateway, máscara de rede).
  - Se estiver a utilizar DHCP, o endereço IP do nó de administração principal na rede de grelha. Consulte "Como os nós de grade descobrem o nó de administração principal" para obter mais informações.

Informações da rede de administração

Para nós que serão conetados à rede de administração StorageGRID opcional, você deve coletar informações sobre a rede VMware criada para essa rede, incluindo:

- O nome da rede.
- O método utilizado para atribuir endereços IP, estáticos ou DHCP.
  - Se você estiver usando endereços IP estáticos, os detalhes de rede necessários para cada nó de grade (endereço IP, gateway, máscara de rede).
  - Se estiver a utilizar DHCP, o endereço IP do nó de administração principal na rede de grelha. Consulte "Como os nós de grade descobrem o nó de administração principal" para obter mais informações.
- A lista de sub-rede externa (ESL) para a rede de administração.

Informações da rede do cliente

Para os nós que serão conetados à rede cliente StorageGRID opcional, você deve coletar informações sobre a rede VMware criada para essa rede, incluindo:

- O nome da rede.
- O método utilizado para atribuir endereços IP, estáticos ou DHCP.
- Se você estiver usando endereços IP estáticos, os detalhes de rede necessários para cada nó de grade (endereço IP, gateway, máscara de rede).

Informações sobre interfaces adicionais

Opcionalmente, você pode adicionar interfaces de tronco ou acesso à VM no vCenter após instalar o 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).

As interfaces adicionadas são exibidas na página interfaces VLAN e na página grupos HA no Gerenciador de Grade.

- Se você adicionar uma interface de tronco, configure uma ou mais interfaces VLAN para cada nova interface pai. "Configurar interfaces VLAN"Consulte .
- Se você adicionar uma interface de acesso, será necessário adicioná-la diretamente aos grupos de HA. "configurar grupos de alta disponibilidade"Consulte .

Volumes de storage para nós de storage virtual

Você deve coletar as seguintes informações para nós de storage baseados em máquina virtual:

- O número e o tamanho dos volumes de armazenamento (LUNs de armazenamento) que pretende adicionar. "Requisitos de storage e desempenho"Consulte .

Informações de configuração da grade

Você deve coletar informações para configurar sua grade:

- Licença de grade
- Endereços IP do servidor NTP (Network Time Protocol)
- Endereços IP do servidor DNS

Como os nós de grade descobrem o nó de administração principal

Os nós de grade se comunicam com o nó de administração principal para configuração e gerenciamento. Cada nó de grade deve saber o endereço IP do nó de administração principal na rede de grade.

Para garantir que um nó de grade possa acessar o nó Admin principal, você pode fazer um dos seguintes procedimentos ao implantar o nó:

- Você pode usar o parâmetro Admin_IP para inserir o endereço IP do nó de administrador principal manualmente.
- Você pode omitir o parâmetro ADMIN_IP para que o nó de grade descubra o valor automaticamente. A

deteção automática é especialmente útil quando a rede de Grade usa DHCP para atribuir o endereço IP ao nó Admin principal.

A deteção automática do nó de administração principal é realizada usando um sistema de nome de domínio multicast (mDNS). Quando o nó de administração principal é iniciado pela primeira vez, ele publica seu endereço IP usando mDNS. Outros nós na mesma sub-rede podem então consultar o endereço IP e adquiri-lo automaticamente. No entanto, como o tráfego IP multicast não é normalmente roteável entre sub-redes, os nós em outras sub-redes não podem adquirir o endereço IP do nó de administração principal diretamente.

Se utilizar a deteção automática:

- Você deve incluir a configuração Admin_IP para pelo menos um nó de grade em todas as sub-redes às quais o nó Admin principal não esteja diretamente conetado. Esse nó de grade publicará o endereço IP do nó de administrador principal para outros nós na sub-rede para serem detetados com mDNS.
- Certifique-se de que a sua infra-estrutura de rede suporta a passagem de tráfego IP multi-cast dentro de uma sub-rede.

Implante um nó StorageGRID como uma máquina virtual

Você usa o VMware vSphere Web Client para implantar cada nó de grade como uma máquina virtual. Durante a implantação, cada nó de grade é criado e conetado a uma ou mais redes StorageGRID.

Se precisar implantar qualquer nó de storage do dispositivo StorageGRID, "Implante o nó de storage do dispositivo" consulte .

Opcionalmente, você pode remapear portas de nós ou aumentar as configurações de CPU ou memória para o nó antes de ligá-lo.

Antes de começar

- Você analisou como "planeje e prepare-se para a instalação"e compreende os requisitos de software, CPU e RAM, armazenamento e desempenho.
- Você está familiarizado com o VMware vSphere Hypervisor e tem experiência na implantação de máquinas virtuais nesse ambiente.

O `open-vm-tools` pacote, uma implementação de código aberto semelhante ao VMware Tools, está incluído na máquina virtual StorageGRID. Você não precisa instalar o VMware Tools manualmente.

- Você baixou e extraiu a versão correta do arquivo de instalação do StorageGRID para VMware.

Se você estiver implantando o novo nó como parte de uma operação de expansão ou recuperação, use a versão do StorageGRID que está sendo executada atualmente na grade.

- Você tem o (`.vmdk`arquivo StorageGRID Virtual Machine Disk):

```
NetApp-SG-version-SHA.vmdk
```

- Você tem os `.ovf` arquivos e `.mf` para cada tipo de nó de grade que está implantando:

Nome do ficheiro	Descrição
vsphere-primary-admin.ovf vsphere-primary-admin.mf	O arquivo de modelo e o arquivo de manifesto para o nó de administração principal.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	O arquivo de modelo e o arquivo de manifesto para um nó de administração não primário.
vsphere-storage.ovf vsphere-storage.mf	O arquivo de modelo e o arquivo de manifesto para um nó de armazenamento.
vsphere-gateway.ovf vsphere-gateway.mf	O arquivo de modelo e o arquivo de manifesto para um Gateway Node.

- Os `.vdmk` ficheiros , `.ovf`, e `.mf` estão todos no mesmo diretório.
- Você tem um plano para minimizar domínios de falha. Por exemplo, você não deve implantar todos os nós do Gateway em um único host do vSphere ESXi.

> Em uma implantação de produção, não execute mais de um nó de armazenamento em uma única máquina virtual. Não execute várias máquinas virtuais no mesmo host ESXi se isso criar um problema inaceitável de domínio de falha.

- Se você estiver implantando um nó como parte de uma operação de expansão ou recuperação, terá o "Instruções para expandir um sistema StorageGRID" ou o "instruções de recuperação e manutenção".
- Se você estiver implantando um nó StorageGRID como uma máquina virtual com armazenamento atribuído a partir de um sistema NetApp ONTAP, você confirmou que o volume não tem uma política de disposição em camadas do FabricPool ativada. Por exemplo, se um nó do StorageGRID estiver sendo executado como uma máquina virtual em um host VMware, verifique se o volume que faz o backup do datastore para o nó 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.

Sobre esta tarefa

Siga estas instruções para implantar inicialmente nós VMware, adicionar um novo nó VMware em uma expansão ou substituir um nó VMware como parte de uma operação de recuperação. Exceto conforme observado nas etapas, o procedimento de implantação do nó é o mesmo para todos os tipos de nó, incluindo nós de administração, nós de storage e nós de gateway.

Se estiver a instalar um novo sistema StorageGRID:

- Você pode implantar nós em qualquer ordem.
- Você deve garantir que cada máquina virtual possa se conetar ao nó de administração principal pela rede de grade.

- Você deve implantar todos os nós de grade antes de configurar a grade.

Se você estiver executando uma operação de expansão ou recuperação:

- Você deve garantir que a nova máquina virtual possa se conetar a todos os outros nós pela rede de Grade.

Se você precisar remapear qualquer uma das portas do nó, não ligue o novo nó até que a configuração de remapeamento de porta esteja concluída.

Passos

1. Usando o vCenter, implante um modelo OVF.

   Se especificar um URL, aponte para uma pasta que contenha os seguintes ficheiros. Caso contrário, selecione cada um desses arquivos em um diretório local.

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-node.ovf
   vsphere-node.mf
   ```

   Por exemplo, se este for o primeiro nó que você está implantando, use esses arquivos para implantar o nó de administrador principal do seu sistema StorageGRID:

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-primary-admin.ovf
   vsphere-primary-admin.mf
   ```

2. Forneça um nome para a máquina virtual.

   A prática padrão é usar o mesmo nome para a máquina virtual e o nó de grade.

3. Coloque a máquina virtual no vApp ou pool de recursos apropriado.
4. Se você estiver implantando o nó Admin principal, leia e aceite o Contrato de Licença de Usuário final.

   Dependendo da sua versão do vCenter, a ordem das etapas variará para aceitar o Contrato de Licença de Usuário final, especificando o nome da máquina virtual e selecionando um datastore.

5. Selecione armazenamento para a máquina virtual.

   Se você estiver implantando um nó como parte da operação de recuperação, execute as instruções no etapa de recuperação de armazenamento para adicionar novos discos virtuais, reconete discos rígidos virtuais do nó de grade com falha ou ambos.

   Ao implantar um nó de armazenamento, use 3 ou mais volumes de armazenamento, com cada volume de armazenamento de 4 TB ou maior. Tem de atribuir pelo menos 4 TB ao volume 0.

O arquivo .ovf do nó de storage define vários VMDKs para armazenamento. A menos que esses VMDKs atendam aos requisitos de storage, você deve removê-los e atribuir VMDKs ou RDMs apropriados para armazenamento antes de ligar o nó. Os VMDKs são mais comumente usados em ambientes VMware 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, mais de 100 MB).

Algumas instalações do StorageGRID podem usar volumes de storage maiores e mais ativos do que os workloads virtualizados típicos. Talvez seja necessário ajustar alguns parâmetros do hipervisor, como `MaxAddressableSpaceTB`, para obter o desempenho ideal. Se você encontrar desempenho insatisfatório, entre em Contato com seu recurso de suporte de virtualização para determinar se o ambiente pode se beneficiar do ajuste de configuração específico do workload.

6. Selecione redes.

   Determine quais redes StorageGRID o nó usará selecionando uma rede de destino para cada rede de origem.

   - A rede de Grade é necessária. Você deve selecionar uma rede de destino no ambiente vSphere. A rede de grade é usada para todo o tráfego interno do StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes. Todos os nós na rede de Grade devem ser capazes de se comunicar com todos os outros nós.
   - Se você usar a rede Admin, selecione uma rede de destino diferente no ambiente vSphere. Se não utilizar a rede Admin, selecione o mesmo destino que selecionou para a rede de grelha.
   - Se você usar a rede do cliente, selecione uma rede de destino diferente no ambiente vSphere. Se você não usar a rede do cliente, selecione o mesmo destino que você selecionou para a rede de grade.
   - Se você usar uma rede Admin ou Client, os nós não precisam estar nas mesmas redes Admin ou Client.

7. Para **Personalizar modelo**, configure as propriedades de nó StorageGRID necessárias.

   a. Introduza o **Nome do nó**.

      Se você estiver recuperando um nó de grade, insira o nome do nó que está recuperando.

   b. Use a lista suspensa **senha de instalação temporária** para especificar uma senha de instalação temporária, de modo que você possa acessar o console da VM ou a API de instalação do StorageGRID, ou usar SSH, antes que o novo nó se una à grade.

      A senha de instalação temporária só é usada durante a instalação do nó. Depois que um nó for adicionado à grade, você poderá acessá-lo usando o "senha do console do nó", que está listado no `Passwords.txt` arquivo no Pacote de recuperação.

      - **Use node name**: O valor fornecido para o campo **Node name** é usado como a senha de instalação temporária.
      - **Use a senha personalizada**: Uma senha personalizada é usada como a senha de instalação temporária.

- **Desativar senha**: Nenhuma senha de instalação temporária será usada. Se precisar acessar a VM para depurar problemas de instalação, "Solucionar problemas de instalação"consulte .

c. Se você selecionou **usar senha personalizada**, especifique a senha de instalação temporária que deseja usar no campo **Senha personalizada**.

d. Na seção **Grid Network (eth0)**, selecione STATIC (ESTÁTICO) ou DHCP (DHCP) para a **Grid network IP Configuration (Configuração IP da rede de grade)**.

- Se você SELECIONAR ESTÁTICO, digite **Grid network IP**, **Grid network mask**, **Grid network gateway** e **Grid network MTU**.
- Se você selecionar DHCP, **Grid network IP**, **Grid network mask** e **Grid network gateway** serão atribuídos automaticamente.

e. No campo **Primary Admin IP** (IP de administrador principal), introduza o endereço IP do nó de administração principal para a rede de grelha.

Esta etapa não se aplica se o nó que você está implantando for o nó Admin principal.

Se você omitir o endereço IP do nó de administrador principal, o endereço IP será automaticamente descoberto se o nó de administrador principal, ou pelo menos um outro nó de grade com ADMIN_IP configurado, estiver presente na mesma sub-rede. No entanto, recomenda-se definir aqui o endereço IP do nó de administração principal.

a. Na seção **Admin Network (eth1)**, selecione ESTÁTICO, DHCP ou DESATIVADO para a **Admin network IP Configuration**.

- Se não pretender utilizar a rede de administração, selecione DISABLED (DESATIVADA) e introduza **0,0.0,0** para o IP da rede de administração. Você pode deixar os outros campos em branco.
- Se você SELECIONAR ESTÁTICO, digite **Admin network IP**, **Admin network mask**, **Admin network gateway** e **Admin network MTU**.
- Se selecionar ESTÁTICO, introduza a lista de sub-redes externas * da rede de administração. Você também deve configurar um gateway.
- Se você selecionar DHCP, **Admin network IP**, **Admin network mask** e **Admin network gateway** serão atribuídos automaticamente.

b. Na seção **rede do cliente (eth2)**, selecione ESTÁTICO, DHCP ou DESATIVADO para a **Configuração IP da rede do cliente**.

- Se não pretender utilizar a rede do cliente, selecione DISABLED (DESATIVADA) e introduza **0,0.0,0** para o IP da rede do cliente. Você pode deixar os outros campos em branco.
- Se SELECIONAR ESTÁTICO, introduza **IP de rede do cliente**, **Máscara de rede do cliente**, **gateway de rede do cliente** e **MTU de rede do cliente**.
- Se você selecionar DHCP, **IP de rede do cliente**, **máscara de rede do cliente** e **gateway de rede do cliente** serão atribuídos automaticamente.

8. Revise a configuração da máquina virtual e faça as alterações necessárias.
9. Quando estiver pronto para concluir, selecione **Finish** para iniciar o upload da máquina virtual.
10. se você implantou este nó como parte da operação de recuperação e esta não é uma recuperação de nó completo, execute estas etapas após a conclusão da implantação:

a. Clique com o botão direito do rato na máquina virtual e selecione **Editar definições**.

b. Selecione cada disco rígido virtual padrão designado para armazenamento e selecione **Remover**.

c. Dependendo das circunstâncias de recuperação de dados, adicione novos discos virtuais de acordo com seus requisitos de armazenamento, reconete quaisquer discos rígidos virtuais preservados do nó de grade com falha removido anteriormente ou ambos.

   Observe as seguintes diretrizes importantes:

   - Se você estiver adicionando novos discos, use o mesmo tipo de dispositivo de armazenamento que estava em uso antes da recuperação do nó.
   - O arquivo .ovf do nó de storage define vários VMDKs para armazenamento. A menos que esses VMDKs atendam aos requisitos de storage, você deve removê-los e atribuir VMDKs ou RDMs apropriados para armazenamento antes de ligar o nó. Os VMDKs são mais comumente usados em ambientes VMware 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, mais de 100 MB).

11. se você precisar remapear as portas usadas por esse nó, siga estas etapas.

Talvez seja necessário remapear uma porta se as políticas de rede corporativa restringirem o acesso a uma ou mais portas usadas pelo StorageGRID. Consulte "diretrizes de rede"para obter informações sobre as portas usadas pelo StorageGRID.

> Não remapegue as portas usadas nos pontos de extremidade do balanceador de carga.

a. Selecione a nova VM.
b. Na guia Configurar, selecione **Configurações** > **Opções do vApp**. A localização do **vApp Options** depende da versão do vCenter.
c. Na tabela **Properties**, localize PORT_REMAP_INBOUND e port_REMAP.
d. Para mapear simetricamente as comunicações de entrada e saída para uma porta, selecione **port_REMAP**.

> Se apenas Port_REMAP estiver definido, o mapeamento que você especificar se aplica às comunicações de entrada e saída. Se Port_REMAP_INBOUND também for especificado, PORT_REMAP se aplica apenas às comunicações de saída.

   i. Selecione **Definir valor**.
   ii. Introduza o mapeamento de portas:

   `<network type>/<protocol>/<default port used by grid node>/<new port>`

   `<network type>` é grid, admin ou client, e `<protocol>` é tcp ou udp.

   Por exemplo, para remapear o tráfego ssh da porta 22 para a porta 3022, digite:

   `client/tcp/22/3022`

   Você pode remapear várias portas usando uma lista separada por vírgulas.

   Por exemplo:

`client/tcp/18082/443, client/tcp/18083/80`

i. Selecione **OK**.

e. Para especificar a porta usada para comunicações de entrada para o nó, selecione **PORT_REMAP_INBOUND**.

> Se você especificar PORT_REMAP_INBOUND e não especificar um valor para PORT_REMAP, as comunicações de saída para a porta não serão alteradas.

i. Selecione **Definir valor**.

ii. Introduza o mapeamento de portas:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>
```

`<network type>` é grid, admin ou client, e `<protocol>` é tcp ou udp.

Por exemplo, para remapear o tráfego SSH de entrada que é enviado para a porta 3022 para que seja recebido na porta 22 pelo nó da grade, digite o seguinte:

```
client/tcp/3022/22
```

Você pode remapear várias portas de entrada usando uma lista separada por vírgulas.

Por exemplo:

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. Selecione **OK**

12. Se você quiser aumentar a CPU ou a memória do nó a partir das configurações padrão:
    a. Clique com o botão direito do rato na máquina virtual e selecione **Editar definições**.
    b. Altere o número de CPUs ou a quantidade de memória, conforme necessário.

       Defina a **reserva de memória** para o mesmo tamanho que a **memória** alocada à máquina virtual.

    c. Selecione **OK**.
13. Ligue a máquina virtual.

Depois de terminar

Se você implantou esse nó como parte de um procedimento de expansão ou recuperação, retorne a essas instruções para concluir o procedimento.

Configurar a grade e a instalação completa (VMware)

Navegue até o Gerenciador de Grade

Use o Gerenciador de Grade para definir todas as informações necessárias para configurar o sistema StorageGRID.

Antes de começar

O nó Admin principal deve ser implantado e ter concluído a sequência inicial de inicialização.

Passos

1. Abra o navegador da Web e navegue até:

   `https://primary_admin_node_ip`

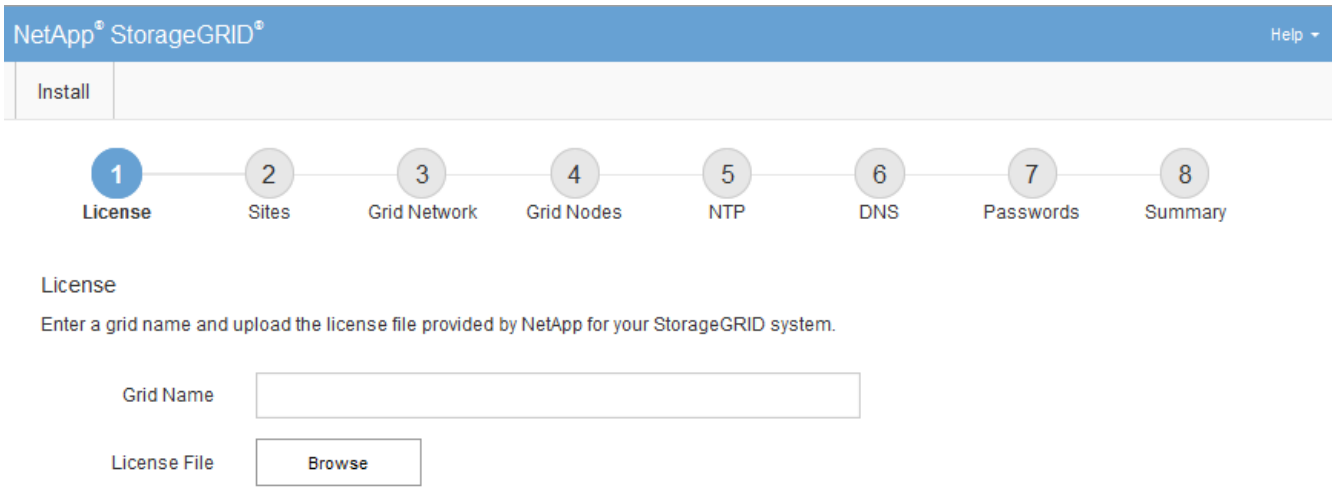
   Como alternativa, você pode acessar o Gerenciador de Grade na porta 8443:

   `https://primary_admin_node_ip:8443`

   Você pode usar o endereço IP do nó de administrador principal IP na rede de grade ou na rede de administração, conforme apropriado para a configuração da rede. Talvez seja necessário usar a opção de segurança/avançada no navegador para navegar para um certificado não confiável.

2. Gerencie uma senha temporária do instalador conforme necessário:
   - Se já tiver sido definida uma palavra-passe utilizando um destes métodos, introduza a palavra-passe para prosseguir.
     - Um usuário define a senha ao acessar o instalador anteriormente
     - A senha SSH/console foi importada automaticamente das propriedades OVF
   - Se não tiver sido definida uma palavra-passe, defina opcionalmente uma palavra-passe para proteger o instalador do StorageGRID.
3. Selecione **Instalar um sistema StorageGRID**.

   A página usada para configurar uma grade StorageGRID é exibida.



Especifique as informações da licença do StorageGRID

Você deve especificar o nome do seu sistema StorageGRID e fazer o upload do arquivo de licença fornecido pelo NetApp.

Passos

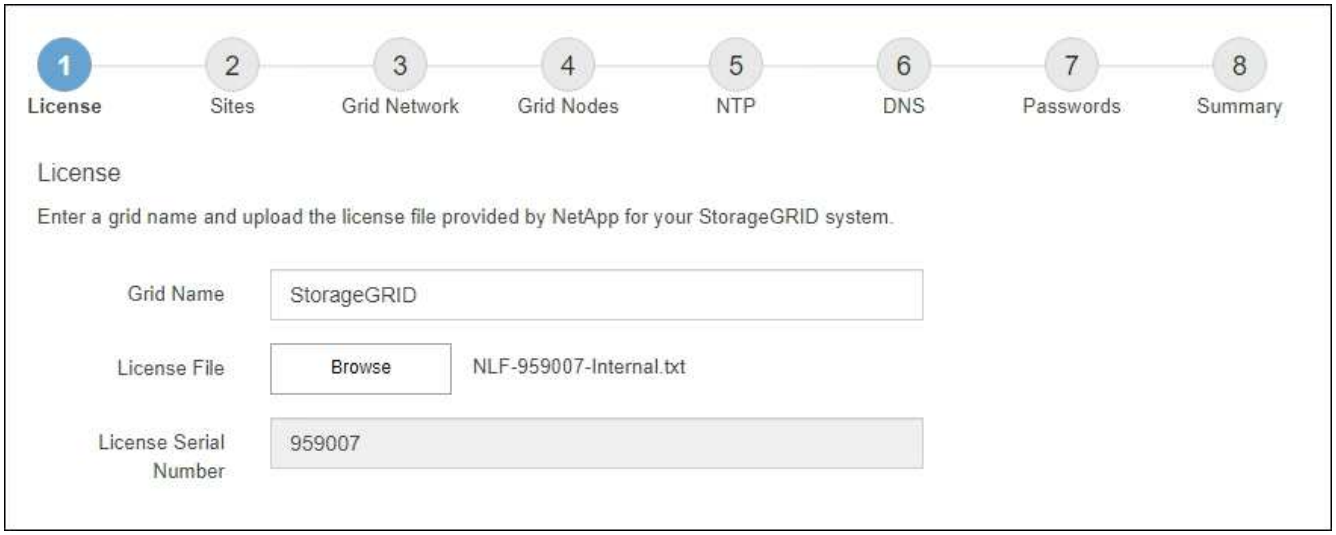
1. Na página Licença, insira um nome significativo para o seu sistema StorageGRID no campo **Nome da Grade**.

   Após a instalação, o nome é exibido na parte superior do menu nós.

2. Selecione **Procurar**, localize o ficheiro de licença NetApp (`NLF-unique-id.txt`) e selecione **abrir**.

   O ficheiro de licença é validado e o número de série é apresentado.

   > O arquivo de instalação do StorageGRID inclui uma licença gratuita que não fornece nenhum direito de suporte para o produto. Você pode atualizar para uma licença que oferece suporte após a instalação.



3. Selecione **seguinte**.

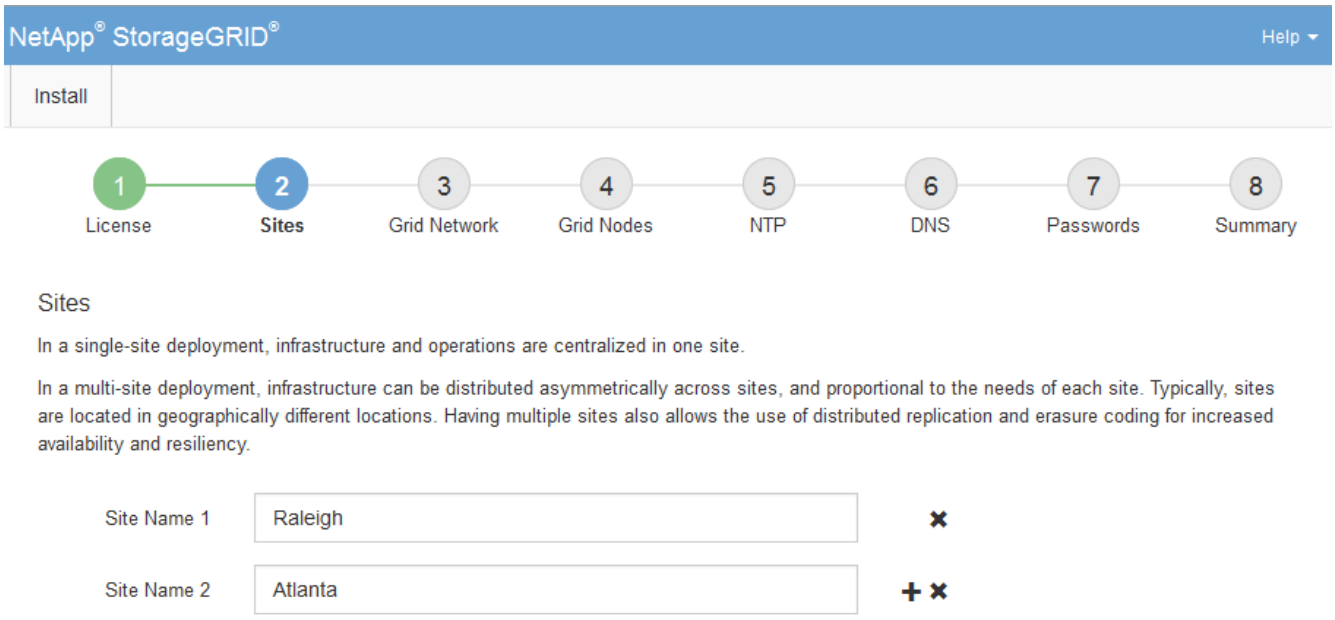
Adicione sites

Você deve criar pelo menos um site quando estiver instalando o StorageGRID. Você pode criar sites adicionais para aumentar a confiabilidade e a capacidade de storage do seu sistema StorageGRID.

Passos

1. Na página Sites, insira o **Nome do Site**.
2. Para adicionar sites adicionais, clique no sinal de adição ao lado da última entrada do site e digite o nome na nova caixa de texto **Nome do site**.

   Adicione tantos locais adicionais quanto necessário para a topologia da grade. Você pode adicionar até 16 sites.



3. Clique em **seguinte**.

Especifique as sub-redes da rede de Grade

Você deve especificar as sub-redes que são usadas na rede de Grade.

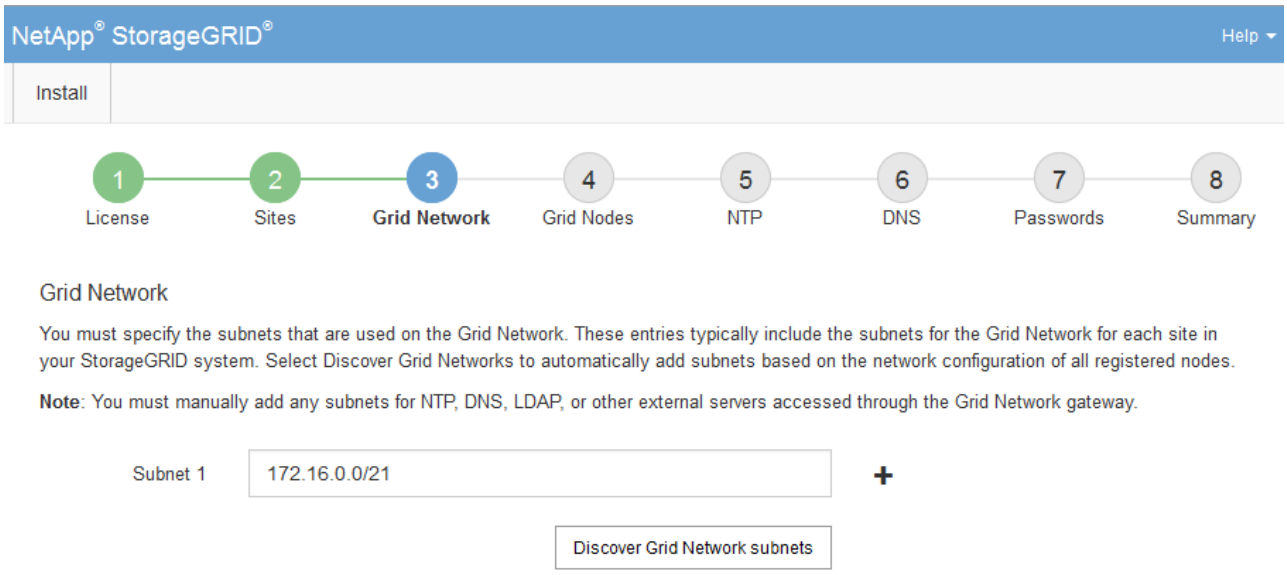
Sobre esta tarefa

As entradas de sub-rede incluem as sub-redes para a rede de Grade para cada site no seu sistema StorageGRID, juntamente com quaisquer sub-redes que precisam ser acessíveis através da rede de Grade.

Se você tiver várias sub-redes de grade, o gateway de rede de grade é necessário. Todas as sub-redes de grade especificadas devem ser acessíveis através deste gateway.

Passos

1. Especifique o endereço de rede CIDR para pelo menos uma rede de Grade na caixa de texto **Subnet 1**.
2. Clique no sinal de mais ao lado da última entrada para adicionar uma entrada de rede adicional. Você deve especificar todas as sub-redes para todos os sites na rede de Grade.
   - Se você já implantou pelo menos um nó, clique em **descobrir sub-redes de redes de Grade** para preencher automaticamente a Lista de sub-redes de rede de Grade com as sub-redes relatadas pelos nós de grade que se registraram no Gerenciador de Grade.
   - Você deve adicionar manualmente quaisquer sub-redes para NTP, DNS, LDAP ou outros servidores externos acessados através do gateway de rede de Grade.



3. Clique em **seguinte**.

Aprovar nós de grade pendentes

Você deve aprovar cada nó de grade antes que ele possa ingressar no sistema StorageGRID.

Antes de começar

Você implantou todos os nós de grade de dispositivos virtuais e StorageGRID.

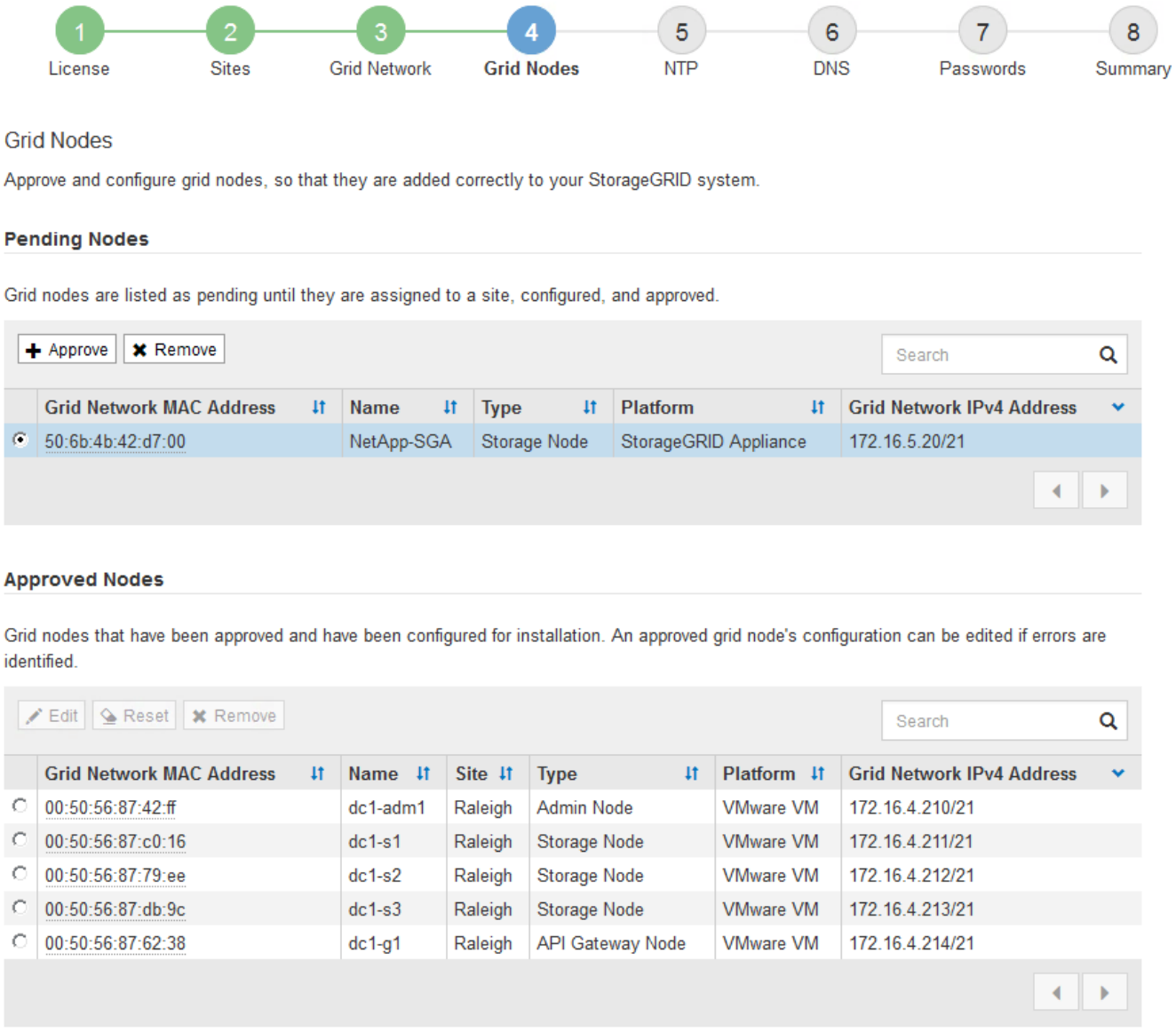
> É mais eficiente executar uma única instalação de todos os nós, em vez de instalar alguns nós agora e alguns nós depois.

Passos

1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade implantados.

> Se um nó de grade estiver ausente, confirme que ele foi implantado com sucesso e que tem o IP de rede de grade correto do nó de administrador principal definido para ADMIN_IP.

2. Selecione o botão de opção ao lado de um nó pendente que você deseja aprovar.



3. Clique em **Approve**.
4. Em Configurações gerais, modifique as configurações para as seguintes propriedades, conforme necessário:

   - **Site**: O nome do sistema do site para este nó de grade.
   - **Nome**: O nome do sistema para o nó. O nome padrão é o nome que você especificou quando configurou o nó.

     Os nomes de sistema são necessários para operações internas do StorageGRID e não podem ser alterados após a conclusão da instalação. No entanto, durante esta etapa do processo de instalação, você pode alterar os nomes do sistema conforme necessário.

     > Para um nó VMware, você pode alterar o nome aqui, mas essa ação não mudará o nome da máquina virtual no vSphere.

   - **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.

> 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.

- * Tipo de armazenamento* (somente nós de armazenamento): Especifique que um novo nó de armazenamento seja usado exclusivamente para dados, somente metadados ou ambos. As opções são **dados e metadados** ("combinados"), **somente dados** e **somente metadados**.

  > "Tipos de nós de storage"Consulte para obter informações sobre os requisitos para esses tipos de nós.

- **ADC Service** (somente nós de armazenamento): Selecione **Automático** para permitir que o sistema determine se o nó requer 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. Não é possível adicionar o serviço ADC a um nó depois que ele é implantado.

5. Na rede de Grade, modifique as configurações para as seguintes propriedades, conforme necessário:

   - **Endereço IPv4 (CIDR)**: O endereço de rede CIDR para a interface Grid Network (eth0 dentro do contentor). Por exemplo: 192.168.1.234/21
   - **Gateway**: O gateway Grid Network. Por exemplo: 192.168.0.1

     > O gateway é necessário se houver várias sub-redes de grade.

   > Se você selecionou DHCP para a configuração da rede de Grade e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

6. Se pretender configurar a rede de administração para o nó da grelha, adicione ou atualize as definições na secção rede de administração, conforme necessário.

   Insira as sub-redes de destino das rotas fora desta interface na caixa de texto **sub-redes (CIDR)**. Se houver várias sub-redes Admin, o gateway Admin é necessário.

   > Se você selecionou DHCP para a configuração da rede Admin e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

   Appliances: para um appliance StorageGRID, se a rede de administração não tiver sido configurada durante a instalação inicial usando o Instalador de appliance StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

   a. Reinicie o aparelho: No Instalador de dispositivos, selecione **Avançado** > **Reiniciar**.

      A reinicialização pode levar vários minutos.

   b. Selecione **Configure Networking** > **Link Configuration** e ative as redes apropriadas.

c. Selecione **Configurar rede** > **Configuração IP** e configure as redes ativadas.
d. Volte à página inicial e clique em **Iniciar instalação**.
e. No Gerenciador de Grade: Se o nó estiver listado na tabela de nós aprovados, remova o nó.
f. Remova o nó da tabela nós pendentes.
g. Aguarde que o nó reapareça na lista de nós pendentes.
h. Confirme se você pode configurar as redes apropriadas. Eles já devem ser preenchidos com as informações fornecidas na página Configuração IP do Instalador de dispositivos.

   Para obter informações adicionais, consulte o "Início rápido para instalação de hardware" para localizar as instruções do seu aparelho.

7. Se pretender configurar a rede do cliente para o nó da grelha, adicione ou atualize as definições na secção rede do cliente, conforme necessário. Se a rede do cliente estiver configurada, o gateway é necessário e ele se torna o gateway padrão para o nó após a instalação.

   > Se você selecionou DHCP para a configuração da rede do cliente e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não está dentro de um pool de endereços DHCP.

   Appliances: para um appliance StorageGRID, se a rede cliente não tiver sido configurada durante a instalação inicial usando o Instalador de appliance StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

   a. Reinicie o aparelho: No Instalador de dispositivos, selecione **Avançado** > **Reiniciar**.

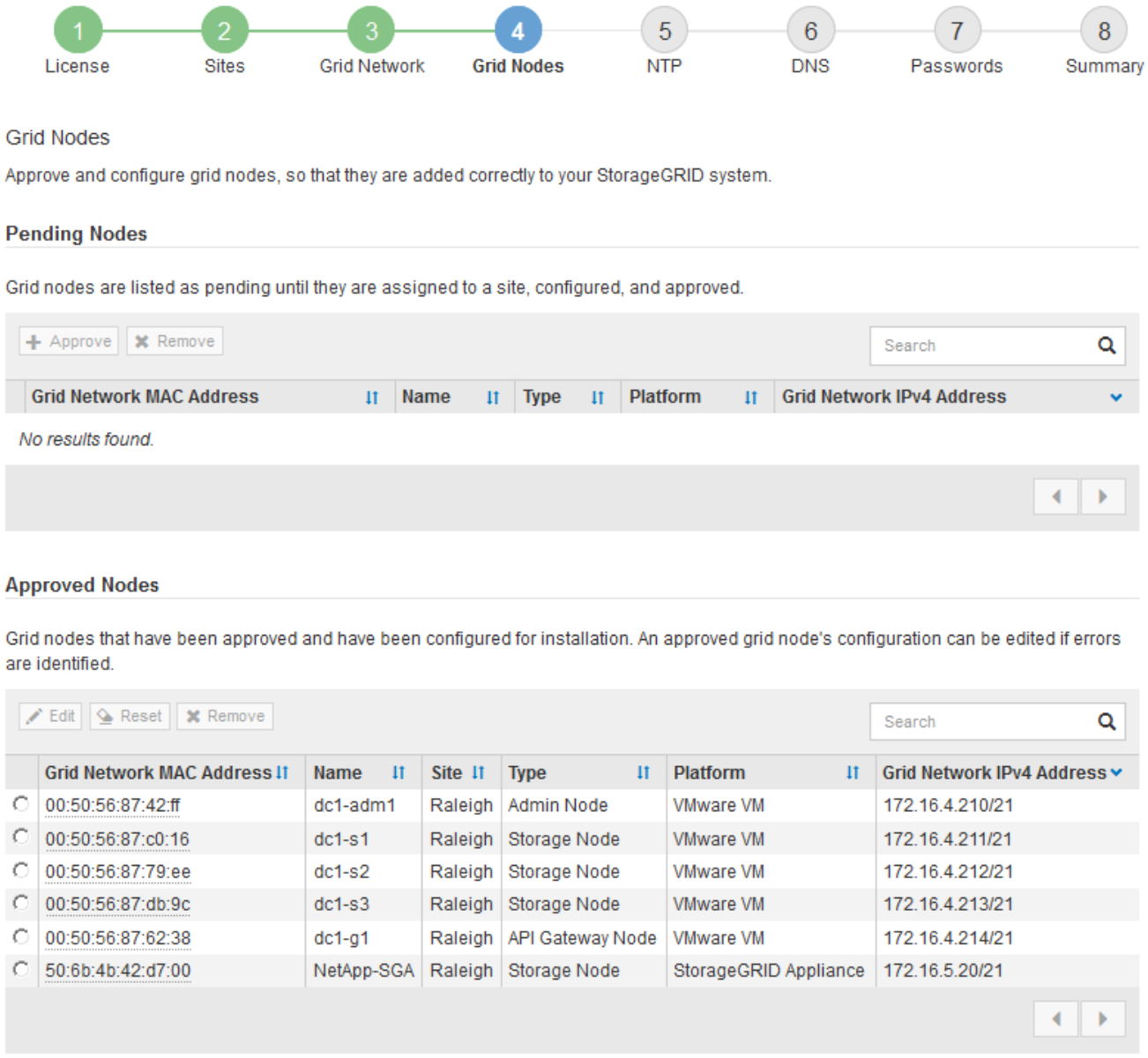
      A reinicialização pode levar vários minutos.

   b. Selecione **Configure Networking** > **Link Configuration** e ative as redes apropriadas.
   c. Selecione **Configurar rede** > **Configuração IP** e configure as redes ativadas.
   d. Volte à página inicial e clique em **Iniciar instalação**.
   e. No Gerenciador de Grade: Se o nó estiver listado na tabela de nós aprovados, remova o nó.
   f. Remova o nó da tabela nós pendentes.
   g. Aguarde que o nó reapareça na lista de nós pendentes.
   h. Confirme se você pode configurar as redes apropriadas. Eles já devem ser preenchidos com as informações fornecidas na página Configuração IP do Instalador de dispositivos.

      Para obter informações adicionais, consulte o "Início rápido para instalação de hardware" para localizar as instruções do seu aparelho.

8. Clique em **Salvar**.

   A entrada do nó de grade se move para a lista de nós aprovados.



9. Repita estas etapas para cada nó de grade pendente que você deseja aprovar.

   Você deve aprovar todos os nós que deseja na grade. No entanto, você pode retornar a esta página a qualquer momento antes de clicar em **Instalar** na página Resumo. Você pode modificar as propriedades de um nó de grade aprovado selecionando seu botão de opção e clicando em **Editar**.

10. Quando terminar de aprovar nós de grade, clique em **Next**.

Especifique as informações do servidor Network Time Protocol

Você deve especificar as informações de configuração do protocolo de tempo de rede (NTP) para o sistema StorageGRID, para que as operações executadas em servidores separados possam ser mantidas sincronizadas.

Sobre esta tarefa

Você deve especificar endereços IPv4 para os servidores NTP.

Tem de especificar servidores NTP externos. Os servidores NTP especificados devem usar o protocolo NTP.

Você deve especificar quatro 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"

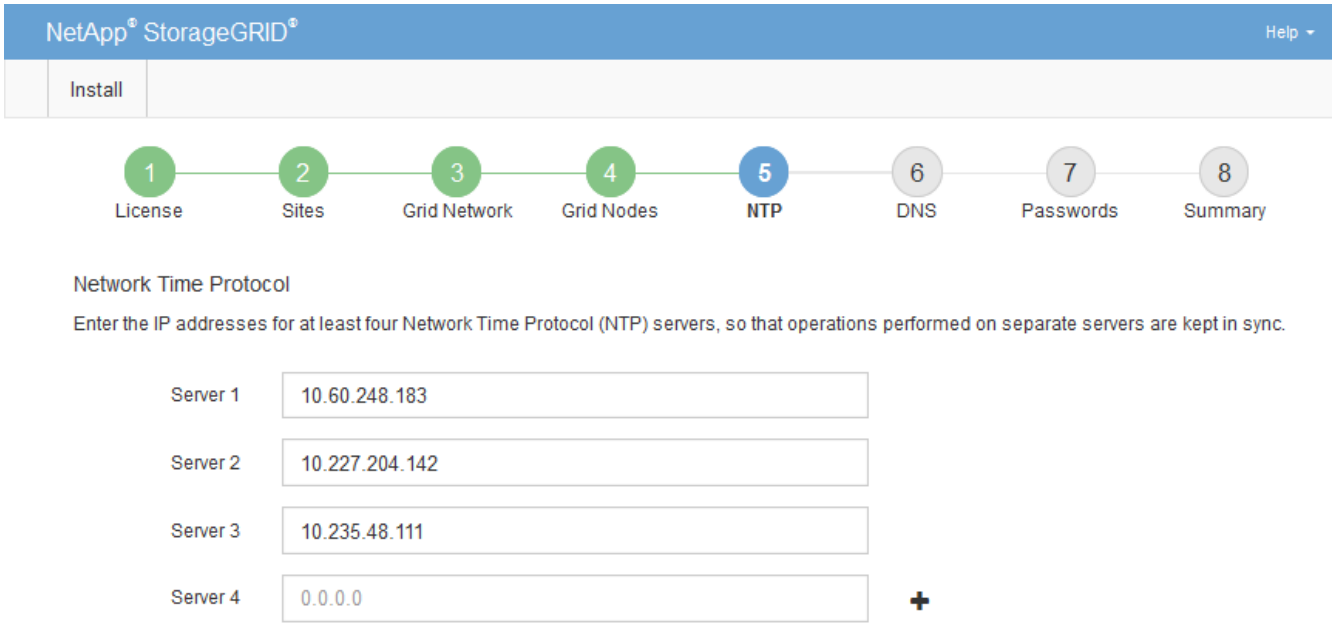
Os servidores NTP externos são usados pelos nós aos quais você atribuiu funções primárias NTP anteriormente.

> 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.

Execute verificações adicionais para VMware, como garantir que o hypervisor use a mesma fonte NTP que a máquina virtual e usar VMTools para desativar a sincronização de tempo entre o hypervisor e as máquinas virtuais StorageGRID.

Passos

1. Especifique os endereços IPv4 para pelo menos quatro servidores NTP nas caixas de texto **Server 1** para **Server 4**.
2. Se necessário, selecione o sinal de adição ao lado da última entrada para adicionar entradas adicionais do servidor.



3. Selecione **seguinte**.

Especifique as informações do servidor DNS

Você deve especificar informações de DNS para seu sistema StorageGRID, para que você possa acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

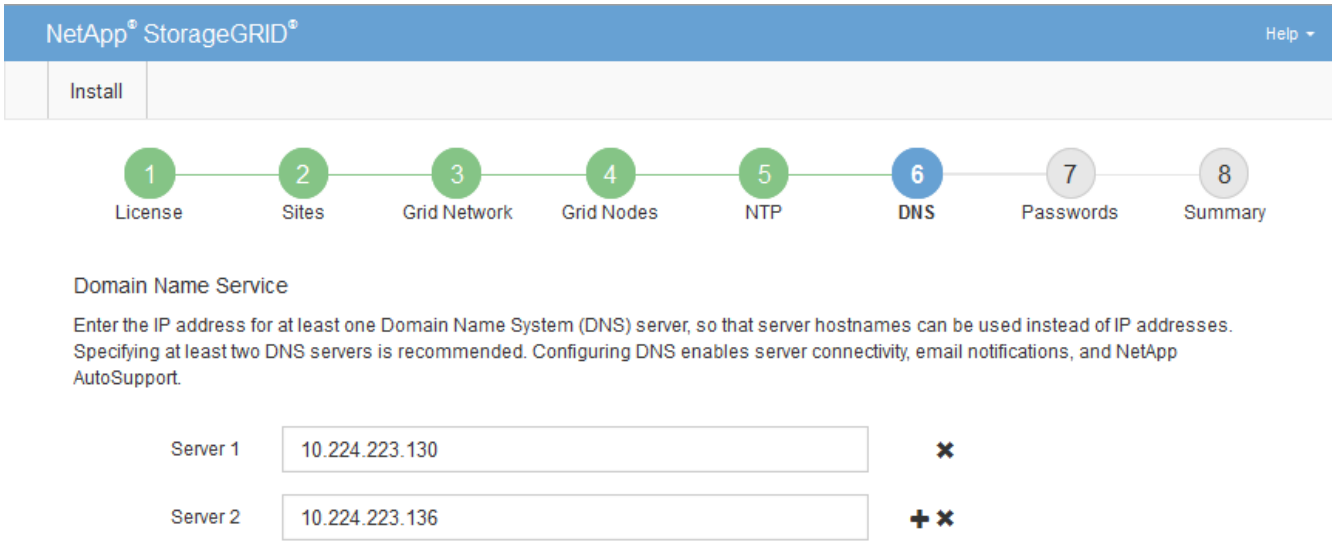
Especificar "Informações do servidor DNS" permite que você use nomes de host de nome de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações de e-mail e AutoSupport.

Para garantir o funcionamento correto, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três serão usados por causa das limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, pode "Personalize a lista de servidores DNS"usar um conjunto diferente de até três servidores DNS para nós individuais (normalmente todos os nós em um site).

Se possível, use servidores DNS que cada site pode acessar localmente para garantir que um site islanded possa resolver os FQDNs para destinos externos.

Passos

1. Especifique o endereço IPv4 para pelo menos um servidor DNS na caixa de texto **Server 1**.
2. Se necessário, selecione o sinal de adição ao lado da última entrada para adicionar entradas adicionais do servidor.



A prática recomendada é especificar pelo menos dois servidores DNS. Você pode especificar até seis servidores DNS.

3. Selecione **seguinte**.

Especifique as senhas do sistema StorageGRID

Como parte da instalação do sistema StorageGRID, você precisa inserir as senhas a serem usadas para proteger o sistema e executar tarefas de manutenção.

Sobre esta tarefa

Use a página Instalar senhas para especificar a senha de provisionamento e a senha de usuário raiz de gerenciamento de grade.

- A senha de provisionamento é usada como uma chave de criptografia e não é armazenada pelo sistema StorageGRID.
- Você deve ter a senha de provisionamento para procedimentos de instalação, expansão e manutenção, incluindo o download do Pacote de recuperação. Portanto, é importante que você armazene a senha de provisionamento em um local seguro.
- Você pode alterar a senha de provisionamento do Gerenciador de Grade se tiver a senha atual.
- A senha do usuário raiz de gerenciamento de grade pode ser alterada usando o Gerenciador de Grade.
- As senhas do console de linha de comando e SSH geradas aleatoriamente são armazenadas no `Passwords.txt` arquivo no Pacote de recuperação.

Passos

1. Em **frase-passe de aprovisionamento**, introduza a frase-passe de aprovisionamento que será necessária para efetuar alterações na topologia de grelha do seu sistema StorageGRID.

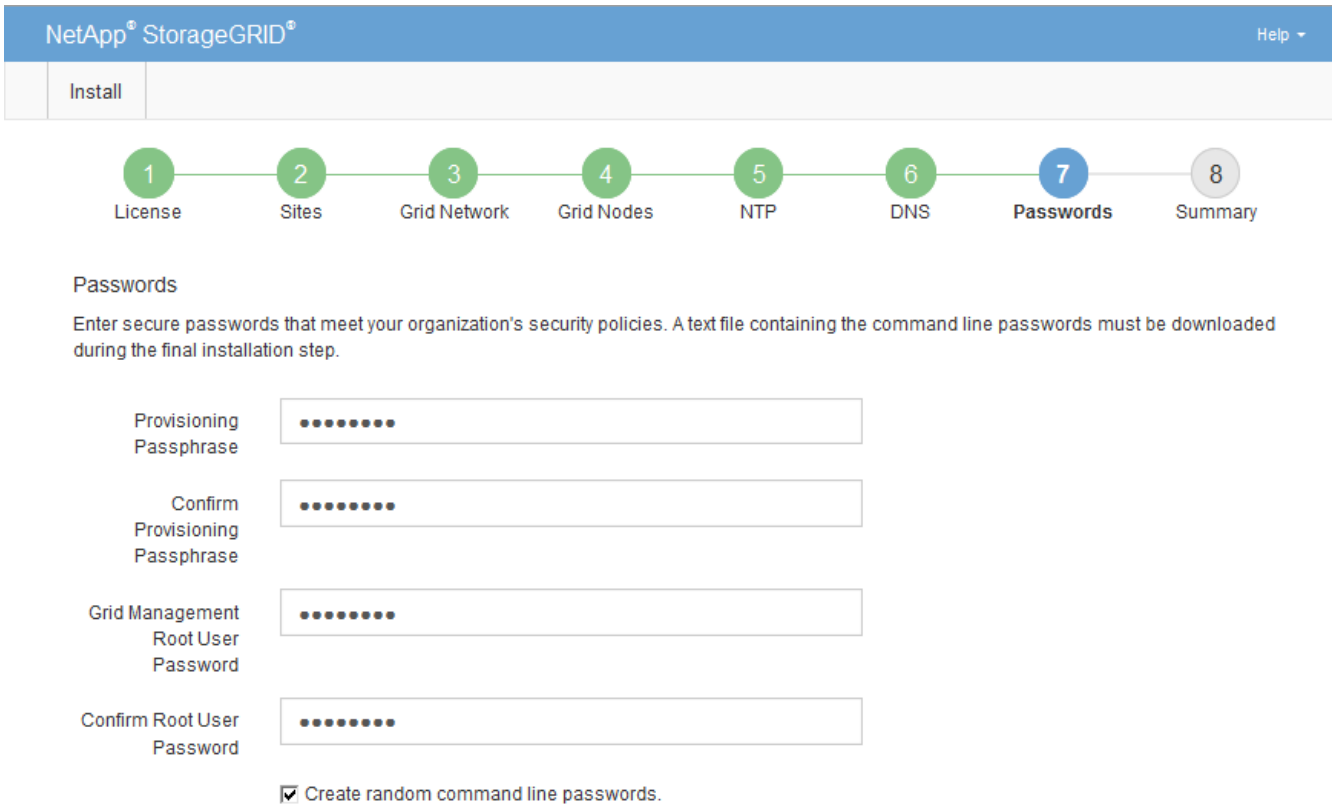
   Armazene a senha de provisionamento em um local seguro.

   > ⓘ Se após a conclusão da instalação e você quiser alterar a senha de provisionamento mais tarde, você pode usar o Gerenciador de Grade. Selecione **CONFIGURATION** > **Access control** > **Grid passwords**.

2. Em **Confirm Provisioning Passphrase** (confirmar frase-passe de aprovisionamento), volte a introduzir a frase-passe de aprovisionamento para a confirmar.
3. Em **Grid Management Root User Password**, insira a senha a ser usada para acessar o Grid Manager como usuário "root".

   Guarde a palavra-passe num local seguro.

4. Em **Confirm root User Password**, digite novamente a senha do Grid Manager para confirmá-la.



5. Se você estiver instalando uma grade para fins de prova de conceito ou demonstração, desmarque a caixa de seleção **criar senhas de linha de comando aleatórias**.

   Para implantações de produção, senhas aleatórias devem sempre ser usadas por razões de segurança. Limpar **criar senhas de linha de comando aleatórias** somente para grades de demonstração se você quiser usar senhas padrão para acessar nós de grade da linha de comando usando a conta "root" ou "admin".

   > Você será solicitado a baixar o arquivo do pacote de recuperação (`sgws-recovery-package-id-revision.zip`) depois de clicar em **Instalar** na página Resumo. Você deve "transfira este ficheiro"concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas `Passwords.txt` no arquivo, contido no arquivo Pacote de recuperação.

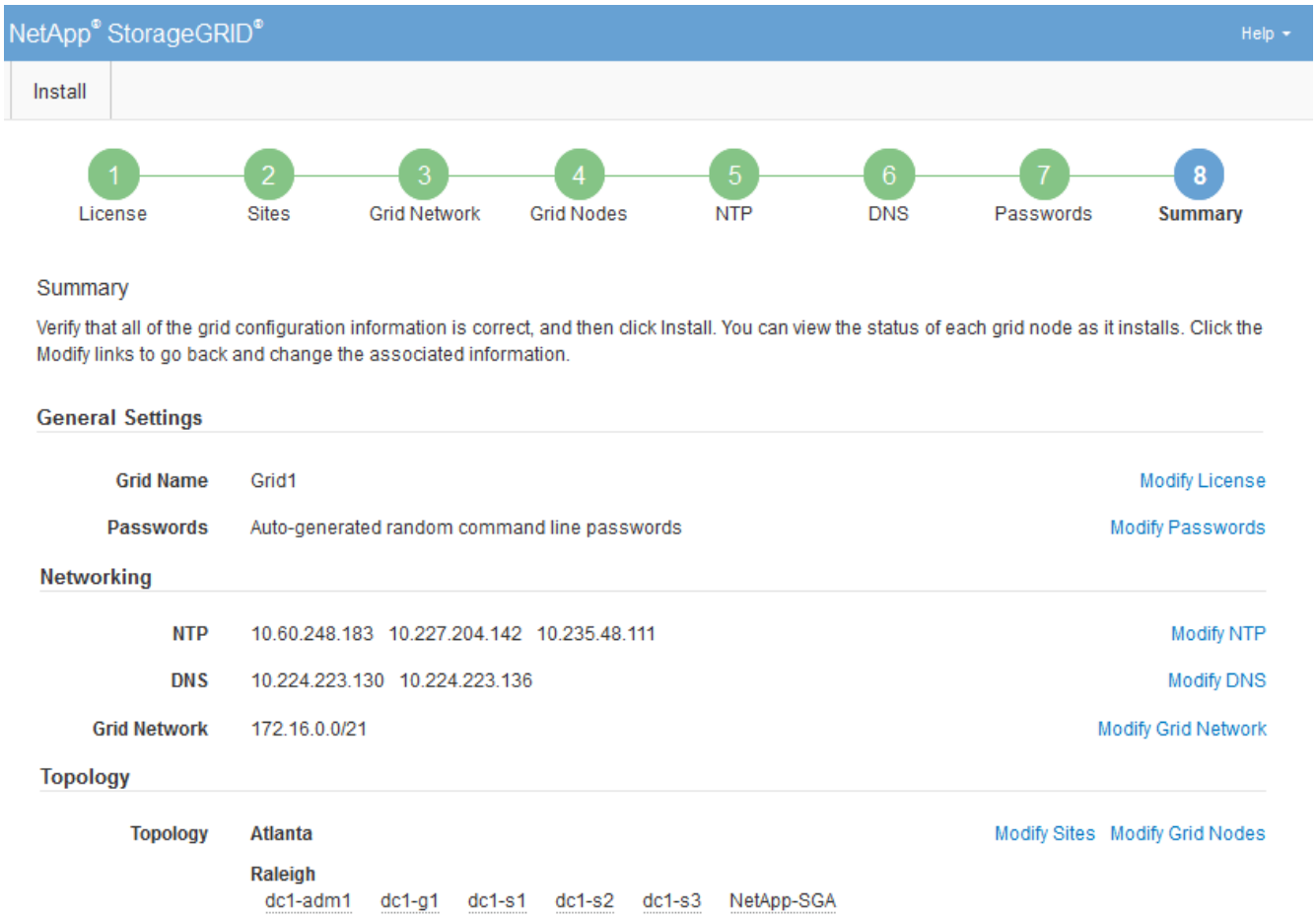
6. Clique em **seguinte**.

Revise sua configuração e conclua a instalação

Você deve analisar cuidadosamente as informações de configuração inseridas para garantir que a instalação seja concluída com êxito.

Passos

1. Veja a página **Summary**.



2. Verifique se todas as informações de configuração da grade estão corretas. Use os links Modificar na página Resumo para voltar e corrigir quaisquer erros.
3. Clique em **Instalar**.

> Se um nó estiver configurado para usar a rede do cliente, o gateway padrão para esse nó alterna da rede da grade para a rede do cliente quando você clica em **Instalar**. Se você perder a conetividade, deve garantir que está acessando o nó de administração principal por meio de uma sub-rede acessível. "Diretrizes de rede"Consulte para obter detalhes.

4. Clique em **Download Recovery Package**.

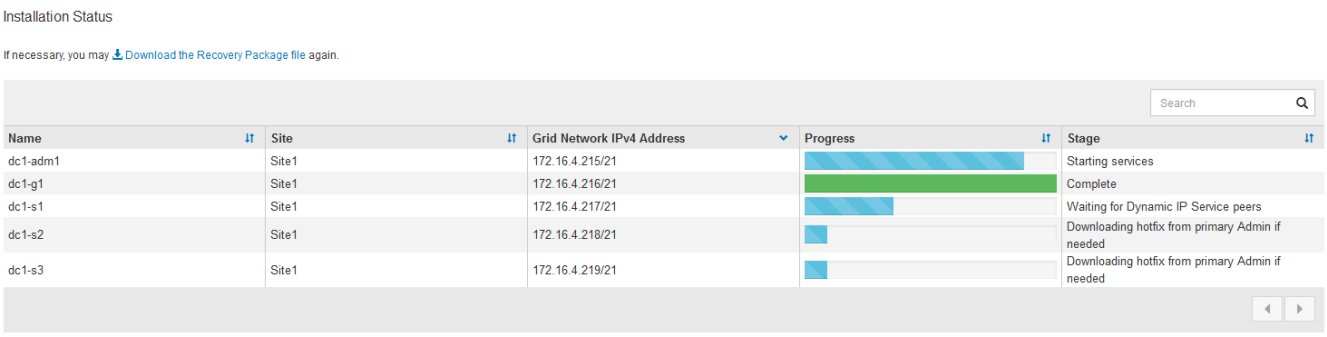
   Quando a instalação progride até o ponto em que a topologia da grade é definida, você será solicitado a baixar o arquivo do Pacote de recuperação (`.zip`) e confirmar que você pode acessar com êxito o conteúdo desse arquivo. Você deve baixar o arquivo do pacote de recuperação para que você possa recuperar o sistema StorageGRID se um ou mais nós de grade falharem. A instalação continua em segundo plano, mas você não pode concluir a instalação e acessar o sistema StorageGRID até baixar e verificar esse arquivo.

5. Verifique se você pode extrair o conteúdo do `.zip` arquivo e salvá-lo em 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.

6. Marque a caixa de seleção **Eu baixei e verifiquei com êxito o arquivo do pacote de recuperação** e clique em **Avançar**.

   Se a instalação ainda estiver em andamento, a página de status será exibida. Esta página indica o progresso da instalação para cada nó de grade.



   Quando o estágio completo é alcançado para todos os nós de grade, a página de login do Gerenciador de Grade é exibida.

7. Inicie sessão no Grid Manager utilizando o utilizador "root" e a palavra-passe especificada durante a instalação.

Diretrizes de pós-instalação

Depois de concluir a implantação e a configuração do nó de grade, siga estas diretrizes para endereçamento DHCP e alterações na configuração da rede.

- Se o DHCP foi usado para atribuir endereços IP, configure uma reserva DHCP para cada endereço IP nas redes que estão sendo usadas.

  Só pode configurar o DHCP durante a fase de implementação. Não é possível configurar o DHCP durante a configuração.

  > Os nós reiniciam quando a configuração da rede de Grade é alterada pelo DHCP, o que pode causar interrupções se uma alteração de DHCP afetar vários nós ao mesmo tempo.

- Você deve usar os procedimentos alterar IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. "Configurar endereços IP"Consulte .
- Se você fizer alterações na configuração de rede, incluindo alterações de roteamento e gateway, a conetividade do cliente para o nó de administração principal e outros nós de grade pode ser perdida. Dependendo das alterações de rede aplicadas, talvez seja necessário restabelecer essas conexões.

API REST de instalação

O StorageGRID fornece a API de instalação do StorageGRID para executar tarefas de instalação.

A API usa a plataforma de API de código aberto Swagger para fornecer a documentação da API. O Swagger permite que desenvolvedores e não desenvolvedores interajam com a API em uma interface de usuário que ilustra como a API responde a parâmetros e opções. Esta documentação pressupõe que você esteja familiarizado com as tecnologias da Web padrão e o formato de dados JSON.

Todas as operações de API executadas usando a página da Documentação da API são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Cada comando REST API inclui o URL da API, uma ação HTTP, quaisquer parâmetros de URL necessários ou opcionais e uma resposta de API esperada.

API de instalação do StorageGRID

A API de instalação do StorageGRID só está disponível quando você estiver configurando inicialmente o sistema StorageGRID e se precisar executar uma recuperação do nó de administração principal. A API de instalação pode ser acessada por HTTPS a partir do Gerenciador de Grade.

Para acessar a documentação da API, vá para a página da Web de instalação no nó de administração principal e selecione **Ajuda** > **Documentação da API** na barra de menus.

A API de instalação do StorageGRID inclui as seguintes seções:

- **Config** — operações relacionadas à versão do produto e versões da API. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **Grid** — operações de configuração em nível de grade. Você pode obter e atualizar configurações de grade, incluindo detalhes de grade, sub-redes de rede de grade, senhas de grade e endereços IP de servidor NTP e DNS.
- **Nodes** — operações de configuração em nível de nó. Você pode recuperar uma lista de nós de grade, excluir um nó de grade, configurar um nó de grade, exibir um nó de grade e redefinir a configuração de um nó de grade.
- **Provisão** — operações de provisionamento. Você pode iniciar a operação de provisionamento e exibir o status da operação de provisionamento.
- **Recovery** — operações de recuperação do nó de administração principal. Você pode redefinir informações, carregar o pacote de recuperação, iniciar a recuperação e exibir o status da operação de recuperação.
- **Recovery-package** — operações para baixar o Recovery Package.
- **Sites** — operações de configuração no nível do local. Você pode criar, exibir, excluir e modificar um site.
- **Temporary-password** — operações na senha temporária para proteger a mgmt-api durante a instalação.

Onde ir a seguir

Depois de concluir uma instalação, execute as tarefas de integração e configuração necessárias. Você pode executar as tarefas opcionais conforme necessário.

Tarefas necessárias

- Configurar o VMware vSphere Hypervisor para reinicialização automática.

  Você deve configurar o hipervisor para reiniciar as máquinas virtuais quando o servidor for reiniciado. Sem uma reinicialização automática, as máquinas virtuais e os nós de grade permanecem desligados após o servidor reiniciar. Para obter detalhes, consulte a documentação do VMware vSphere Hypervisor.

- "Crie uma conta de locatário" Para o protocolo cliente S3 que será utilizado para armazenar objetos no seu sistema StorageGRID.

- "Controle o acesso ao sistema" configurando grupos e contas de usuário. Opcionalmente, você pode "configure uma fonte de identidade federada" (como ative Directory ou OpenLDAP), para que você possa importar grupos de administração e usuários. Ou, você pode "crie grupos locais e usuários".
- Integre e teste os "S3 API" aplicativos cliente que você usará para carregar objetos para seu sistema StorageGRID.
- "Configure as regras de gerenciamento do ciclo de vida das informações (ILM) e a política ILM" você deseja usar para proteger os dados do objeto.
- Se a instalação incluir nós de storage do dispositivo, use o SANtricity os para concluir as seguintes tarefas:
  - Ligue a cada dispositivo StorageGRID.
  - Verifique a receção dos dados do AutoSupport.

    ```
    https://docs.netapp.com/us-en/storagegrid-
    appliances/installconfig/configuring-hardware.html["Configure o
    hardware"^]Consulte .
    ```

- Analise e siga o "Diretrizes de fortalecimento do sistema StorageGRID" para eliminar os riscos de segurança.
- "Configurar notificações por e-mail para alertas do sistema".

Tarefas opcionais

- "Atualize os endereços IP do nó da grade" Se eles foram alterados desde que você planejou sua implantação e gerou o Pacote de recuperação.
- "Configurar a criptografia de armazenamento", se necessário.
- "Configurar a compressão de armazenamento" para reduzir o tamanho dos objetos armazenados, se necessário.
- "Configurar interfaces VLAN" para isolar e particionar o tráfego de rede, se necessário.
- "Configurar grupos de alta disponibilidade" Para melhorar a disponibilidade de conexão para os clientes Grid Manager, Tenant Manager e S3, se necessário.
- "Configurar pontos de extremidade do balanceador de carga" Para conetividade de cliente S3, se necessário.

Solucionar problemas de instalação

Se ocorrerem problemas durante a instalação do sistema StorageGRID, pode aceder aos ficheiros de registo de instalação.

A seguir estão os principais arquivos de log de instalação, que suporte técnico pode precisar para resolver problemas.

- `/var/local/log/install.log` (encontrado em todos os nós da grade)
- `/var/local/log/gdu-server.log` (Encontrado no nó de administração principal)

Informações relacionadas

Para saber como acessar os arquivos de log, "Referência de ficheiros de registo"consulte .

Se precisar de ajuda adicional, entre em Contato "Suporte à NetApp"com .

A reserva de recursos da máquina virtual requer ajuste

Os arquivos OVF incluem uma reserva de recursos projetada para garantir que cada nó de grade tenha RAM e CPU suficientes para operar com eficiência. Se você criar máquinas virtuais implantando esses arquivos OVF no VMware e o número predefinido de recursos não estiver disponível, as máquinas virtuais não serão iniciadas.

Sobre esta tarefa

Se você tiver certeza de que o host da VM tem recursos suficientes para cada nó de grade, ajuste manualmente os recursos alocados para cada máquina virtual e tente iniciar as máquinas virtuais.

Passos

1. Na árvore cliente do VMware vSphere Hypervisor, selecione a máquina virtual que não foi iniciada.
2. Clique com o botão direito do rato na máquina virtual e selecione **Edit Settings** (Editar definições).
3. Na janela Propriedades de máquinas virtuais, selecione a guia **recursos**.
4. Ajuste os recursos alocados à máquina virtual:
   a. Selecione **CPU** e, em seguida, use o controle deslizante de reserva para ajustar o MHz reservado para esta máquina virtual.
   b. Selecione **memória** e, em seguida, use o controle deslizante reserva para ajustar o MB reservado para esta máquina virtual.
5. Clique em **OK**.
6. Repita conforme necessário para outras máquinas virtuais hospedadas no mesmo host da VM.

A palavra-passe de instalação temporária foi desativada

Ao implantar um nó VMware, você pode especificar opcionalmente uma senha de instalação temporária. Você deve ter essa senha para acessar o console da VM ou usar SSH antes que o novo nó se una à grade.

Se você optou por desativar a senha de instalação temporária, você deve executar etapas adicionais para depurar problemas de instalação.

Você pode fazer um dos seguintes procedimentos:

- Reimplante a VM, mas especifique uma senha de instalação temporária para que você possa acessar o console ou usar SSH para depurar problemas de instalação.
- Use o vCenter para definir a senha:
  a. Desligue a VM.
  b. Vá para **VM**, selecione a guia **Configure** e selecione **vApp Options**.
  c. Especifique o tipo de senha de instalação temporária a definir:
     - Selecione **CUSTOM_TEMPORARY_password** para definir uma senha temporária personalizada.
     - Selecione **TEMPORARY_PASSWORD_TYPE** para usar o nome do nó como senha temporária.
  d. Selecione **Definir valor**.
  e. Defina a senha temporária:
     - Altere **CUSTOM_TEMPORARY_PASSWORD** para um valor de senha personalizado.

- Atualize o **TEMPORARY_PASSWORD_TYPE** com o valor **Use node name**.

f. Reinicie a VM para aplicar a nova senha.

Atualize o software StorageGRID

Atualize o software StorageGRID

Use estas instruções para atualizar um sistema StorageGRID para uma nova versão.

Ao realizar a atualização, todos os nós do seu sistema StorageGRID são atualizados.

Antes de começar

Revise esses tópicos para saber mais sobre os novos recursos e aprimoramentos no StorageGRID 11,9, determinar se algum recurso foi descontinuado ou removido e descobrir as alterações nas APIs do StorageGRID.

- "Novidades do StorageGRID 11,9"
- "Recursos removidos ou obsoletos"
- "Alterações na API Grid Management"
- "Alterações na API de gerenciamento do locatário"

Novidades do StorageGRID 11,9

Esta versão do StorageGRID introduz os seguintes recursos e alterações funcionais.

Escalabilidade

Nós de storage somente de dados

Para permitir um dimensionamento mais granular, agora você pode instalar "Nós de storage somente de dados"o . Quando o processamento de metadados não é essencial, você pode otimizar sua infraestrutura de forma econômica. Essa flexibilidade ajuda a acomodar workloads e padrões de crescimento variáveis.

Melhorias no Cloud Storage Pool

Funções do IAM em qualquer lugar

O StorageGRID agora oferece suporte a credenciais de curto prazo usando "Funções do IAM em qualquer lugar no Amazon S3 para Cloud Storage Pools"o .

O uso de credenciais de longo prazo para acessar buckets do S3 representa riscos de segurança se essas credenciais forem comprometidas. As credenciais de curto prazo têm uma vida útil limitada, o que reduz o risco de acesso não autorizado.

S3 baldes de bloqueio de objetos

Agora você pode "Configure um pool de armazenamento em nuvem usando um endpoint do Amazon S3". O bloqueio de objetos S3 ajuda a evitar a exclusão acidental ou maliciosa de objetos. Se você categorizar dados do StorageGRID para o Amazon S3, ter o bloqueio de objetos ativado em ambos os sistemas aumenta a proteção de dados em todo o ciclo de vida dos dados.

Alocação a vários clientes

Limites do balde

Por "Definição de limites em baldes S3", você pode impedir que os inquilinos monopolizem a capacidade. Além disso, o crescimento descontrolado pode resultar em custos inesperados. Com limites definidos, você pode estimar melhor as despesas de storage do locatário.

5.000 buckets por locatário

Para aumentar a escalabilidade, o StorageGRID agora oferece suporte "5.000 S3 buckets por locatário"a até . Cada grade pode ter um máximo de 100.000 baldes.

Para suportar buckets do 5.000, cada nó de armazenamento na grade deve ter um mínimo de 64 GB de RAM.

S3 melhorias no bloqueio de objetos

Os recursos de configuração por locatário fornecem o equilíbrio apropriado entre flexibilidade e segurança dos dados. Agora você pode configurar as configurações de retenção por locatário para:

- Permitir ou desativar o modo de conformidade
- Defina um período de retenção máximo

Consulte:

- "Gerencie objetos com o S3 Object Lock"
- "Como os administradores de grade controlam a retenção de objetos"
- "Crie uma conta de locatário"

Compatibilidade com S3

x-amz-checksum-sha256 soma de verificação

- A API REST do S3 agora fornece suporte para `x-amz-checksum-sha256` checksum.
- O StorageGRID agora fornece suporte para soma de verificação SHA-256 para OPERAÇÕES PUT, GET e HEAD. Essas somas de verificação melhoram a integridade dos dados.

Alterações ao suporte ao protocolo S3

- Adicionado suporte para ponto de montagem para o Amazon S3, que permite que os aplicativos se conetem diretamente aos buckets do S3 como se fossem sistemas de arquivos locais. Agora você pode usar o StorageGRID com mais aplicativos e mais casos de uso.
- Como parte da adição de suporte para ponto de montagem, o StorageGRID 11,9 "Alterações adicionais ao suporte ao protocolo S3"contém .

Manutenção e suporte

AutoSupport

"AutoSupport" agora cria automaticamente casos de falha de hardware para dispositivos legados.

Operações expandidas de clone de nó

A usabilidade do clone de nó foi expandida para oferecer suporte a nós de storage maiores.

Processamento ILM melhorado dos marcadores de exclusão expirados

As regras de tempo de ingestão de ILM com um período de dias agora também removem marcadores de exclusão de objetos expirados. Os marcadores de exclusão só são removidos quando um período de dias tiver passado e o criador de exclusão atual tiver expirado (não há versões não atuais).

"Como objetos com versão S3 são excluídos"Consulte e "Exemplo de ciclo de vida do bucket tendo prioridade sobre a política de ILM".

Desativação aprimorada de nós

Para proporcionar uma transição suave e eficiente para o hardware de última geração da StorageGRID, "desativação do nó"foi melhorado.

Syslog para pontos de extremidade do balanceador de carga

Os logs de acesso de terminais do balanceador de carga contêm informações de solução de problemas, como códigos de status HTTP. O StorageGRID agora "exportando esses logs para um servidor syslog externo"suporta . Esse aprimoramento permite o gerenciamento e a integração de logs mais eficientes com sistemas de monitoramento e alerta existentes.

Melhorias adicionais para manutenção e suporte

- Atualização da IU de métricas
- Novas qualificações do sistema operacional
- Suporte para novos componentes de terceiros

Segurança

Rotação das teclas de acesso SSH

Os administradores de grade podem agora "Atualize e gire chaves SSH". A capacidade de girar chaves SSH é uma prática recomendada de segurança e um mecanismo de defesa pró-ativo.

Alertas para logins raiz

Quando uma entidade desconhecida entra no Gerenciador de Grade como root, "um alerta é acionado". Monitorar logins de SSH raiz é um passo proativo para proteger sua infraestrutura.

Melhorias no Grid Manager

Página de perfis de codificação de apagamento movida

A página de perfis de codificação de apagamento está agora localizada em **CONFIGURATION** > **System** > **Erasure Coding**. Ele costumava estar no menu ILM.

Melhorias de pesquisa

O "Campo de pesquisa no Gerenciador de Grade" agora inclui uma lógica de correspondência melhor, permitindo que você encontre páginas pesquisando abreviaturas comuns e pelos nomes de certas configurações dentro de uma página. Você também pode pesquisar mais tipos de itens, como nós, usuários e

contas de locatários.

Recursos e recursos removidos ou obsoletos

Alguns recursos e recursos foram removidos ou obsoletos nesta versão. Revise esses itens para entender se você precisa atualizar aplicativos do cliente ou modificar sua configuração antes de atualizar.

Definições

Obsoleto

O recurso **não deve** ser usado em novos ambientes de produção. Os ambientes de produção existentes podem continuar usando o recurso.

Fim da vida

Última versão fornecida que suporta o recurso. Em alguns casos, a documentação do recurso pode ser removida nesta fase.

Removido

Primeira versão que **não** suporta o recurso.

Suporte de fim de recurso do StorageGRID

Os recursos obsoletos serão removidos em mais de 2 versões principais. Por exemplo, se um recurso estiver obsoleto na versão N (por exemplo, 6,3), a última versão em que o recurso existirá é N-1 (por exemplo, 6,4). A versão N-2 (por exemplo, 6,5) é a primeira versão quando o recurso não existe no produto.

Consulte "Página de suporte da versão de software" para obter informações adicionais.

> Em certas situações, o NetApp pode terminar o suporte para recursos específicos mais cedo do que o indicado.

Recurso	Obsoleto	Fim da vida	Removido	Links para documentação anterior
Alarmes legados (*não alertas*)	11,7	11,8	11,9	"Referência de alarmes (StorageGRID 11,8)"

Recurso	Obsoleto	Fim da vida	Removido	Links para documentação anterior
Suporte ao Archive Node	11,7	11,8	11,9	"Considerações para a desativação de nós de arquivo (StorageGRID 11,8)" **Nota**: Antes de iniciar o upgrade, você deve: 1. Desativar todos os nós de arquivamento. "Desativação do nó de grade (StorageGRID 11,8 doc site)"Consulte . 2. Remova todas as referências de nó de arquivo de pools de armazenamento e políticas de ILM. "Base de dados de Conhecimento da NetApp: Guia de resolução de atualização do software StorageGRID 11,9"Consulte .
Auditoria de exportação através de CIFS/Samba	11,1	11,6	11,7	
Serviço CLB	11,4	11,6	11,7	
Mecanismo de contêiner do Docker	11,8	11,9	A DETERMINAR	O suporte para Docker como o mecanismo de contentor para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contentor em uma versão futura. Consulte a "Lista de versões do Docker atualmente suportadas".
Exportação de auditoria NFS	11,8	11,9	12,0	"Configurar acesso de cliente de auditoria para NFS (StorageGRID 11,8)"
Suporte à API Swift	11,7	11,9	12,0	"Usar API REST Swift (StorageGRID 11,8)"
RHEL 8,8	11,9	11,9	12,0	
RHEL 9,0	11,9	11,9	12,0	
RHEL 9,2	11,9	11,9	12,0	
Ubuntu 18,04.04	11,9	11,9	12,0	
Ubuntu 20,04.04	11,9	11,9	12,0	

Recurso	Obsoleto	Fim da vida	Removido	Links para documentação anterior
Debian 11	11,9	11,9	12,0	

Consulte também:

- "Alterações na API Grid Management"
- "Alterações na API de gerenciamento do locatário"

Alterações na API Grid Management

O StorageGRID 11,9 usa a versão 4 da API de gerenciamento de grade. A versão 4 desconsidera a versão 3; no entanto, as versões 1, 2 e 3 ainda são suportadas.

> Você pode continuar usando versões obsoletas da API de gerenciamento com o StorageGRID 11,9; no entanto, o suporte para essas versões da API será removido em uma versão futura do StorageGRID. Depois de atualizar para o StorageGRID 11,9, você pode desativar as APIs obsoletas usando a `PUT /grid/config/management` API.

Para saber mais, "Use a API de gerenciamento de grade"acesse .

Revise as configurações de conformidade depois de ativar o bloqueio de objetos S3 global

Revise as configurações de conformidade dos locatários existentes depois de ativar a configuração global S3 Object Lock. Quando você ativa essa configuração, as configurações de bloqueio de objeto S3 por locatário dependem da versão do StorageGRID no momento em que o locatário foi criado.

Solicitações legadas de mgmt-api removidas

Essas solicitações legadas foram removidas:

`/grid/server-types`

`/grid/ntp-roles`

Alterações à `GET /private/storage-usage` API

- Uma nova propriedade, `usageCacheDuration`, foi adicionada ao corpo de resposta. Esta propriedade especifica a duração (em segundos) para a qual o cache de pesquisa de uso permanece válido. Esse valor se aplica ao verificar o uso em relação aos limites de cota de armazenamento do locatário e capacidade do bucket.
- O `GET /api/v4/private/storage-usage` comportamento foi corrigido para combinar o aninhamento do esquema.
- Essas alterações se aplicam somente à API privada.

Alterações à `GET cross-grid-replication` API

A API **/org/containers/:name/cross-grid-replication** GET não requer mais a (`rootAccess`permissão root Access); no entanto, você deve pertencer a um grupo de usuários que tenha a (`viewAllContainers`permissão Gerenciar todos os buckets (`manageAllContainers`) ou

Exibir todos os buckets).

A API PUT **/org/containers/:name/cross-grid-replication** não foi alterada e ainda requer a (`rootAccess`permissão root Access).

Alterações na API de gerenciamento do locatário

O StorageGRID 11,9 usa a versão 4 da API de gerenciamento do locatário. A versão 4 desconsidera a versão 3; no entanto, as versões 1, 2 e 3 ainda são suportadas.

> Você pode continuar usando versões obsoletas da API de gerenciamento de locatário com o StorageGRID 11,9; no entanto, o suporte para essas versões da API será removido em uma versão futura do StorageGRID. Depois de atualizar para o StorageGRID 11,9, você pode desativar as APIs obsoletas usando a `PUT /grid/config/management` API.

Para saber mais, "Entenda a API de gerenciamento do locatário"acesse .

Nova API para limite de capacidade do bucket

Você pode usar a `/org/containers/{bucketName}/quota-object-bytes` API com operações DE GET/PUT para obter e definir o limite de capacidade de storage para um bucket.

Planeje e prepare-se para o upgrade

Estime o tempo para concluir uma atualização

Considere quando atualizar, com base em quanto tempo a atualização pode demorar. Esteja ciente de quais operações você pode e não pode executar durante cada etapa da atualização.

Sobre esta tarefa

O tempo necessário para concluir uma atualização do StorageGRID depende de uma variedade de fatores, como carga do cliente e desempenho do hardware.

A tabela resume as principais tarefas de atualização e lista o tempo aproximado necessário para cada tarefa. As etapas após a tabela fornecem instruções que você pode usar para estimar o tempo de atualização para o seu sistema.

Tarefa de atualização	Descrição	Tempo aproximado necessário	Durante esta tarefa
Execute pré-verificações e atualize o nó de administração principal	As pré-verificações de atualização são executadas e o nó Admin principal é interrompido, atualizado e reiniciado.	de 30 minutos a 1 hora, com os nós do dispositivo de serviços que exigem mais tempo. Os erros de pré-verificação não resolvidos aumentarão este tempo.	Não é possível acessar o nó de administração principal. Erros de conexão podem ser relatados, o que você pode ignorar. Executar as pré-verificações de atualização antes de iniciar a atualização permite resolver quaisquer erros antes da janela de manutenção de atualização agendada.
Inicie o serviço de atualização	O arquivo de software é distribuído e o serviço de atualização é iniciado.	3 minutos por nó de grade	
Atualizar outros nós de grade	O software em todos os outros nós de grade é atualizado, na ordem em que você aprova os nós. Cada nó em seu sistema será derrubado um de cada vez.	de 15 minutos a 1 hora por nó, com os nós do dispositivo que exigem mais tempo **Nota**: Para nós de appliance, o Instalador de appliance StorageGRID é atualizado automaticamente para a versão mais recente.	• Não altere a configuração da grade. • Não altere a configuração do nível de auditoria. • Não atualize a configuração do ILM. • Você está impedido de executar outros procedimentos de manutenção, como hotfix, desativação ou expansão. **Nota**: Se você precisar executar uma recuperação, entre em Contato com o suporte técnico.
Ativar funcionalidades	As novas funcionalidades para a nova versão estão ativadas.	Menos de 5 minutos	• Não altere a configuração da grade. • Não altere a configuração do nível de auditoria. • Não atualize a configuração do ILM. • Não é possível executar outro procedimento de manutenção.
Atualizar banco de dados	O processo de atualização verifica cada nó para verificar se o banco de dados Cassandra não precisa ser atualizado.	10 segundos por nó ou alguns minutos para toda a grade	A atualização do StorageGRID 11,8 para o 11,9 não requer uma atualização do banco de dados Cassandra; no entanto, o serviço Cassandra será interrompido e reiniciado em cada nó de armazenamento. Para futuras versões de recursos do StorageGRID, a etapa de atualização do banco de dados do Cassandra pode levar vários dias para ser concluída.

Tarefa de atualização	Descrição	Tempo aproximado necessário	Durante esta tarefa
Etapas finais da atualização	Os arquivos temporários são removidos e a atualização para a nova versão é concluída.	5 minutos	Quando a tarefa **etapas finais de atualização** for concluída, você poderá executar todos os procedimentos de manutenção.

Passos

1. Estime o tempo necessário para atualizar todos os nós de grade.
   a. Multiplique o número de nós em seu sistema StorageGRID por 1 hora/nó.

      Como regra geral, os nós de dispositivo demoram mais tempo a atualizar do que os nós baseados em software.

   b. Adicione 1 hora a esta hora para ter em conta o tempo necessário para baixar o `.upgrade` arquivo, executar validações de pré-verificação e concluir as etapas finais de atualização.
2. Se você tiver nós do Linux, adicione 15 minutos para cada nó para ter em conta o tempo necessário para baixar e instalar o pacote RPM ou DEB.
3. Calcule o tempo total estimado para a atualização adicionando os resultados das etapas 1 e 2.

Exemplo: Tempo estimado para atualizar para o StorageGRID 11,9

Suponha que seu sistema tenha 14 nós de grade, dos quais 8 são nós de Linux.

1. Multiplique 14 por 1 hora/nó.
2. Adicione 1 hora para ter em conta as etapas de download, pré-verificação e final.

   O tempo estimado para atualizar todos os nós é de 15 horas.

3. Multiplique 8 por 15 minutos/nó para contabilizar o tempo de instalação do pacote RPM ou DEB nos nós Linux.

   O tempo estimado para este passo é de 2 horas.

4. Adicione os valores juntos.

   Você deve permitir até 17 horas para concluir a atualização do seu sistema para o StorageGRID 11,9.0.

> Conforme necessário, você pode dividir a janela de manutenção em janelas menores aprovando subconjuntos de nós de grade para atualizar em várias sessões. Por exemplo, você pode preferir atualizar os nós no local A em uma sessão e, em seguida, atualizar os nós no local B em uma sessão posterior. Se você optar por realizar a atualização em mais de uma sessão, esteja ciente de que você não pode começar a usar os novos recursos até que todos os nós tenham sido atualizados.

Como seu sistema é afetado durante a atualização

Saiba como seu sistema StorageGRID será afetado durante a atualização.

As atualizações do StorageGRID não causam interrupções

O sistema StorageGRID pode obter e recuperar dados de aplicativos clientes durante todo o processo de atualização. Se aprovar a atualização de todos os nós do mesmo tipo (por exemplo, nós de storage), os nós serão derrubados um de cada vez, portanto, não haverá tempo em que todos os nós de grade ou todos os nós de grade de um determinado tipo estejam indisponíveis.

Para permitir disponibilidade contínua, verifique se sua política de ILM contém regras que especificam o armazenamento de várias cópias de cada objeto. Você também deve garantir que todos os clientes S3 externos estejam configurados para enviar solicitações para um dos seguintes:

- Um endereço IP virtual do grupo de alta disponibilidade (HA)
- Um balanceador de carga de terceiros de alta disponibilidade
- Vários nós de gateway para cada cliente
- Vários nós de storage para cada cliente

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 atualização; no entanto, as conexões de clientes com nós de gateway individuais ou nós de storage podem ser interrompidas temporariamente se a atualização precisar reiniciar os serviços nesses nós. A conetividade será restaurada após a conclusão do processo de atualização e os serviços são retomados nos nós individuais.

Talvez seja necessário agendar o tempo de inatividade para aplicar uma atualização se a perda de conetividade 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 atualização. Consulte as instruções para "configurando grupos de alta disponibilidade".

O firmware do dispositivo foi atualizado

Durante a atualização do StorageGRID 11,9:

- Todos os nós do dispositivo StorageGRID são atualizados automaticamente para a versão 3,9 do firmware do instalador do StorageGRID Appliance.
- Os dispositivos SG6060 e SGF6024 são atualizados automaticamente para a versão 3B08.EX do firmware do BIOS e para a versão 4.00.07 do firmware do BMC.
- Os dispositivos SG100 e SG1000 são atualizados automaticamente para a versão 3B13.EC do firmware do BIOS e para a versão 4.74.07 do firmware do BMC.
- Os dispositivos SGF6112, SG6160, SG110 e SG1100 são atualizados automaticamente para a versão 3.16.07 do firmware BMC.

As políticas de ILM são tratadas de forma diferente de acordo com seu status

- A política ativa permanecerá a mesma após a atualização.
- Apenas as últimas 10 políticas históricas são preservadas na atualização.
- Se houver uma política proposta, ela será excluída durante a atualização.

Os alertas podem ser acionados

Os alertas podem ser acionados quando os serviços começam e param 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). Outros alertas podem ser acionados após a conclusão da atualização.

Por exemplo, você pode ver o alerta **não é possível se comunicar com o nó** quando os serviços são interrompidos, ou você pode ver o alerta **erro de comunicação do Cassandra** quando alguns nós foram atualizados para o StorageGRID 11,9, mas outros nós ainda estão executando o StorageGRID 11,8. Em geral, esses alertas serão apagados quando a atualização for concluída.

O alerta **ILM Placement unachievable** pode ser acionado quando os nós de armazenamento são interrompidos durante a atualização para o StorageGRID 11,9. Esse alerta pode persistir por 1 dia após a conclusão da atualização.

Após a conclusão da atualização, você pode revisar qualquer alerta relacionado a atualização selecionando **alertas resolvidos recentemente** ou **alertas atuais** no painel do Gerenciador de Grade.

Muitas notificações SNMP são geradas

Esteja ciente de que um grande número de notificações SNMP pode ser gerado quando os nós de grade são interrompidos e reiniciados durante a atualização. Para evitar notificações excessivas, desmarque a caixa de seleção **Ativar notificações de agente SNMP** (**CONFIGURAÇÃO** > **Monitoramento** > **agente SNMP**) para desativar as notificações SNMP antes de iniciar a atualização. Em seguida, reative as notificações após a atualização estar concluída.

As alterações de configuração são restritas

> Esta lista aplica-se especificamente às atualizações do StorageGRID 11,8 para o StorageGRID 11,9. Se você estiver atualizando para outra versão do StorageGRID, consulte a lista de alterações restritas nas instruções de atualização para essa versão.

Até que a tarefa **Ativar novo recurso** seja concluída:

- Não faça alterações na configuração da grade.
- Não ative ou desative nenhum novo recurso.
- Não atualize a configuração do ILM. Caso contrário, você pode experimentar comportamento inconsistente e inesperado de ILM.
- Não aplique um hotfix ou recupere um nó de grade.

  > Entre em Contato com o suporte técnico se precisar recuperar um nó durante a atualização.

- Você não deve gerenciar grupos de HA, interfaces VLAN ou pontos de extremidade do balanceador de carga durante a atualização para o StorageGRID 11,9.

- Não exclua nenhum grupo de HA até que a atualização para o StorageGRID 11,9 esteja concluída. Os endereços IP virtuais em outros grupos de HA podem ficar inacessíveis.

Até que a tarefa **etapas de atualização final** seja concluída:

- Não execute um procedimento de expansão.
- Não efetue um procedimento de desativação.

Não é possível visualizar os detalhes do bucket nem gerenciar buckets do Tenant Manager

Durante a atualização para o StorageGRID 11,9 (ou seja, enquanto o sistema estiver operando como um ambiente de versão mista), você não pode exibir detalhes do bucket ou gerenciar buckets usando o Gerenciador do locatário. Um dos seguintes erros aparece na página baldes no Tenant Manager:

- Você não pode usar essa API enquanto estiver atualizando para 11,9.
- Você não pode exibir detalhes de versão do bucket no Gerenciador de inquilinos enquanto estiver atualizando para o 11,9.

Este erro será resolvido após a atualização para o 11,9 estar concluída.

Solução alternativa

Enquanto a atualização do 11,9 estiver em andamento, use as seguintes ferramentas para exibir detalhes do bucket ou gerenciar buckets, em vez de usar o Gerenciador do locatário:

- Para efetuar operações S3 padrão num balde, utilize a "S3 API REST" ou a "API de gerenciamento do locatário".
- Para executar operações personalizadas do StorageGRID em um bucket (por exemplo, exibindo e modificando a consistência do bucket, habilitando ou desativando as atualizações do último tempo de acesso ou configurando a integração de pesquisa), use a API de Gerenciamento do locatário.

Verifique a versão instalada do StorageGRID

Antes de iniciar a atualização, verifique se a versão anterior do StorageGRID está atualmente instalada com o hotfix disponível mais recente aplicado.

Sobre esta tarefa

Antes de atualizar para o StorageGRID 11,9, sua grade deve ter o StorageGRID 11,8 instalado. Se você estiver usando uma versão anterior do StorageGRID, você deve instalar todos os arquivos de atualização anteriores juntamente com seus hotfixes mais recentes (fortemente recomendado) até que a versão atual da grade seja StorageGRID 11,8.*x.y*.

Um possível caminho de atualização é mostrado no exemplo.

> O NetApp recomenda vivamente que aplique a correção mais recente para cada versão do StorageGRID antes de atualizar para a próxima versão e que também aplique a correção mais recente para cada nova versão que instalar. Em alguns casos, você deve aplicar um hotfix para evitar o risco de perda de dados. Consulte "NetApp Downloads: StorageGRID" e as notas de versão de cada hotfix para saber mais.

Passos

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".

2. Na parte superior do Gerenciador de Grade, selecione **Ajuda** > **sobre**.
3. Verifique se **Version** é 11,8.*x.y*.

   No número da versão do StorageGRID 11,8.*x.y*:

   - A **versão principal** tem um valor *x* de 0 (11,8.0).
   - Um **hotfix**, se um tiver sido aplicado, tem um valor *y* (por exemplo, 11,8.0,1).
4. Se **Version** não for 11,8.*x.y*, aceda a "NetApp Downloads: StorageGRID" para transferir os ficheiros para cada versão anterior, incluindo a correção mais recente para cada versão.
5. Obtenha as instruções de atualização para cada versão que você baixou. Em seguida, execute o procedimento de atualização de software para essa versão e aplique o hotfix mais recente para essa versão (altamente recomendado).

   Consulte "Procedimento de correção do StorageGRID".

exemplo: Atualize para o StorageGRID 11,9 a partir da versão 11,6

O exemplo a seguir mostra as etapas para atualizar do StorageGRID versão 11,6 para a versão 11,8 em preparação para uma atualização do StorageGRID 11,9.

Transfira e instale o software na seguinte sequência para preparar o seu sistema para a atualização:

1. Atualize para a versão principal do StorageGRID 11.6.0.
2. Aplique o hotfix do StorageGRID 11,6.0.*y* mais recente.
3. Atualize para a versão principal do StorageGRID 11.7.0.
4. Aplique o hotfix do StorageGRID 11,7.0.*y* mais recente.
5. Atualize para a versão principal do StorageGRID 11.8.0.
6. Aplique o hotfix do StorageGRID 11,8.0.*y* mais recente.

Obtenha os materiais necessários para uma atualização de software

Antes de iniciar a atualização de software, obtenha todos os materiais necessários.

Item	Notas
Serviço de laptop	O computador portátil de serviço deve ter: • Porta de rede • Cliente SSH (por exemplo, PuTTY)
"Navegador da Web suportado"	O suporte do navegador normalmente muda para cada versão do StorageGRID. Certifique-se de que o seu navegador é compatível com a nova versão do StorageGRID.
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 listada no `Passwords.txt` arquivo.

Item	Notas
Arquivo RPM ou DEB do Linux	Se algum nó for implantado em hosts Linux, você deve "Baixe e instale o pacote RPM ou DEB em todos os hosts" antes de iniciar a atualização. Certifique-se de que seu sistema operacional atenda aos requisitos mínimos de versão do kernel do StorageGRID: • "Instale o StorageGRID em hosts Linux Red Hat Enterprise" • "Instale o StorageGRID em hosts Ubuntu ou Debian"
Documentação do StorageGRID	• "Notas de lançamento" Para o StorageGRID 11,9 (é necessário iniciar sessão). Certifique-se de lê-las cuidadosamente antes de iniciar a atualização. • "Guia de resolução de atualização do software StorageGRID" para a versão principal para a qual você está atualizando (login necessário) • Outro "Documentação do StorageGRID", conforme necessário.

Verifique o estado do sistema

Antes de atualizar um sistema StorageGRID, verifique se o sistema está pronto para acomodar a atualização. Certifique-se de que o sistema está funcionando normalmente e que todos os nós de grade estejam operacionais.

Passos

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Verifique e resolva quaisquer alertas ativos.
3. Confirme se não há tarefas de grade conflitantes ativas ou pendentes.
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***site*** > ***Main Admin Node*** > **CMN** > **Grid Tasks** > **Configuration**.

      As tarefas de avaliação de gerenciamento do ciclo de vida das informações (ILME) são as únicas tarefas de grade que podem ser executadas simultaneamente com a atualização do software.

   c. Se quaisquer outras tarefas de grade estiverem ativas ou pendentes, aguarde até que elas terminem ou liberem seu bloqueio.

      Contacte o suporte técnico se uma tarefa não terminar ou libertar o respetivo bloqueio.

4. "Comunicações internas do nó da grade"Consulte e "Comunicações externas" para garantir que todas as portas necessárias para o StorageGRID 11,9 estejam abertas antes de atualizar.

   Não são necessárias portas adicionais ao atualizar para o StorageGRID 11,9.

   A seguinte porta necessária foi adicionada no StorageGRID 11,7. Certifique-se de que está disponível antes de atualizar para o StorageGRID 11,9.

Porta	Descrição
18086	Porta TCP usada para solicitações S3 do balanceador de carga StorageGRID para LDR e o novo serviço LDR. Antes de atualizar, confirme se essa porta está aberta de todos os nós de grade para todos os nós de storage. Bloquear esta porta causará S3 interrupções de serviço após a atualização para o StorageGRID 11,9.

Se tiver aberto quaisquer portas de firewall personalizadas, será notificado durante a pré-verificação da atualização. Você deve entrar em Contato com o suporte técnico antes de prosseguir com a atualização.

Atualizar o software

Atualize o início rápido

Antes de iniciar a atualização, reveja o fluxo de trabalho geral. A página Atualização do StorageGRID orienta você em cada etapa de atualização.

1 Prepare hosts Linux

Se algum nó do StorageGRID for implantado em hosts Linux, "Instale o pacote RPM ou DEB em cada host" antes de iniciar a atualização.

2 Carregar ficheiros de atualização e correção

A partir do nó de administração principal, aceda à página Atualização do StorageGRID e carregue o ficheiro de atualização e o ficheiro de correção, se necessário.

3 Baixar Recovery Package

Baixe o pacote de recuperação atual antes de iniciar a atualização.

4 Execute as pré-verificações de atualização

As pré-verificações de atualização ajudam a detetar problemas, para que você possa resolvê-los antes de iniciar a atualização real.

5 Inicie a atualização

Quando você inicia a atualização, as pré-verificações são executadas novamente e o nó de administração principal é atualizado automaticamente. Não é possível acessar o Gerenciador de Grade enquanto o nó Admin principal estiver sendo atualizado. Os logs de auditoria também estarão indisponíveis. Esta atualização pode demorar até 30 minutos.

6 Baixar Recovery Package

Depois que o nó Admin principal tiver sido atualizado, faça o download de um novo pacote de recuperação.

7 Aprovar nós

Você pode aprovar nós de grade individuais, grupos de nós de grade ou todos os nós de grade.

> Não aprove a atualização para um nó de grade a menos que você tenha certeza de que o nó está pronto para ser interrompido e reinicializado.

8 Retomar as operações

Quando todos os nós de grade tiverem sido atualizados, novos recursos serão ativados e você poderá retomar as operações. Você deve esperar para executar um procedimento de desativação ou expansão até que a tarefa **Atualizar banco de dados** em segundo plano e a tarefa **etapas finais de atualização** tenham sido concluídas.

Informações relacionadas

"Estime o tempo para concluir uma atualização"

Linux: Baixe e instale o pacote RPM ou DEB em todos os hosts

Se algum nó StorageGRID for implantado em hosts Linux, baixe e instale um pacote RPM ou DEB adicional em cada um desses hosts antes de iniciar a atualização.

Faça o download de arquivos de atualização, Linux e hotfix

Ao executar uma atualização do StorageGRID a partir do Gerenciador de Grade, você será solicitado a baixar o arquivo de atualização e qualquer hotfix necessário como a primeira etapa. No entanto, se você precisar baixar arquivos para atualizar hosts Linux, você pode economizar tempo baixando todos os arquivos necessários com antecedência.

Passos

1. Vá para "NetApp Downloads: StorageGRID".
2. Selecione o botão para baixar a versão mais recente ou selecione outra versão no menu suspenso e selecione **Go**.

   As versões do software StorageGRID têm este formato: 11.*x.y*. Os hotfixes do StorageGRID têm este formato: 11.*x.y.z*.

3. Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.
4. Se um aviso de cuidado/MustRead for exibido, anote o número do hotfix e marque a caixa de seleção.
5. Leia o Contrato de Licença de Utilizador final (EULA), selecione a caixa de verificação e, em seguida, selecione **Accept & continue**.

   É apresentada a página de transferências para a versão selecionada. A página contém três colunas.

6. Na segunda coluna (**Upgrade StorageGRID**), baixe dois arquivos:

- O arquivo de atualização para a versão mais recente (este é o arquivo na seção **VMware, SG1000 ou SG100 Main Admin Node**). Embora esse arquivo não seja necessário até que você execute a atualização, baixá-lo agora economizará tempo.
- Um arquivo RPM ou DEB em qualquer `.tgz` formato ou `.zip`. Selecione o `.zip` ficheiro se estiver a executar o Windows no computador portátil de serviço.
  - Red Hat Enterprise Linux
    `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
    `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
  - Ubuntu ou Debian
    `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
    `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

7. Se você precisar concordar com um aviso de cuidado/MustRead devido a um hotfix necessário, baixe o hotfix:
   a. Volte para "NetApp Downloads: StorageGRID".
   b. Selecione o número do hotfix na lista suspensa.
   c. Aceite novamente o aviso de precaução e o EULA.
   d. Baixe e salve o hotfix e seu README.

      Ser-lhe-á pedido que carregue o ficheiro de correção na página Atualização do StorageGRID quando iniciar a atualização.

Instale o arquivo em todos os hosts Linux

Execute estas etapas antes de atualizar o software StorageGRID.

Passos

1. Extraia os pacotes RPM ou DEB do arquivo de instalação.
2. Instale os pacotes RPM ou DEB em todos os hosts Linux.

   Consulte as etapas para instalar os serviços de host do StorageGRID nas instruções de instalação:

   - "Red Hat Enterprise Linux: Instale os serviços de host do StorageGRID"
   - "Ubuntu ou Debian: Instale serviços host StorageGRID"

   Os novos pacotes são instalados como pacotes adicionais.

Remover arquivos de instalação para versões anteriores

Para liberar espaço em hosts Linux, você pode remover os arquivos de instalação de versões anteriores do StorageGRID que você não precisa mais.

Passos

1. Remova os arquivos de instalação antigos do StorageGRID.

Red Hat

1. Capture a lista de pacotes StorageGRID instalados: `dnf list | grep -i storagegrid`.

   Exemplo:

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. Remover pacotes StorageGRID anteriores: `dnf remove` *`images-package service-package`*

   > ⚠ Não remova os arquivos de instalação para a versão do StorageGRID que você está executando atualmente ou as versões do StorageGRID para o qual você está planejando atualizar.

   Você pode ignorar com segurança os avisos que aparecem. Eles se referem a arquivos que foram substituídos quando você instala pacotes StorageGRID mais recentes.

   Exemplo:

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
================================================================================
```

```
========
Package            Architecture      Version           Repository
Size
================================================================================
========
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
================================================================================
========
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__.
pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:
remove failed: No such file or directory
```

```
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl
itter.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p
yc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:
remove failed: No such file or directory

  Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64   2/2
  Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  2/2
```

```
Installed products updated.

Removed:
  StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64
  StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64

Complete!
[root@rhel-example ~]#
```

Ubuntu e Debian

1. Capture a lista de pacotes StorageGRID instalados: `dpkg -l | grep storagegrid`

   Exemplo:

```
root@debian-example:~# dpkg -l | grep storagegrid
ii  storagegrid-webscale-images-11-6-0  11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale docker images for 11.6.0
ii  storagegrid-webscale-images-11-7-0  11.7.0-
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker
images for 11.7.0
ii  storagegrid-webscale-images-11-8-0  11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale docker images for 11.8.0
ii  storagegrid-webscale-images-11-9-0  11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale docker images for 11.9.0
ii  storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale host services for 11.6.0
ii  storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c
amd64 StorageGRID Webscale host services for 11.7.0
ii  storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale host services for 11.8.0
ii  storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale host services for 11.9.0
root@debian-example:~#
```

2. Remover pacotes StorageGRID anteriores: `dpkg -r images-package service-package`

   > Não remova os arquivos de instalação para a versão do StorageGRID que você está executando atualmente ou as versões do StorageGRID para o qual você está planejando atualizar.

   Exemplo:

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. Remova imagens do recipiente StorageGRID.

Docker

1. Capture a lista de imagens de contentor instaladas: `docker images`

   Exemplo:

```
[root@docker-example ~]# docker images
REPOSITORY           TAG             IMAGE ID       CREATED
SIZE
storagegrid-11.9.0   Admin_Node      610f2595bcb4   2 days ago
2.77GB
storagegrid-11.9.0   Storage_Node    7f73d33eb880   2 days ago
2.65GB
storagegrid-11.9.0   API_Gateway     2f0bb79526e9   2 days ago
1.82GB
storagegrid-11.8.0   Storage_Node    7125480de71b   7 months ago
2.54GB
storagegrid-11.8.0   Admin_Node      404e9f1bd173   7 months ago
2.63GB
storagegrid-11.8.0   Archive_Node    c3294a29697c   7 months ago
2.39GB
storagegrid-11.8.0   API_Gateway     1f88f24b9098   7 months ago
1.74GB
storagegrid-11.7.0   Storage_Node    1655350eff6f   16 months ago
2.51GB
storagegrid-11.7.0   Admin_Node      872258dd0dc8   16 months ago
2.48GB
storagegrid-11.7.0   Archive_Node    121e7c8b6d3b   16 months ago
2.41GB
storagegrid-11.7.0   API_Gateway     5b7a26e382de   16 months ago
1.77GB
storagegrid-11.6.0   Admin_Node      ee39f71a73e1   2 years ago
2.38GB
storagegrid-11.6.0   Storage_Node    f5ef895dcad0   2 years ago
2.08GB
storagegrid-11.6.0   Archive_Node    5782de552db0   2 years ago
1.95GB
storagegrid-11.6.0   API_Gateway     cb480ed37eea   2 years ago
1.35GB
[root@docker-example ~]#
```

2. Remova as imagens do contentor para versões anteriores do StorageGRID: `docker rmi` *`image id`*

Não remova as imagens de contentor para a versão do StorageGRID que você está executando atualmente ou as versões do StorageGRID para o qual você está planejando atualizar.

Exemplo:

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051dd
f02
Deleted:
sha256:5f269aabf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8ccc
afa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66
bde
[root@docker-example ~]#
```

Podman

1. Capture a lista de imagens de contentor instaladas: `podman images`

   Exemplo:

```
[root@podman-example ~]# podman images
REPOSITORY                    TAG           IMAGE ID      CREATED
SIZE
localhost/storagegrid-11.8.0  Storage_Node  7125480de71b  7 months
ago   2.57 GB
localhost/storagegrid-11.8.0  Admin_Node    404e9f1bd173  7 months
ago   2.67 GB
localhost/storagegrid-11.8.0  Archive_Node  c3294a29697c  7 months
ago   2.42 GB
localhost/storagegrid-11.8.0  API_Gateway   1f88f24b9098  7 months
ago   1.77 GB
localhost/storagegrid-11.7.0  Storage_Node  1655350eff6f  16 months
ago  2.54 GB
localhost/storagegrid-11.7.0  Admin_Node    872258dd0dc8  16 months
ago  2.51 GB
localhost/storagegrid-11.7.0  Archive_Node  121e7c8b6d3b  16 months
ago  2.44 GB
localhost/storagegrid-11.7.0  API_Gateway   5b7a26e382de  16 months
ago  1.8 GB
localhost/storagegrid-11.6.0  Admin_Node    ee39f71a73e1  2 years
ago    2.42 GB
localhost/storagegrid-11.6.0  Storage_Node  f5ef895dcad0  2 years
ago    2.11 GB
localhost/storagegrid-11.6.0  Archive_Node  5782de552db0  2 years
ago    1.98 GB
localhost/storagegrid-11.6.0  API_Gateway   cb480ed37eea  2 years
ago    1.38 GB
[root@podman-example ~]#
```

2. Remova as imagens do contentor para versões anteriores do StorageGRID: `podman rmi` *`image id`*

> Não remova as imagens de contentor para a versão do StorageGRID que você está executando atualmente ou as versões do StorageGRID para o qual você está planejando atualizar.

Exemplo:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

Execute a atualização

Você pode atualizar para o StorageGRID 11,9 e aplicar o hotfix mais recente para essa versão ao mesmo tempo. A página de atualização do StorageGRID fornece o caminho de atualização recomendado e links diretamente para as páginas de download corretas.

Antes de começar

Você revisou todas as considerações e concluiu todas as etapas de Planejamento e preparação.

Acesse a página Atualização do StorageGRID

Como primeira etapa, acesse a página Atualização do StorageGRID no Gerenciador de Grade.

Passos

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Selecione **MAINTENANCE** > **System** > **Software update**.
3. No bloco de atualização do StorageGRID, selecione **Upgrade**.

Selecione ficheiros

O caminho de atualização na página Atualização do StorageGRID indica quais versões principais (por exemplo, 11,9.0) e hotfixes (por exemplo, 11,9.0,1) você deve instalar para chegar à versão mais recente do StorageGRID. Você deve instalar as versões recomendadas e hotfixes na ordem mostrada.

> Se não for apresentado nenhum caminho de atualização, o seu browser poderá não conseguir aceder ao Site de suporte da NetApp ou a caixa de verificação **verificar atualizações de software** na página AutoSupport (**SUPPORT** > **Tools** > **AutoSupport** > **Settings**) pode estar desativada.

Passos

1. Para a etapa **Select Files**, revise o caminho de atualização.
2. Na seção Download de arquivos, selecione cada link **Download** para baixar os arquivos necessários do site de suporte da NetApp.

   Se não for apresentado nenhum caminho de atualização, aceda a "NetApp Downloads: StorageGRID" para determinar se está disponível uma nova versão ou correção e para transferir os ficheiros de que necessita.

   > Se você precisar baixar e instalar um pacote RPM ou DEB em todos os hosts Linux, talvez você já tenha os arquivos de atualização e hotfix do StorageGRID listados no caminho de atualização.

3. Selecione **Procurar** para carregar o ficheiro de atualização da versão para o StorageGRID: `NetApp_StorageGRID_11.9.0_Software_uniqueID.upgrade`

   Quando o processo de upload e validação é concluído, uma marca de seleção verde aparece ao lado do nome do arquivo.

4. Se você baixou um arquivo de hotfix, selecione **Procurar** para fazer o upload desse arquivo. O hotfix será aplicado automaticamente como parte da atualização de versão.
5. Selecione **continuar**.

Execute as pré-verificações

Executar pré-verificações permite detetar e resolver quaisquer problemas de atualização antes de iniciar a atualização da grelha.

Passos

1. Para a etapa **Executar pré-verificações**, comece digitando a senha de provisionamento para sua grade.
2. Selecione **Baixar pacote de recuperação**.

   Você deve baixar a cópia atual do arquivo do pacote de recuperação antes de atualizar o nó de administração principal. O arquivo do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.

3. Quando o arquivo for baixado, confirme se você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo.
4. Copie o arquivo 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.

5. Selecione **Executar pré-verificações** e aguarde até que as pré-verificações sejam concluídas.
6. Reveja os detalhes de cada pré-verificação comunicada e resolva quaisquer erros comunicados. "Guia de resolução de atualização do software StorageGRID"Consulte a para obter a versão do StorageGRID 11,9.

   Você deve resolver todos os erros *de pré-verificação* antes de poder atualizar seu sistema. No entanto, você não precisa resolver o pré-check *warnings* antes de atualizar.

   > Se tiver aberto quaisquer portas de firewall personalizadas, será notificado durante a validação de pré-verificação. Você deve entrar em Contato com o suporte técnico antes de prosseguir com a atualização.

7. Se você fez alterações de configuração para resolver os problemas relatados, selecione **Executar pré-verificações** novamente para obter resultados atualizados.

   Se todos os erros tiverem sido resolvidos, você será solicitado a iniciar a atualização.

Inicie a atualização e atualize o nó de administração principal

Quando você inicia a atualização, as pré-verificações de atualização são executadas novamente e o nó de administração principal é atualizado automaticamente. Esta parte da atualização pode demorar até 30 minutos.

> Você não poderá acessar nenhuma outra página do Gerenciador de Grade enquanto o nó Admin principal estiver sendo atualizado. Os logs de auditoria também estarão indisponíveis.

Passos

1. Selecione **Iniciar atualização**.

   Um aviso aparece para lembrar que você perderá temporariamente o acesso ao Gerenciador de Grade.

2. Selecione **OK** para confirmar o aviso e iniciar a atualização.

3. Aguarde que as pré-verificações de atualização sejam executadas e que o nó de administração principal seja atualizado.

   Se algum erro de pré-verificação for relatado, resolva-os e selecione **Iniciar atualização** novamente.

   Se a grade tiver outro nó Admin que esteja on-line e pronto, você poderá usá-lo para monitorar o status do nó Admin principal. Assim que o nó de administração principal for atualizado, você poderá aprovar os outros nós de grade.

4. Conforme necessário, selecione **continuar** para acessar a etapa **Atualizar outros nós**.

Atualizar outros nós

Você deve atualizar todos os nós de grade, mas pode executar várias sessões de atualização e personalizar a sequência de atualização. Por exemplo, você pode preferir atualizar os nós no local A em uma sessão e, em seguida, atualizar os nós no local B em uma sessão posterior. Se você optar por realizar a atualização em mais de uma sessão, esteja ciente de que você não pode começar a usar os novos recursos até que todos os nós tenham sido atualizados.

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 próximo nó ou grupo de nós.

Quando a atualização começa em um nó de grade, os serviços nesse nó são interrompidos. Mais tarde, o nó de grade é reinicializado. Para evitar interrupções de serviço para aplicativos clientes que estão se comunicando com o nó, não aprove a atualização para um nó a menos que você tenha certeza de que o nó está pronto para ser interrompido e reinicializado. Conforme necessário, agende uma janela de manutenção ou notifique os clientes.

Passos

1. Para a etapa **Atualizar outros nós**, revise o Resumo, que fornece a hora de início da atualização como um todo e o status de cada tarefa de atualização principal.
   - **Iniciar serviço de atualização** é a primeira tarefa de atualização. Durante esta tarefa, o arquivo de software é distribuído para os nós de grade e o serviço de atualização é iniciado em cada nó.
   - Quando a tarefa **Start upgrade Service** estiver concluída, a tarefa **Upgrade other Grid Nodes** (Atualizar outros nós de grade) é iniciada e você será solicitado a fazer o download de uma nova cópia do pacote de recuperação.
2. Quando solicitado, insira sua senha de provisionamento e faça o download de uma nova cópia do Pacote de recuperação.

   Você deve fazer o download de uma nova cópia do arquivo do pacote de recuperação depois que o nó de administração principal for atualizado. O arquivo do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.

3. Revise as tabelas de status para cada tipo de nó. Existem tabelas para nós de administração não primários, nós de gateway e nós de storage.

   Um nó de grade pode estar em um desses estágios quando as tabelas aparecem pela primeira vez:

   - Desembalar a atualização
   - A transferir

- A aguardar aprovação

4. quando estiver pronto para selecionar nós de grade para atualização (ou se você precisar desaprovar nós selecionados), use estas instruções:

Tarefa	Instrução
PESQUISE nós específicos para aprovar, como todos os nós em um determinado site	Introduza a cadeia de carateres de pesquisa no campo **pesquisar**
Selecione todos os nós para atualização	Selecione **Approve All Nodes** (aprovar todos os nós)
Selecione todos os nós do mesmo tipo para atualização (por exemplo, todos os nós de storage)	Selecione o botão **Approve All** para o tipo de nó Se aprovar mais de um nó do mesmo tipo, os nós serão atualizados um de cada vez.
Selecione um nó individual para atualização	Selecione o botão **Approve** para o nó
Adiar a atualização em todos os nós selecionados	Selecione **Desaprovar todos os nós**
Adiar a atualização em todos os nós selecionados do mesmo tipo	Selecione o botão **Desaprovar tudo** para o tipo de nó
Adiar a atualização em um nó individual	Selecione o botão **Desaprovar** para o nó

5. Aguarde até que os nós aprovados prossigam esses estágios de atualização:
   - Aprovado e esperando para ser atualizado
   - Parar serviços

     Não é possível remover um nó quando o Stage atinge **parando serviços**. O botão **Desaprovar** está desativado.

   - Parar o recipiente
   - Limpeza de imagens Docker
   - Atualizando pacotes base do SO

     Quando um nó de appliance atinge esse estágio, o software Instalador de appliance StorageGRID no appliance é atualizado. Esse processo automatizado garante que a versão do instalador do StorageGRID Appliance permaneça sincronizada com a versão do software StorageGRID.

   - A reiniciar

     Alguns modelos de appliance podem reiniciar várias vezes para atualizar o firmware e o BIOS.

- Executar etapas após a reinicialização
- Iniciar serviços
- Concluído

6. Repita o passo de aprovação quantas vezes for necessário até que todos os nós da grade tenham sido atualizados.

Atualização completa

Quando todos os nós de grade tiverem concluído os estágios de atualização, a tarefa **Atualizar outros nós de grade** é mostrada como concluída. As restantes tarefas de atualização são executadas automaticamente em segundo plano.

Passos

1. Assim que a tarefa **Ativar recursos** estiver concluída (o que ocorre rapidamente), você pode começar a usar o "novas funcionalidades"na versão atualizada do StorageGRID.
2. Durante a tarefa **Atualizar banco de dados**, o processo de atualização verifica cada nó para verificar se o banco de dados Cassandra não precisa ser atualizado.

> A atualização do StorageGRID 11,8 para o 11,9 não requer uma atualização do banco de dados Cassandra; no entanto, o serviço Cassandra será interrompido e reiniciado em cada nó de armazenamento. Para futuras versões de recursos do StorageGRID, a etapa de atualização do banco de dados do Cassandra pode levar vários dias para ser concluída.

3. Quando a tarefa **Atualizar banco de dados** estiver concluída, aguarde alguns minutos para que os **passos finais de atualização** sejam concluídos.
4. Quando os **passos de atualização final** tiverem sido concluídos, a atualização é feita. O primeiro passo, **Select Files**, é reexibido com um banner verde de sucesso.
5. Verifique se as operações da grade voltaram ao normal:
   a. Verifique se os serviços estão a funcionar normalmente e se não existem alertas inesperados.
   b. Confirme se as conexões do cliente com o sistema StorageGRID estão operando conforme esperado.

Solucionar problemas de atualização

Se algo der errado quando você executa uma atualização, você pode resolver o problema sozinho. Se você não conseguir resolver um problema, reúna o máximo de informações possível e entre em Contato com o suporte técnico.

A atualização não foi concluída

As seções a seguir descrevem como recuperar de situações em que a atualização falhou parcialmente.

Atualizar erros de pré-verificação

Para detetar e resolver problemas, você pode executar manualmente as pré-verificações de atualização antes de iniciar a atualização real. A maioria dos erros de pré-verificação fornece informações sobre como resolver o problema.

Falhas de provisionamento

Se o processo de provisionamento automático falhar, entre em Contato com o suporte técnico.

O nó de grade falha ou falha ao iniciar

Se um nó de grade falhar durante o processo de atualização ou não conseguir iniciar com êxito após a conclusão da atualização, entre em Contato com o suporte técnico para investigar e corrigir quaisquer problemas subjacentes.

A obtenção ou recuperação de dados é interrompida

Se a ingestão ou recuperação de dados for inesperadamente interrompida quando você não estiver atualizando um nó de grade, entre em Contato com o suporte técnico.

Erros de atualização do banco de dados

Se a atualização do banco de dados falhar com um erro, tente novamente a atualização. Se falhar novamente, entre em Contato com o suporte técnico.

Informações relacionadas

"Verificar o estado do sistema antes de atualizar o software"

Problemas na interface do usuário

Você pode ter problemas com o Gerenciador de Grade ou o Gerenciador de Locatário durante ou após a atualização.

O Grid Manager exibe várias mensagens de erro durante a atualização

Se você atualizar seu navegador ou navegar para outra página do Gerenciador de Grade enquanto o nó Admin principal estiver sendo atualizado, você poderá ver várias mensagens "503: Serviço indisponível" e "problema na conexão com o servidor". Você pode ignorar essas mensagens com segurança, elas deixarão de aparecer assim que o nó for atualizado.

Se essas mensagens forem exibidas por mais de uma hora depois de iniciar a atualização, talvez tenha ocorrido algo que impediu que o nó de administração principal fosse atualizado. Se você não conseguir resolver o problema sozinho, entre em Contato com o suporte técnico.

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 normalmente muda para cada versão do StorageGRID.

- 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.

Mensagens de erro "verificação de disponibilidade de imagem Docker"

Ao tentar iniciar o processo de atualização, você pode receber uma mensagem de erro que diz "os seguintes problemas foram identificados pelo pacote de validação de verificação de disponibilidade de imagem Docker". Todos os problemas devem ser resolvidos antes que você possa concluir a atualização.

Contacte o suporte técnico se não tiver a certeza das alterações necessárias para resolver os problemas identificados.

Mensagem	Causa	Solução
Não foi possível determinar a versão de atualização. O ficheiro de informação da versão de atualização `{file_path}` não corresponde ao formato esperado.	O pacote de atualização está corrompido.	Volte a carregar o pacote de atualização e tente novamente. Se o problema persistir, entre em Contato com o suporte técnico.
O ficheiro de informação da versão de atualização `{file_path}` não foi encontrado. Não foi possível determinar a versão de atualização.	O pacote de atualização está corrompido.	Volte a carregar o pacote de atualização e tente novamente. Se o problema persistir, entre em Contato com o suporte técnico.
Não foi possível determinar a versão de versão instalada no `{node_name}`.	Um arquivo crítico no nó está corrompido.	Entre em Contato com o suporte técnico.
Erro de ligação ao tentar listar versões em `{node_name}`	O nó está offline ou a conexão foi interrompida.	Verifique se todos os nós estão online e acessíveis a partir do nó de administração principal e tente novamente.
O host para nó `{node_name}` não tem a imagem StorageGRID `{upgrade_version}` carregada. As imagens e os serviços devem ser instalados no host antes que a atualização possa prosseguir.	Os pacotes RPM ou DEB para a atualização não foram instalados no host onde o nó está sendo executado, ou as imagens ainda estão em processo de importação. **Nota:** este erro só se aplica a nós que estão sendo executados como contentores no Linux.	Verifique se os pacotes RPM ou DEB foram instalados em todos os hosts Linux em que os nós estão sendo executados. Certifique-se de que a versão está correta tanto para o serviço como para o ficheiro de imagens. Aguarde alguns minutos e tente novamente. "Linux: Instale o pacote RPM ou DEB em todos os hosts"Consulte .
Erro ao verificar o nó `{node_name}`	Ocorreu um erro inesperado.	Aguarde alguns minutos e tente novamente.
Erro não detetado durante a execução das pré-verificações. `{error_string}`	Ocorreu um erro inesperado.	Aguarde alguns minutos e tente novamente.

Aplique o hotfix do 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

Não é possível aplicar um hotfix do StorageGRID quando outro procedimento de manutenção estiver sendo executado. Por exemplo, não é possível aplicar um hotfix enquanto um procedimento de desativação, expansão ou recuperação estiver em execução.

> 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 de 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.

Para obter mais informações, "Configure o nó de administração principal de substituição"consulte .

Como seu sistema é afetado quando você aplica um hotfix

Você deve entender como seu sistema StorageGRID será afetado quando você aplicar um hotfix.

Os hotfixes do StorageGRID não causam interrupções

O sistema StorageGRID pode obter e recuperar dados de aplicativos clientes durante todo o processo de hotfix. Se você aprovar todos os nós do mesmo tipo para hotfix (por exemplo, nós de storage), os nós serão derrubados um de cada vez, portanto, não haverá tempo em que todos os nós de grade ou todos os nós de grade de um determinado tipo não estejam disponíveis.

Para permitir disponibilidade contínua, verifique se sua política de ILM contém regras que especificam o armazenamento de várias cópias de cada objeto. Você também deve garantir que todos os clientes S3 externos estejam configurados para enviar solicitações para um dos seguintes:

- Um endereço IP virtual do grupo de alta disponibilidade (HA)
- Um balanceador de carga de terceiros de alta disponibilidade
- Vários nós de gateway para cada cliente
- Vários nós de storage para cada cliente

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 conetividade 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 conetividade 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.
• 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"caso ocorram problemas durante o hotfix. Em seguida, 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 faz parte do arquivo Recovery Package `.zip`.
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 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.

Transfira o ficheiro de correção

Tem de transferir o ficheiro de correção para poder aplicar a correção.

Passos

1. Vá para "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 tiver apenas "Recuperado o nó de administração principal" e precisar aplicar um hotfix, selecione a mesma versão de hotfix 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**.

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 conetados à grade.

   Os nós conetados têm marcas de verificação verdes na página nós.

3. Verifique e resolva quaisquer alertas atuais, se possível.
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, não é possível aplicar um hotfix enquanto um procedimento de desativação, expansão ou recuperação estiver em execução.

Se um nó ou site "o procedimento de desativação está em pausa", 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 "Atualizando o software StorageGRID".

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.

Antes de começar

- Você revisou o "considerações para aplicar um hotfix".
- Você tem a senha de provisionamento.
- Você tem acesso root ou a permissão Manutenção.

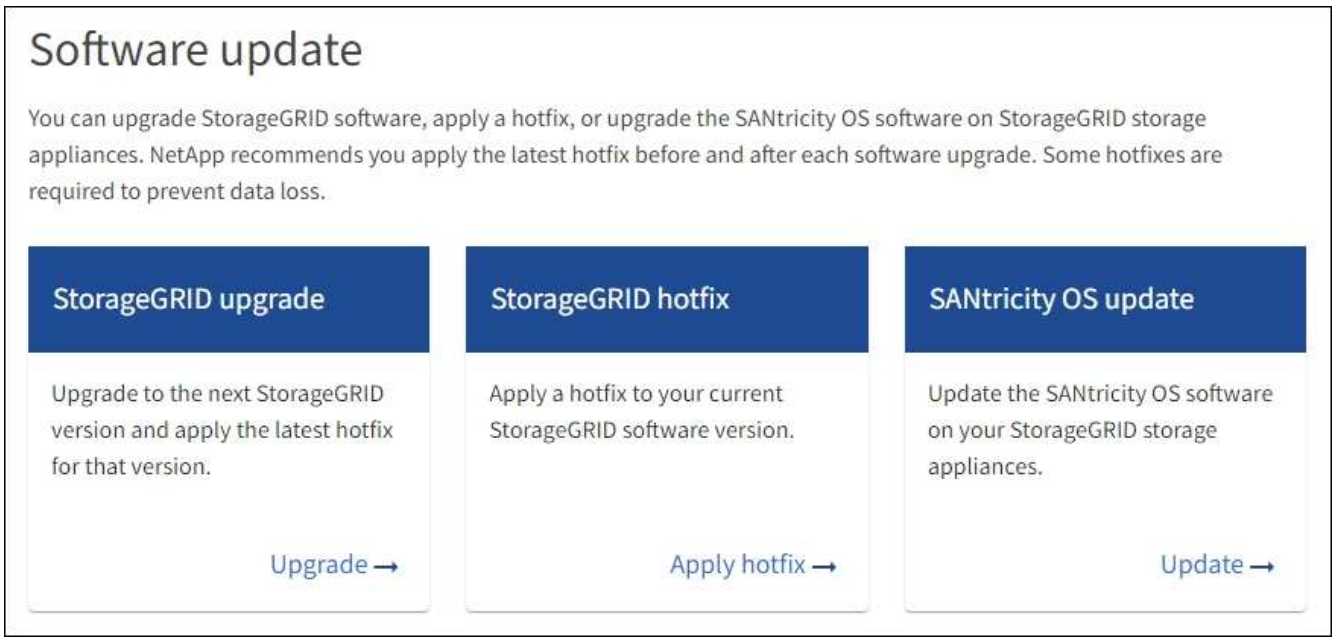
Sobre esta tarefa

- 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 o processo de correção seja concluído.

Passos

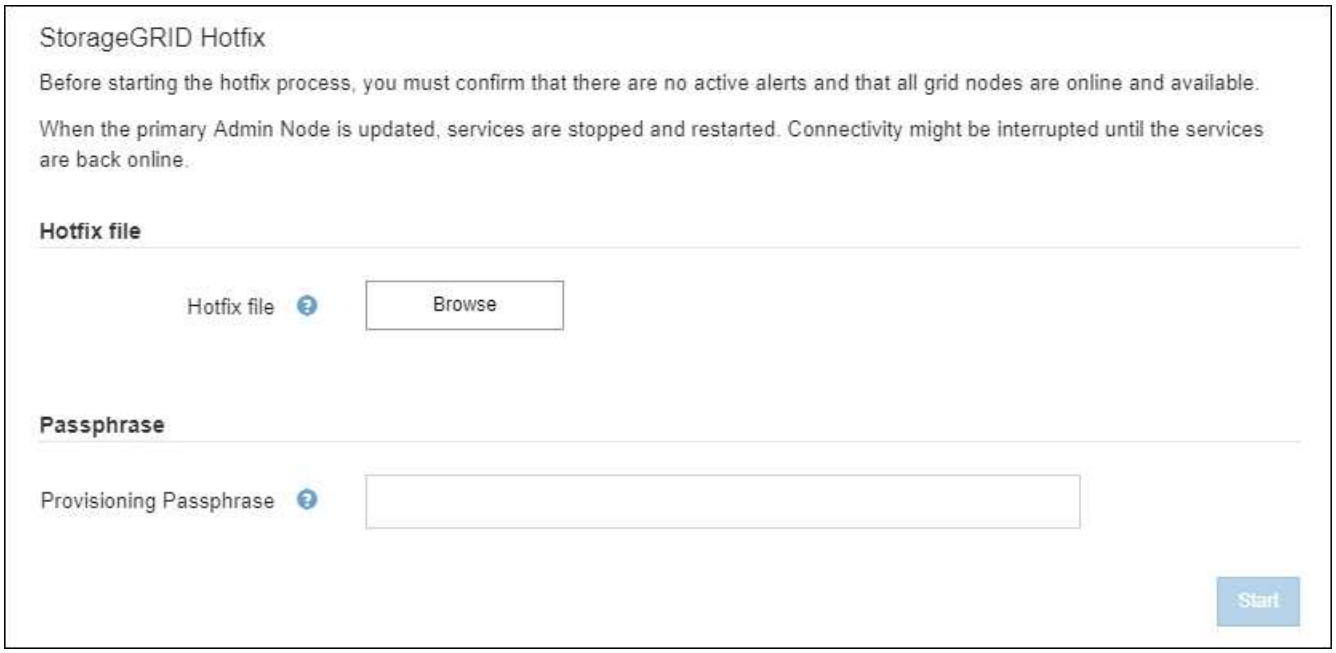
1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Selecione **MAINTENANCE** > **System** > **Software update**.

   A página Atualização de software é exibida.



3. Selecione **aplicar hotfix**.

   A página de correção do StorageGRID é exibida.



4. Selecione o arquivo de hotfix que você baixou no site de suporte da NetApp.

   a. Selecione **Procurar**.

   b. Localize e selecione o ficheiro.

      `hotfix-install-version`

   c. 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 porque 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.

7. Selecione **OK** para começar a aplicar o hotfix ao nó de administração principal.

   Quando o hotfix é iniciado:

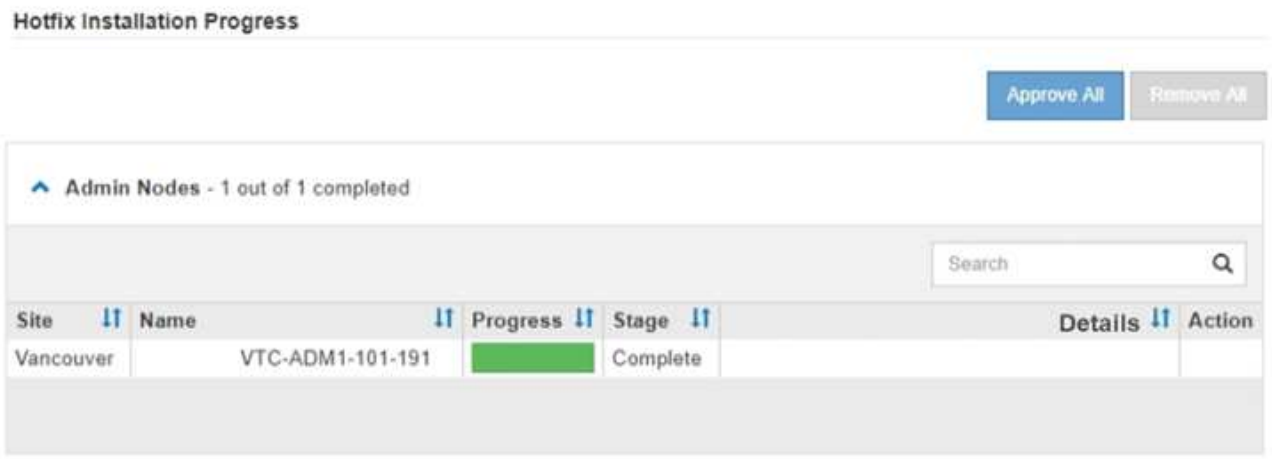
   a. As validações de hotfix são executadas.

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 administrador, nós de gateway e nós de storage).

c. A barra de progresso atinge a conclusão e, em seguida, o nó de administração principal é mostrado como "completo".



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 é 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.

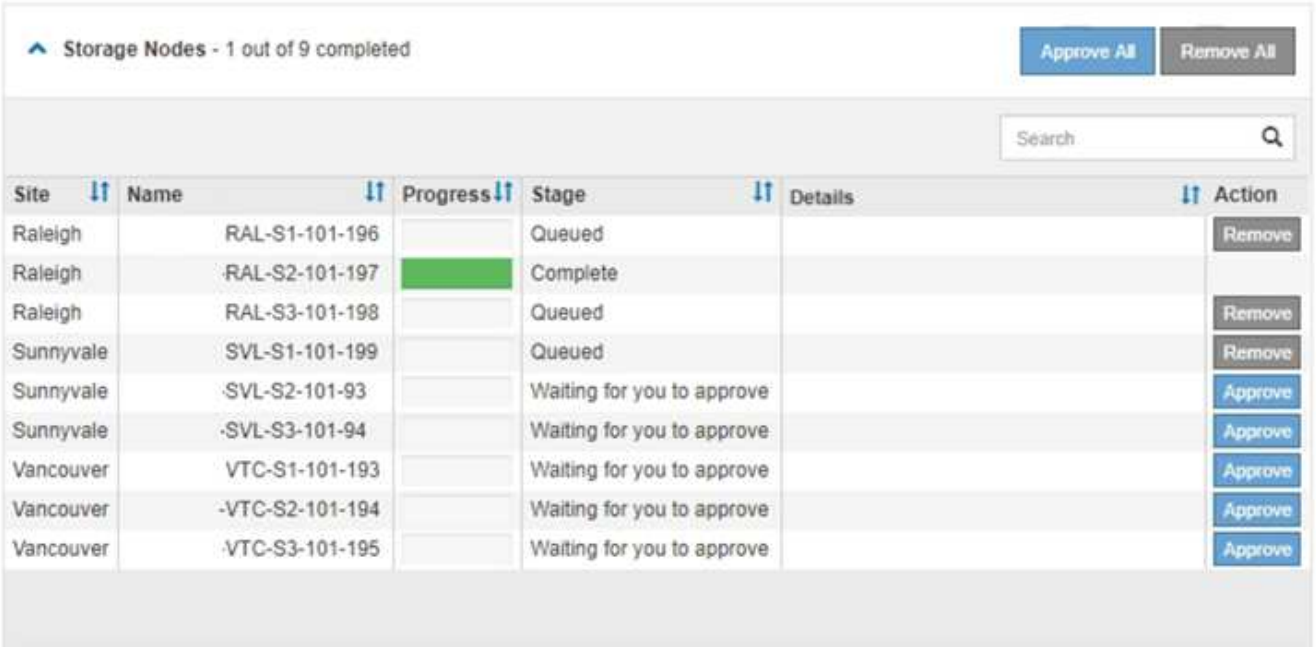
     O botão **Approve All** na parte superior da página aprova todos os nós listados na página, enquanto o botão **Approve All** na parte superior de um agrupamento de tabelas só aprova todos os nós nesse grupo. Se a ordem em que os nós são atualizados for importante, aprove nós ou grupos de nós um de cada 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 **Remover** ou **Remover tudo** para remover um nó ou todos os nós da fila de correções.

  Quando o Estágio progride além de "enfileirado", o botão **Remover** fica oculto e você não pode mais remover o nó do processo de hotfix.



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.

Configurar e gerenciar um sistema StorageGRID

Administrar o StorageGRID

Administrar o StorageGRID

Use estas instruções para configurar e administrar um sistema StorageGRID.

Sobre estas instruções

As principais tarefas de configuração e administração do StorageGRID permitem:

- Use o Gerenciador de Grade para configurar grupos e usuários
- Crie contas de inquilino para permitir que aplicativos clientes S3 armazenem e recuperem objetos
- Configurar e gerenciar redes StorageGRID
- Configurar o AutoSupport
- Gerencie as configurações do nó

Antes de começar

- Você tem uma compreensão geral do sistema StorageGRID.
- Você tem conhecimento bastante detalhado de shells de comando do Linux, rede e configuração e configuração de hardware do servidor.

Comece a usar o Grid Manager

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Faça login no Gerenciador de Grade

Você acessa a página de login do Gerenciador de Grade inserindo o nome de domínio totalmente qualificado (FQDN) ou o endereço IP de um nó Admin na barra de endereços de um navegador da Web compatível.

Cada sistema StorageGRID inclui um nó de administração principal e qualquer número de nós de administração não primários. Você pode entrar no Gerenciador de Grade em qualquer nó de administrador para gerenciar o sistema StorageGRID. No entanto, alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

Ligar ao grupo HA

Se os nós de administração estiverem incluídos em um grupo de alta disponibilidade (HA), você se conetará usando o endereço IP virtual do grupo de HA ou um nome de domínio totalmente qualificado que mapeia para o endereço IP virtual. O nó de administração principal deve ser selecionado como a interface principal do grupo, de modo que, quando você acessa o Gerenciador de grade, você o acessa no nó de administração principal, a menos que o nó de administração principal não esteja disponível. "Gerenciar grupos de alta disponibilidade"Consulte .

Use SSO

Os passos de início de sessão são ligeiramente diferentes se "Logon único (SSO) foi configurado".

Inicie sessão no Grid Manager no primeiro nó de administração

Antes de começar

- Você tem suas credenciais de login.
- Você está usando um "navegador da web suportado".
- Os cookies são ativados no seu navegador.
- Você pertence a um grupo de usuários que tem pelo menos uma permissão.
- Você tem o URL para o Gerenciador de Grade:

  `https://FQDN_or_Admin_Node_IP/`

  Você pode usar o nome de domínio totalmente qualificado, o endereço IP de um nó Admin ou o endereço IP virtual de um grupo de HA de nós Admin.

  Para acessar o Gerenciador de Grade em uma porta diferente da porta padrão para HTTPS (443), inclua o número da porta no URL:

  `https://FQDN_or_Admin_Node_IP:port/`

  > O SSO não está disponível na porta do Gerenciador de Grade restrito. Tem de utilizar a porta 443.

Passos

1. Inicie um navegador da Web compatível.
2. Na barra de endereços do navegador, insira o URL do Gerenciador de Grade.

3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador. "Gerenciar certificados de segurança"Consulte .
4. Faça login no Gerenciador de Grade.

   O ecrã de início de sessão que aparece depende se o início de sessão único (SSO) foi configurado para o StorageGRID.

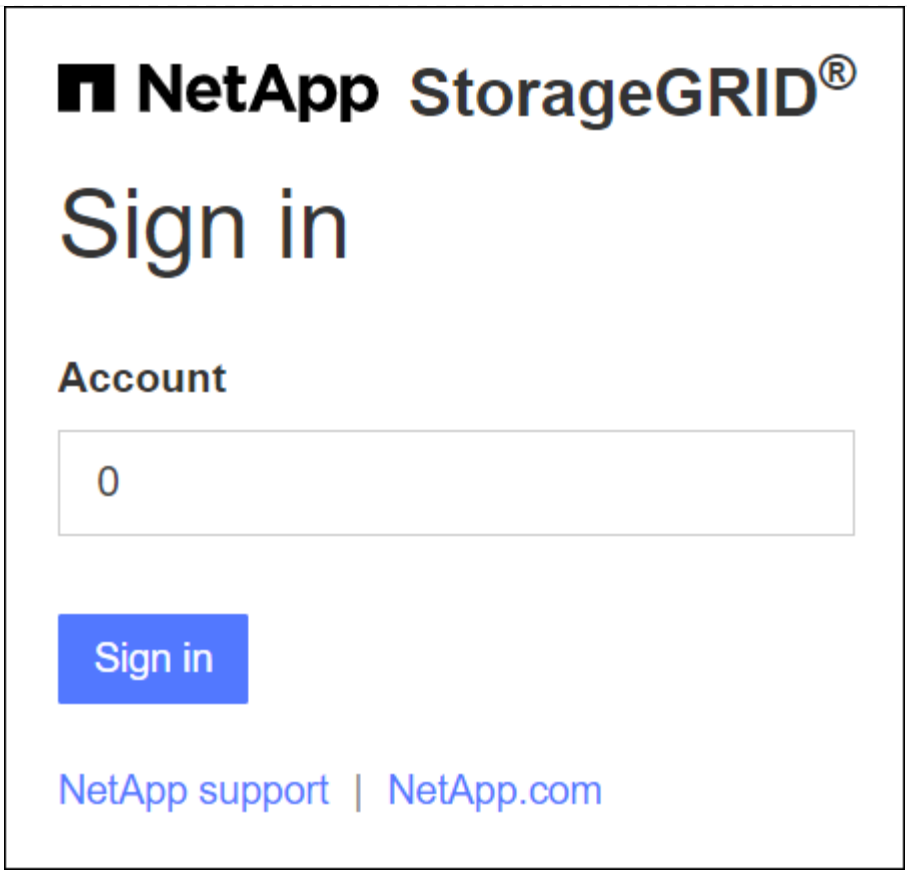
Não está a utilizar SSO

a. Insira seu nome de usuário e senha para o Gerenciador de Grade.

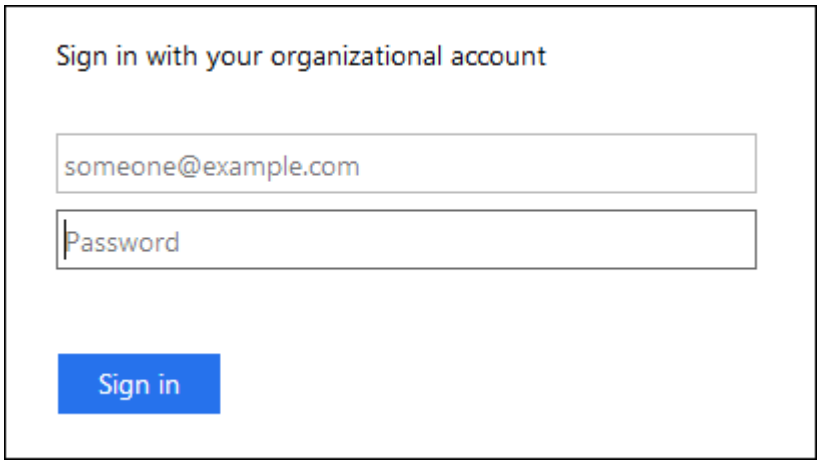
b. Selecione **entrar**.

Usando SSO

- Se o StorageGRID estiver usando SSO e esta é a primeira vez que você acessou o URL neste navegador:
  i. Selecione **entrar**. Você pode deixar o 0 no campo conta.



ii. Insira suas credenciais SSO padrão na página de login SSO da sua organização. Por exemplo:

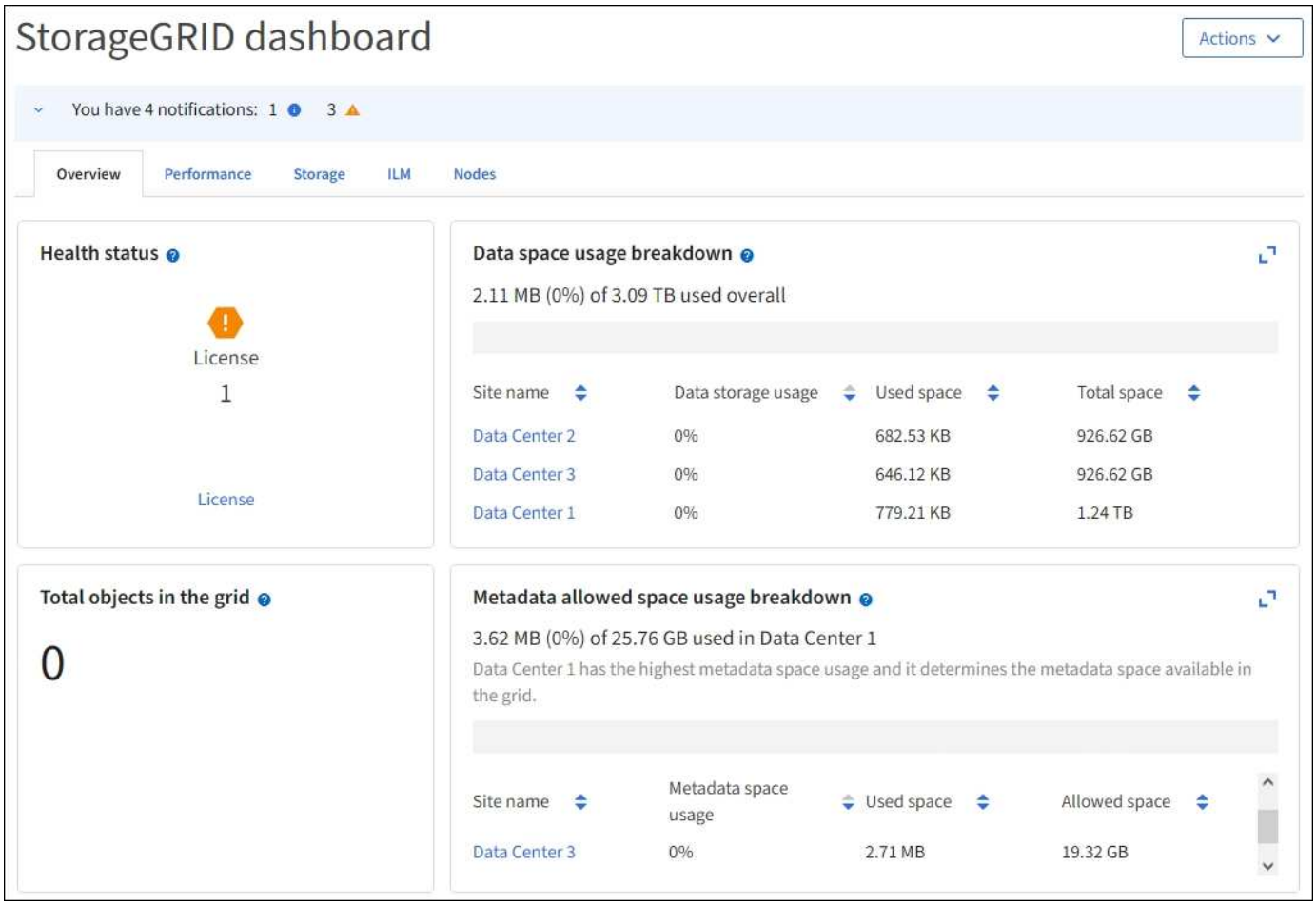


- Se o StorageGRID estiver usando SSO e você tiver acessado anteriormente o Gerenciador de Grade ou uma conta de locatário:
  i. Digite **0** (o ID da conta do Gerenciador de Grade) ou selecione **Gerenciador de Grade** se aparecer na lista de contas recentes.

ii. Selecione **entrar**.

iii. Inicie sessão com as suas credenciais SSO padrão na página de início de sessão SSO da sua organização.

Quando você estiver conetado, a página inicial do Gerenciador de Grade será exibida, que inclui o painel. Para saber quais informações são fornecidas, "Visualizar e gerenciar o painel"consulte .



Entre em outro nó de administração

Siga estes passos para iniciar sessão noutro nó de administração.

Não está a utilizar SSO

Passos

1. Na barra de endereços do navegador, insira o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração. Inclua o número da porta conforme necessário.
2. Insira seu nome de usuário e senha para o Gerenciador de Grade.
3. Selecione **entrar**.

Usando SSO

Se o StorageGRID estiver usando SSO e você tiver feito login em um nó de administrador, você poderá acessar outros nós de administrador sem precisar fazer login novamente.

Passos

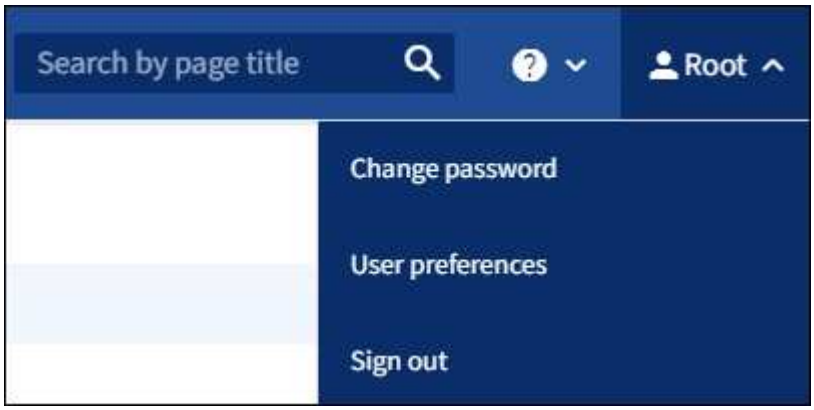
1. Introduza o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração na barra de endereços do browser.
2. Se sua sessão SSO expirou, insira suas credenciais novamente.

Saia do Grid Manager

Quando terminar de trabalhar com o Gerenciador de Grade, você deve sair para garantir que usuários não autorizados não possam acessar o sistema StorageGRID. Fechar seu navegador pode não sair do sistema, com base nas configurações de cookies do navegador.

Passos

1. Selecione seu nome de usuário no canto superior direito.



2. Selecione **Sair**.

Opção	Descrição
SSO não em uso	Você está desconetado do Admin Node. A página de login do Gerenciador de Grade é exibida. **Nota:** se você tiver feito login em mais de um nó Admin, você deve sair de cada nó.
SSO ativado	Você está desconetado de todos os nós de administrador que estava acessando. É apresentada a página de início de sessão do StorageGRID. **Grid Manager** está listado como padrão no menu suspenso **Recent Accounts** e o campo **Account ID** mostra 0. **Observação:** se o SSO estiver ativado e você também estiver conetado ao Gerenciador de Locatário, você também "saia da conta de locatário" deverá entrar "Sair do SSO"no .

Altere a sua palavra-passe

Se você é um usuário local do Gerenciador de Grade, você pode alterar sua própria senha.

Antes de começar

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

Sobre esta tarefa

Se você entrar no StorageGRID como um usuário federado ou se o logon único (SSO) estiver ativado, não será possível alterar sua senha no Gerenciador de Grade. Em vez disso, você deve alterar sua senha na fonte de identidade externa, por exemplo, ative Directory ou OpenLDAP.

Passos

1. No cabeçalho do Gerenciador de Grade, selecione ***your name*** > **Change password**.
2. Introduza a sua palavra-passe atual.
3. Introduza uma nova palavra-passe.

   Sua senha deve conter pelo menos 8 e não mais de 32 carateres. As senhas diferenciam maiúsculas de minúsculas.

4. Volte a introduzir a nova palavra-passe.
5. Selecione **Guardar**.

Veja as informações da licença do StorageGRID

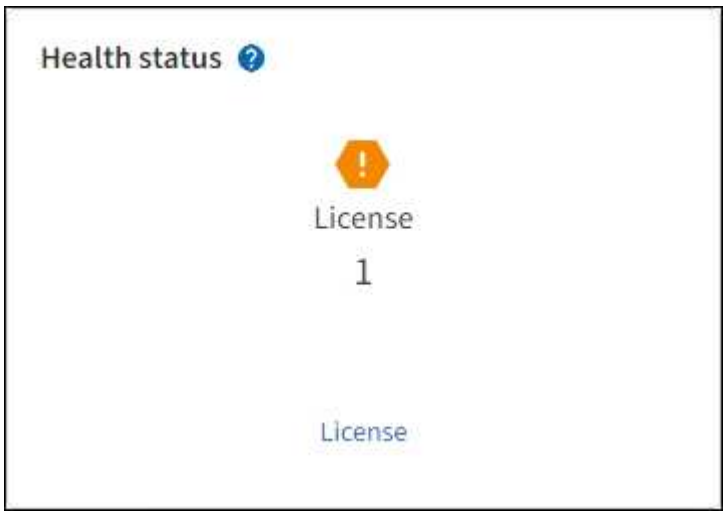
Você pode visualizar as informações de licença do seu sistema StorageGRID, como a capacidade máxima de armazenamento da grade, sempre que necessário.

Antes de começar

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

Sobre esta tarefa

Se houver um problema com a licença de software para este sistema StorageGRID, o cartão de status de integridade no painel inclui um ícone de status de licença e um link **Licença**. O número indica o número de problemas relacionados à licença.



Passos

1. Acesse a página Licença executando um dos seguintes procedimentos:
   - Selecione **MAINTENANCE** > **System** > **License**.
   - No cartão de estado de saúde no painel, selecione o ícone de estado da licença ou o link **Licença**.

     Este link aparece somente se houver um problema com a licença.

2. Veja os detalhes somente leitura da licença atual:
   - ID do sistema StorageGRID, que é o número de identificação exclusivo para esta instalação do StorageGRID
   - Número de série da licença
   - Tipo de licença, seja **Perpetual** ou **assinatura**
   - Capacidade de armazenamento licenciada da rede
   - Capacidade de armazenamento suportada
   - Data de término da licença. **N/A** aparece para uma licença perpétua.
   - Data de término do suporte

     Essa data é lida a partir do arquivo de licença atual e pode estar desatualizada se você estendeu ou renovou o contrato de serviço de suporte após a obtenção do arquivo de licença. Para atualizar esse valor, "Atualizar informações de licença do StorageGRID"consulte . Você também pode visualizar a data de término real do contrato usando o Active IQ.

   - Conteúdo do arquivo de texto da licença

Atualizar informações de licença do StorageGRID

Você deve atualizar as informações de licença do seu sistema StorageGRID a qualquer momento que os termos de sua licença mudarem. Por exemplo, você deve atualizar as informações da licença se adquirir capacidade de armazenamento adicional para sua grade.

Antes de começar

- Você tem um novo arquivo de licença para aplicar ao seu sistema StorageGRID.
- Você "permissões de acesso específicas"tem .
- Você tem a senha de provisionamento.

Passos

1. Selecione **MAINTENANCE** > **System** > **License**.
2. Na seção Atualizar licença, selecione **Procurar**.
3. Localize e selecione o novo ficheiro de licença (`.txt`).

   O novo ficheiro de licença é validado e apresentado.

4. Introduza a frase-passe de aprovisionamento.
5. Selecione **Guardar**.

Use a API

Use a API de gerenciamento de grade

Você pode executar tarefas de gerenciamento do sistema usando a API REST do Grid Management em vez da interface de usuário do Grid Manager. Por exemplo, você pode querer usar a API para automatizar operações ou criar várias entidades, como usuários, mais rapidamente.

Recursos de nível superior

A API de gerenciamento de grade fornece os seguintes recursos de nível superior:

- `/grid`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas.
- `/org`: O acesso é restrito a usuários que pertencem a um grupo LDAP local ou federado para uma conta de locatário. Para obter detalhes, "Use uma conta de locatário"consulte .
- `/private`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas. As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

Emitir solicitações de API

A API de gerenciamento de grade usa a plataforma de API de código aberto Swagger. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores realizem operações em tempo real no StorageGRID com a API.

A interface do usuário Swagger fornece detalhes completos e documentação para cada operação da API.

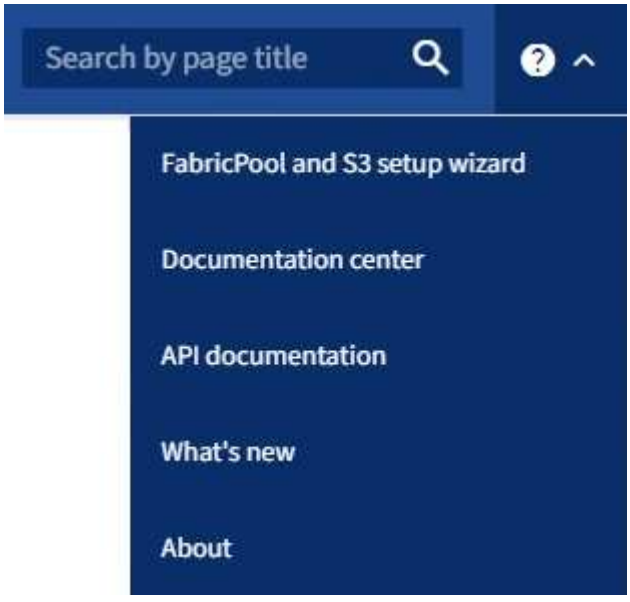
Antes de começar

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

> Todas as operações de API executadas usando a página da Documentação da API são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. No cabeçalho do Gerenciador de Grade, selecione o ícone de ajuda e selecione **Documentação da API**.



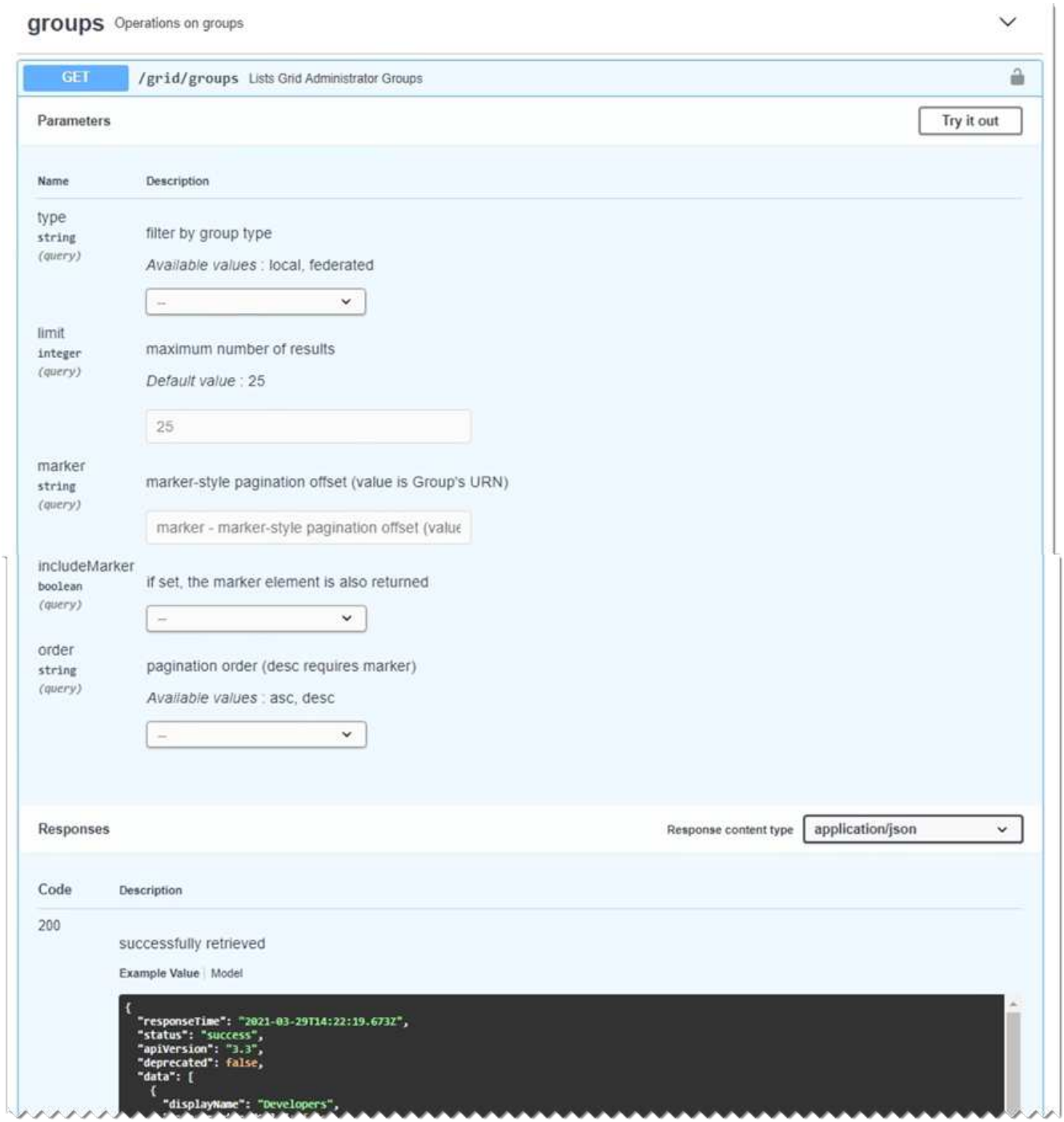
2. Para executar uma operação com a API privada, selecione **ir para a documentação da API privada** na página da API de gerenciamento do StorageGRID.

As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

3. Selecione a operação desejada.

   Ao expandir uma operação de API, você pode ver as ações HTTP disponíveis, como GET, PUT, UPDATE e DELETE.

4. Selecione uma ação HTTP para ver os detalhes da solicitação, incluindo o URL do endpoint, uma lista de todos os parâmetros necessários ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.



5. Determine se a solicitação requer parâmetros adicionais, como um grupo ou ID de usuário. Em seguida,

obtenha esses valores. Talvez você precise emitir uma solicitação de API diferente primeiro para obter as informações de que precisa.

6. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode selecionar **modelo** para aprender os requisitos para cada campo.
7. Selecione **Experimente**.
8. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
9. Selecione **Executar**.
10. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API Grid Management

A API Grid Management organiza as operações disponíveis nas seções a seguir.

Esta lista inclui apenas as operações disponíveis na API pública.

- **Contas**: Operações para gerenciar contas de inquilinos de armazenamento, incluindo a criação de novas contas e recuperação de uso de armazenamento para uma determinada conta.
- **Alert-history**: Operações em alertas resolvidos.
- **Alert-receivers**: Operações em recetores de notificação de alerta (e-mail).
- **Alert-rules**: Operações em regras de alerta.
- **Silêncios de alerta**: Operações em silêncios de alerta.
- **Alertas**: Operações em alertas.
- **Audit**: Operações para listar e atualizar a configuração da auditoria.
- **Auth**: Operações para realizar autenticação de sessão do usuário.

  A API de gerenciamento de grade suporta o esquema de autenticação de token do portador. Para fazer login, você fornece um nome de usuário e senha no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com êxito, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("autorização: Portador *token*"). O token expira após 16 horas.

  Se o logon único estiver ativado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte "autenticar na API se o logon único estiver ativado."

  Consulte "proteção contra falsificação de solicitação entre sites" para obter informações sobre como melhorar a segurança de autenticação.

- **Certificados de cliente**: Operações para configurar certificados de cliente para que o StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **Config**: Operações relacionadas à versão do produto e versões da API Grid Management. Você pode listar a versão de lançamento do produto e as principais versões da API de Gerenciamento de Grade suportadas por essa versão, e você pode desativar versões obsoletas da API.
- **Disabled-features**: Operações para visualizar recursos que podem ter sido desativados.
- **Servidores dns**: Operações para listar e alterar servidores DNS externos configurados.
- **Detalhes da unidade**: Operações em unidades para modelos específicos de dispositivos de armazenamento.

- * Endpoint-domain-nanos*: Operações para listar e alterar nomes de domínio de endpoint S3.
- **Codificação de apagamento**: Operações em perfis de codificação de apagamento.
- **Expansão**: Operações de expansão (nível de procedimento).
- **Expansion-nonos**: Operações em expansão (nível de nó).
- **Expansão-sites**: Operações em expansão (nível do local).
- **Grid-networks**: Operações para listar e alterar a Grid Network List.
- * Grid-passwords*: Operações para gerenciamento de senhas de grade.
- **Groups**: Operações para gerenciar grupos de Administrador de Grade local e recuperar grupos de Administrador de Grade federados de um servidor LDAP externo.
- **Identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **ilm**: Operações de gerenciamento do ciclo de vida da informação (ILM).
- **In-progress-Procedures**: Recupera os procedimentos de manutenção que estão atualmente em andamento.
- **Licença**: Operações para recuperar e atualizar a licença StorageGRID.
- **Logs**: Operações para coletar e baixar arquivos de log.v
- **Métricas**: Operações em métricas do StorageGRID, incluindo consultas de métricas instantâneas em um único ponto no tempo e consultas de métricas de intervalo ao longo de um intervalo de tempo. A API Grid Management usa a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de back-end. Para obter informações sobre a construção de consultas Prometheus, consulte o site Prometheus.

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

- * Node-details*: Operações em detalhes do nó.
- **Node-health**: Operações no status de integridade do nó.
- **Node-storage-State**: Operações no status de armazenamento de nós.
- **ntp-serviders**: Operações para listar ou atualizar servidores NTP (Network Time Protocol) externos.
- * Objetos*: Operações em objetos e metadados de objetos.
- **Recuperação**: Operações para o procedimento de recuperação.
- **Recovery-package**: Operações para baixar o Recovery Package.
- **Regiões**: Operações para visualizar e criar regiões.
- **S3-object-lock**: Operações em configurações globais de bloqueio de objetos S3D.
- **Certificado de servidor**: Operações para visualizar e atualizar certificados de servidor do Grid Manager.
- **snmp**: Operações na configuração SNMP atual.
- **Marcas d'água de armazenamento**: Marcas d'água de nó de armazenamento.
- **Classes de tráfego**: Operações para políticas de classificação de tráfego.
- **Não confiável-cliente-rede**: Operações na configuração de rede cliente não confiável.
- **Usuários**: Operações para visualizar e gerenciar usuários do Grid Manager.

A API de gerenciamento de grade usa o controle de versão para suportar atualizações sem interrupções.

Por exemplo, este URL de solicitação especifica a versão 4 da API.

`https://hostname_or_ip_address/api/v4/authorize`

A versão principal da API é quebrada quando alterações são feitas que são *não compatíveis* com versões mais antigas. A versão menor da API é quebrada quando alterações são feitas que *são compatíveis* com versões mais antigas. As alterações compatíveis incluem a adição de novos endpoints ou novas propriedades.

O exemplo a seguir ilustra como a versão da API é carregada com base no tipo de alterações feitas.

Tipo de alteração para API	Versão antiga	Nova versão
Compatível com versões mais antigas	2,1	2,2
Não compatível com versões mais antigas	2,1	3,0

Quando você instala o software StorageGRID pela primeira vez, apenas a versão mais recente da API é ativada. No entanto, quando você atualiza para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.

Pode configurar as versões suportadas. Consulte a seção **config** da documentação da API Swagger para "API de gerenciamento de grade"obter mais informações. Você deve desativar o suporte para a versão mais antiga depois de atualizar todos os clientes de API para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Deprecated: True"
- O corpo de resposta JSON inclui "obsoleto": True
- Um aviso obsoleto é adicionado ao nms.log. Por exemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determine quais versões de API são suportadas na versão atual

Use a `GET /versions` solicitação de API para retornar uma lista das principais versões da API suportada. Esta solicitação está localizada na seção **config** da documentação da API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especifique uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v4`) ou um cabeçalho (`Api-Version: 4`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Proteger contra falsificação de solicitação entre locais (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra StorageGRID usando tokens CSRF para melhorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes de API podem optar por ativá-lo quando fizerem login.

Um invasor que pode acionar uma solicitação para um site diferente (como um POST de formulário HTTP) pode fazer com que certas solicitações sejam feitas usando os cookies do usuário conetado.

O StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro específico DO corpo DO POST.

Para ativar a funcionalidade, defina o `csrfToken` parâmetro para `true` durante a autenticação. A predefinição é `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando verdadeiro, um `GridCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Grade, e o `AccountCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Tenant.

Se o cookie estiver presente, todas as solicitações que podem modificar o estado do sistema (POST, PUT, PATCH, DELETE) devem incluir um dos seguintes itens:

- O `X-Csrf-Token` cabeçalho, com o valor do cabeçalho definido para o valor do cookie de token CSRF.
- Para endpoints que aceitam um corpo codificado por formulário: Um `csrfToken` parâmetro corpo de solicitação codificado por formulário.

Consulte a documentação da API on-line para obter exemplos e detalhes adicionais.

> As solicitações que têm um conjunto de cookies de token CSRF também irão aplicar o cabeçalho "Content-Type: Application/json" para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

Use a API se o logon único estiver ativado

Use a API se o logon único estiver ativado (ative Directory)

Se você tiver "Logon único configurado e habilitado (SSO)" e usar o ative Directory como provedor SSO, deverá emitir uma série de solicitações de API para obter um token de autenticação válido para a API de Gerenciamento de Grade ou para a API de Gerenciamento do locatário.

Faça login na API se o logon único estiver ativado

Estas instruções se aplicam se você estiver usando o ative Directory como provedor de identidade SSO.

Antes de começar

- Você conhece o nome de usuário e a senha SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py` script Python, que está localizado no diretório de arquivos de instalação do StorageGRID (`./rpms`para Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho curl pode ter um tempo limite se você o executar muito lentamente. Você pode ver o erro: `A valid SubjectConfirmation was not found on this Response`.

  > O fluxo de trabalho cURL de exemplo não protege a senha de ser vista por outros usuários.

Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py` script Python. Avance para o passo 2.
   - Use solicitações curl. Avance para o passo 3.
2. Se você quiser usar o `storagegrid-ssoauth.py` script, passe o script para o interpretador Python e execute o script.

   Quando solicitado, insira valores para os seguintes argumentos:

   - O método SSO. Introduza ADFS ou adfs.
   - O nome de usuário SSO
   - O domínio onde o StorageGRID está instalado
   - O endereço para StorageGRID
   - O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.
3. Se você quiser usar solicitações curl, use o procedimento a seguir.
   a. Declare as variáveis necessárias para iniciar sessão.

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export SAMLDOMAIN='my-domain'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   export AD_FS_ADDRESS='adfs.example.com'
   ```

   > ⓘ Para acessar a API de gerenciamento de grade, use 0 como `TENANTACCOUNTID`.

   b. Para receber um URL de autenticação assinada, emita uma SOLICITAÇÃO POST para `/api/v3/authorize-saml`, e remova a codificação JSON adicional da resposta.

   Este exemplo mostra uma SOLICITAÇÃO POST para um URL de autenticação assinada para

`TENANTACCOUNTID`. Os resultados serão passados para `python -m json.tool` remover a codificação JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

A resposta para este exemplo inclui um URL assinado que é codificado por URL, mas não inclui a camada adicional de codificação JSON.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salve o `SAMLRequest` da resposta para uso em comandos subsequentes.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenha um URL completo que inclua o ID de solicitação do cliente do AD FS.

Uma opção é solicitar o formulário de login usando o URL da resposta anterior.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

A resposta inclui o ID de solicitação do cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salve o ID de solicitação do cliente da resposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envie suas credenciais para a ação de formulário da resposta anterior.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

O AD FS retorna um redirecionamento 302, com informações adicionais nos cabeçalhos.

> Se a autenticação multifator (MFA) estiver ativada para seu sistema SSO, o post de formulário também conterá a segunda senha ou outras credenciais.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salve o `MSISAuth` cookie da resposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envie uma SOLICITAÇÃO GET para o local especificado com os cookies do POST de autenticação.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Os cabeçalhos de resposta conterão informações de sessão do AD FS para uso posterior de logout e o corpo de resposta contém o SAMLResponse em um campo de formulário oculto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Salve o `SAMLResponse` do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Usando o `SAMLResponse` , faça uma solicitação StorageGRID`/api/saml-response` para gerar um token de autenticação StorageGRID.

Para `RelayState`, use o ID da conta do locatário ou use 0 se quiser entrar na API de gerenciamento de grade.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

A resposta inclui o token de autenticação.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salve o token de autenticação na resposta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Agora você pode usar `MYTOKEN` para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Saia da API se o logon único estiver ativado

Se o logon único (SSO) tiver sido ativado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatário. Estas instruções se aplicam se você estiver usando o ative Directory como provedor de identidade SSO

Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID fazendo logout da página de logout única da sua organização. Ou, você pode acionar o logout único (SLO) do StorageGRID, que requer um token válido do portador do StorageGRID.

Passos

1. Para gerar uma solicitação de logout assinada, passe "cookie "sso" para a API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Um URL de logout é retornado:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Salve o URL de logout.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para o StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

A resposta 302 é devolvida. O local de redirecionamento não é aplicável ao logout somente API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Exclua o token do portador do StorageGRID.

A exclusão do token portador do StorageGRID funciona da mesma forma que sem SSO. Se "cookie "sso" não for fornecido, o usuário será desconetado do StorageGRID sem afetar o estado SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

Uma `204 No Content` resposta indica que o usuário está desconetado agora.

```
HTTP/1.1 204 No Content
```

Use a API se o logon único estiver habilitado (Azure)

Se você tiver "Logon único configurado e habilitado (SSO)" e usar o Azure como provedor SSO, você pode usar dois scripts de exemplo para obter um token de autenticação válido para a API de Gerenciamento de Grade ou a API de Gerenciamento do locatário.

Inicie sessão na API se o início de sessão único do Azure estiver ativado

Estas instruções se aplicam se você estiver usando o Azure como provedor de identidade SSO

Antes de começar

- Você sabe o endereço de e-mail SSO e a senha de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar os seguintes scripts de exemplo:

- O `storagegrid-ssoauth-azure.py` script Python
- O `storagegrid-ssoauth-azure.js` script Node.js

Ambos os scripts estão localizados no diretório de arquivos de instalação do StorageGRID (`./rpms`para o Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian e `./vsphere` para VMware).

Para escrever sua própria integração com a API do Azure, consulte o `storagegrid-ssoauth-azure.py` script. O script Python faz duas solicitações diretamente ao StorageGRID (primeiro para obter o SAMLRequest e depois para obter o token de autorização), e também chama o script Node.js para interagir com o Azure para executar as operações SSO.

As operações SSO podem ser executadas usando uma série de solicitações de API, mas isso não é simples. O módulo Puppeteer Node.js é usado para raspar a interface SSO do Azure.

Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version`.

Passos

1. Instale as dependências necessárias, da seguinte forma:
   a. Instale o Node.js ("https://nodejs.org/en/download/"consulte).
   b. Instale os módulos Node.js necessários (puppeteer e jsdom):

      ```
      npm install -g <module>
      ```

2. Passe o script Python para o interpretador Python para executar o script.

   O script Python chamará então o script Node.js correspondente para executar as interações SSO do Azure.

3. Quando solicitado, insira valores para os seguintes argumentos (ou passe-os usando parâmetros):
   - O endereço de e-mail SSO usado para entrar no Azure
   - O endereço para StorageGRID

◦ O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário

4. Quando solicitado, insira a senha e esteja preparado para fornecer uma autorização de MFA ao Azure, se solicitado.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> O script assume que o MFA é feito usando o Microsoft Authenticator. Talvez seja necessário modificar o script para dar suporte a outras formas de MFA (como inserir um código recebido em uma mensagem de texto).

O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Use a API se o logon único estiver ativado (PingFederate)

Se você tem "Logon único configurado e habilitado (SSO)" e usa o PingFederate como provedor SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de Gerenciamento de Grade ou para a API de Gerenciamento do locatário.

Faça login na API se o logon único estiver ativado

Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

Antes de começar

- Você conhece o nome de usuário e a senha SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py` script Python, que está localizado no diretório de arquivos de instalação do StorageGRID (`./rpms`para Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho curl pode ter um tempo limite se você o executar muito lentamente. Você pode ver o erro: `A valid SubjectConfirmation was not found on this Response`.

  > O fluxo de trabalho cURL de exemplo não protege a senha de ser vista por outros usuários.

  Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py` script Python. Avance para o passo 2.
   - Use solicitações curl. Avance para o passo 3.
2. Se você quiser usar o `storagegrid-ssoauth.py` script, passe o script para o interpretador Python e execute o script.

   Quando solicitado, insira valores para os seguintes argumentos:

   - O método SSO. Você pode inserir qualquer variação de "pingfederate" (PINGFEDERATE, pingfederate, e assim por diante).
   - O nome de usuário SSO
   - O domínio onde o StorageGRID está instalado. Este campo não é usado para PingFederate. Você pode deixá-lo em branco ou inserir qualquer valor.
   - O endereço para StorageGRID
   - O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

3. Se você quiser usar solicitações curl, use o procedimento a seguir.

   a. Declare as variáveis necessárias para iniciar sessão.

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   ```

   > Para acessar a API de gerenciamento de grade, use 0 como `TENANTACCOUNTID`.

   b. Para receber um URL de autenticação assinada, emita uma SOLICITAÇÃO POST para `/api/v3/authorize-saml`, e remova a codificação JSON adicional da resposta.

   Este exemplo mostra uma SOLICITAÇÃO POST para uma URL de autenticação assinada para TENANTACCOUNTID. Os resultados serão passados para Python -m json.tool para remover a

codificação JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

A resposta para este exemplo inclui um URL assinado que é codificado por URL, mas não inclui a camada adicional de codificação JSON.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salve o `SAMLRequest` da resposta para uso em comandos subsequentes.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Exporte a resposta e o cookie e ecoe a resposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exporte o valor 'pf.adapterId' e ecoe a resposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporte o valor 'href' (remova a barra à direita /) e faça eco da resposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exportar o valor "ação":

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Enviar cookies juntamente com credenciais:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Salve o `SAMLResponse` do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Usando o `SAMLResponse` , faça uma solicitação StorageGRID`/api/saml-response` para gerar um token de autenticação StorageGRID.

Para `RelayState`, use o ID da conta do locatário ou use 0 se quiser entrar na API de gerenciamento de grade.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

A resposta inclui o token de autenticação.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salve o token de autenticação na resposta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Agora você pode usar `MYTOKEN` para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Saia da API se o logon único estiver ativado

Se o logon único (SSO) tiver sido ativado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatário. Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID fazendo logout da página de logout única da sua organização. Ou, você pode acionar o logout único (SLO) do StorageGRID, que requer um token válido do portador do StorageGRID.

Passos

1. Para gerar uma solicitação de logout assinada, passe "cookie "sso" para a API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Um URL de logout é retornado:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Salve o URL de logout.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para o StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

A resposta 302 é devolvida. O local de redirecionamento não é aplicável ao logout somente API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Exclua o token do portador do StorageGRID.

   A exclusão do token portador do StorageGRID funciona da mesma forma que sem SSO. Se "cookie "sso" não for fornecido, o usuário será desconetado do StorageGRID sem afetar o estado SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

   Uma `204 No Content` resposta indica que o usuário está desconetado agora.

```
HTTP/1.1 204 No Content
```

Desative recursos com a API

Você pode usar a API de gerenciamento de grade para desativar completamente certos recursos no sistema StorageGRID. Quando um recurso é desativado, ninguém pode receber permissões para executar as tarefas relacionadas a esse recurso.

Sobre esta tarefa

O sistema de funcionalidades desativadas permite-lhe impedir o acesso a determinadas funcionalidades no sistema StorageGRID. Desativar um recurso é a única maneira de impedir que o usuário root ou usuários que pertencem a grupos de administração com permissão **root Access** possam usar esse recurso.

Para entender como essa funcionalidade pode ser útil, considere o seguinte cenário:

A empresa A é um provedor de serviços que aluga a capacidade de armazenamento de seu sistema StorageGRID criando contas de inquilino. Para proteger a segurança dos objetos de seus arrendatários, a empresa A quer garantir que seus próprios funcionários nunca possam acessar qualquer conta de locatário depois que a conta tiver sido implantada.

*A empresa A pode atingir esse objetivo usando o sistema Deactivate Features na API Grid Management. Ao desativar completamente o recurso **alterar senha de root do locatário** no Gerenciador de Grade (tanto a UI quanto a API), a empresa A garante que os usuários Admin - incluindo o usuário raiz e os usuários pertencentes a grupos com a permissão **root Access** - não podem alterar a senha para o usuário root de*

qualquer conta de locatário.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade. "Use a API de gerenciamento de grade"Consulte .
2. Localize o endpoint Deactivate Features
3. Para desativar um recurso, como alterar a senha de root do locatário, envie um corpo para a API assim:

```
{ "grid": {"changeTenantRootPassword": true} }
```

Quando a solicitação estiver concluída, o recurso alterar senha raiz do locatário é desativado. A permissão de gerenciamento * alterar senha de root do locatário * não aparece mais na interface do usuário, e qualquer solicitação de API que tente alterar a senha de raiz de um locatário falhará com "403 Forbidden".

Reativar funcionalidades desativadas

Por padrão, você pode usar a API de Gerenciamento de Grade para reativar um recurso que foi desativado. No entanto, se você quiser impedir que os recursos desativados sejam reativados, você pode desativar o próprio recurso **activateFeatures**.

O recurso **activateFeatures** não pode ser reativado. Se você decidir desativar esse recurso, esteja ciente de que você perderá permanentemente a capacidade de reativar quaisquer outros recursos desativados. Você deve entrar em Contato com o suporte técnico para restaurar qualquer funcionalidade perdida.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade.
2. Localize o endpoint Deactivate Features
3. Para reativar todos os recursos, envie um corpo para a API assim:

```
{ "grid": null }
```

Quando essa solicitação estiver concluída, todos os recursos, incluindo o recurso alterar senha de root do locatário, são reativados. A permissão de gerenciamento **alterar senha de root do locatário** agora aparece na interface do usuário, e qualquer solicitação de API que tente alterar a senha de root de um locatário terá êxito, assumindo que o usuário tenha a permissão de gerenciamento **acesso root** ou **alterar senha de root do locatário**.

O exemplo anterior faz com que os recursos *All* desativados sejam reativados. Se outros recursos tiverem sido desativados que devem permanecer desativados, você deverá especificá-los explicitamente na SOLICITAÇÃO PUT. Por exemplo, para reativar o recurso alterar senha de root do locatário e continuar a desativar a permissão de gerenciamento do storageAdmin, envie esta SOLICITAÇÃO DE COMPRA

```
{ "grid": {"storageAdmin": true} }
```

Controle o acesso ao StorageGRID

Controle o acesso à StorageGRID

Você controla quem pode acessar o StorageGRID e quais tarefas os usuários podem executar criando ou importando grupos e usuários e atribuindo permissões a cada grupo. Opcionalmente, você pode ativar o logon único (SSO), criar certificados de cliente e alterar senhas de grade.

Controle o acesso ao Gerenciador de Grade

Você determina quem pode acessar o Gerenciador de Grade e a API de Gerenciamento de Grade importando grupos e usuários de um serviço de federação de identidade ou configurando grupos locais e usuários locais.

O uso do "federação de identidade" torna a configuração "grupos" "usuários"mais rápida e permite que os usuários façam login no StorageGRID usando credenciais familiares. Você pode configurar a federação de identidade se usar o ative Directory, OpenLDAP ou Oracle Directory Server.

> Contacte o suporte técnico se pretender utilizar outro serviço LDAP v3.

Você determina quais tarefas cada usuário pode executar atribuindo diferentes "permissões" a cada grupo. Por exemplo, você pode querer que os usuários de um grupo possam gerenciar regras ILM e usuários de outro grupo para executar tarefas de manutenção. Um usuário deve pertencer a pelo menos um grupo para acessar o sistema.

Opcionalmente, você pode configurar um grupo para ser somente leitura. Os usuários em um grupo somente leitura só podem exibir configurações e recursos. Eles não podem fazer alterações ou executar quaisquer operações no Gerenciador de Grade ou na API de Gerenciamento de Grade.

Ative o logon único

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0). Depois de "Configurar e ativar SSO"você , todos os usuários devem ser autenticados por um provedor de identidade externo antes que possam acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de Gerenciamento de Grade ou a API de Gerenciamento de Locatário. Os usuários locais não podem entrar no StorageGRID.

Alterar a frase-passe do aprovisionamento

A senha de provisionamento é necessária para muitos procedimentos de instalação e manutenção e para baixar o Pacote de recuperação do StorageGRID. A senha também é necessária para fazer o download de backups das informações de topologia de grade e chaves de criptografia para o sistema StorageGRID. Você pode "altere a frase-passe"como necessário.

Altere as senhas do console do nó

Cada nó na sua grade tem uma senha exclusiva do console de nó, que você precisa fazer login no nó como "admin" usando SSH, ou para o usuário root em uma conexão VM/console físico. Conforme necessário, você pode "altere a senha do console do nó" para cada nó.

Altere a frase-passe de aprovisionamento

Use este procedimento para alterar a senha de provisionamento do StorageGRID. A frase-passe é necessária para procedimentos de recuperação, expansão e manutenção. A senha também é necessária para baixar backups do pacote de recuperação que

incluem informações de topologia de grade, senhas de console de nó de grade e chaves de criptografia para o sistema StorageGRID.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de Manutenção ou Acesso root.
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

A frase-passe de aprovisionamento é necessária para muitos procedimentos de instalação e manutenção, e para "Transferir o pacote de recuperação"o . A senha de provisionamento não está listada no `Passwords.txt` arquivo. Certifique-se de documentar a senha de provisionamento e mantê-la em um local seguro e seguro.

Passos

1. Selecione **CONFIGURATION** > **access control**> **Grid passwords**.
2. Em **alterar senha de provisionamento**, selecione **fazer uma alteração**
3. Introduza a sua frase-passe de aprovisionamento atual.
4. Introduza a nova frase-passe. A frase-passe deve conter pelo menos 8 e não mais de 32 carateres. As senhas são sensíveis a maiúsculas e minúsculas.
5. Armazene a nova senha de provisionamento em um local seguro. É necessário para procedimentos de instalação, expansão e manutenção.
6. Digite novamente a nova senha e selecione **Salvar**.

   O sistema exibe um banner verde de sucesso quando a alteração da senha de provisionamento estiver concluída.

7. Selecione **Pacote de recuperação**.
8. Insira a nova senha de provisionamento para baixar o novo Pacote de recuperação.

   Depois de alterar a senha de provisionamento, você deve baixar imediatamente um novo Pacote de recuperação. O arquivo do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.

Altere as senhas do console do nó

Cada nó na sua grade tem uma senha exclusiva do console de nó, que você precisa fazer login no nó. Use estas etapas para alterar cada senha exclusiva do console de nó para cada nó na grade.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

Use a senha do console do nó para fazer login em um nó como "admin" usando SSH, ou para o usuário raiz em uma conexão VM/console físico. O processo de alteração de senha do console do nó cria novas senhas para cada nó na grade e armazena as senhas em um arquivo atualizado `Passwords.txt` no Pacote de recuperação. As senhas são listadas na coluna Senha no arquivo Passwords.txt.

> Existem senhas de acesso SSH separadas para as chaves SSH usadas para comunicação entre nós. As senhas de acesso SSH não são alteradas por este procedimento.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Access control** > **Grid passwords**.
2. Em **alterar senhas de console de nó**, selecione **fazer uma alteração**.

Introduza a frase-passe de aprovisionamento

Passos

1. Introduza a frase-passe de aprovisionamento da grelha.
2. Selecione **continuar**.

Baixe o pacote de recuperação atual

Antes de alterar as senhas do console do nó, baixe o Pacote de recuperação atual. Você pode usar as senhas neste arquivo se o processo de alteração de senha falhar em qualquer nó.

Passos

1. Selecione **Baixar pacote de recuperação**.
2. Copie o arquivo do pacote de recuperação (`.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.

3. Selecione **continuar**.
4. Quando a caixa de diálogo de confirmação for exibida, selecione **Sim** se estiver pronto para começar a alterar as senhas do console do nó.

   Não é possível cancelar este processo após o início.

Altere as senhas do console do nó

Quando o processo de senha do console do nó é iniciado, um novo Pacote de recuperação é gerado que inclui as novas senhas. Em seguida, as senhas são atualizadas em cada nó.

Passos

1. Aguarde que o novo pacote de recuperação seja gerado, o que pode levar alguns minutos.
2. Selecione **Transferir novo pacote de recuperação**.
3. Quando o download for concluído:

a. Abra o `.zip` ficheiro.

b. Confirme se você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo, que contém as novas senhas do console do nó.

c. Copie o novo arquivo do pacote de recuperação (`.zip`) para dois locais seguros, seguros e separados.

> Não substitua o pacote de recuperação antigo.

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.

4. Marque a caixa de seleção para indicar que você baixou o novo Pacote de recuperação e verificou o conteúdo.
5. Selecione **alterar senhas do console de nós** e aguarde que todos os nós sejam atualizados com as novas senhas. Isso pode levar alguns minutos.

   Se as senhas forem alteradas para todos os nós, um banner verde de sucesso será exibido. Vá para a próxima etapa.

   Se houver um erro durante o processo de atualização, uma mensagem de banner lista o número de nós que não conseguiram alterar suas senhas. O sistema irá tentar novamente automaticamente o processo em qualquer nó que não tenha a sua palavra-passe alterada. Se o processo terminar com alguns nós ainda não tendo uma senha alterada, o botão **Repetir** será exibido.

   Se a atualização da palavra-passe tiver falhado para um ou mais nós:

   a. Reveja as mensagens de erro listadas na tabela.

   b. Resolva os problemas.

   c. Selecione **Repetir**.

   > A tentativa de novo altera apenas as senhas do console do nó nos nós que falharam durante tentativas anteriores de alteração de senha.

6. Depois que as senhas do console do nó tiverem sido alteradas para todos os nós, exclua o Primeiro pacote de recuperação que você baixou.
7. Opcionalmente, use o link **Recovery package** para baixar uma cópia adicional do novo Recovery Package.

Alterar senhas de acesso SSH para nós de administrador

Alterar as senhas de acesso SSH para nós de administrador também atualiza os conjuntos exclusivos de chaves SSH internas para cada nó na grade. O nó Admin principal usa essas chaves SSH para acessar nós usando autenticação segura e sem senha.

Use uma chave SSH para fazer login em um nó como `admin` ou para o usuário raiz em uma VM ou conexão de console físico.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

As novas senhas de acesso para nós de administração e as novas chaves internas para cada nó são armazenadas `Passwords.txt` no arquivo no Pacote de recuperação. As chaves são listadas na coluna Senha nesse arquivo.

Existem senhas de acesso SSH separadas para as chaves SSH usadas para comunicação entre nós. Estes não são alterados por este procedimento.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Access control** > **Grid passwords**.
2. Em **alterar chaves SSH**, selecione **fazer uma alteração**.

Baixe o pacote de recuperação atual

Antes de alterar as chaves de acesso SSH, faça o download do Pacote de recuperação atual. Você pode usar as chaves neste arquivo se o processo de mudança de chave falhar para qualquer nó.

Passos

1. Introduza a frase-passe de aprovisionamento da grelha.
2. Selecione **Baixar pacote de recuperação**.
3. Copie o arquivo do pacote de recuperação (`.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.

4. Selecione **continuar**.
5. Quando a caixa de diálogo de confirmação for exibida, selecione **Sim** se estiver pronto para começar a alterar as chaves de acesso SSH.

> Não é possível cancelar este processo após o início.

Alterar chaves de acesso SSH

Quando o processo alterar chaves de acesso SSH é iniciado, um novo Pacote de recuperação é gerado que inclui as novas chaves. Em seguida, as chaves são atualizadas em cada nó.

Passos

1. Aguarde que o novo pacote de recuperação seja gerado, o que pode levar alguns minutos.
2. Quando o botão Transferir novo pacote de recuperação estiver ativado, selecione **Transferir novo pacote de recuperação** e guarde o novo ficheiro do pacote de recuperação (`.zip`) em dois locais seguros, seguros e separados.
3. Quando o download for concluído:

a. Abra o `.zip` ficheiro.

b. Confirme que você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo, que contém as novas chaves de acesso SSH.

c. Copie o novo arquivo do pacote de recuperação (`.zip`) para dois locais seguros, seguros e separados.

> ⚠ Não substitua o pacote de recuperação antigo.

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.

4. Aguarde que as chaves sejam atualizadas em cada nó, o que pode levar alguns minutos.

   Se as chaves forem alteradas para todos os nós, um banner verde de sucesso será exibido.

   Se houver um erro durante o processo de atualização, uma mensagem de banner lista o número de nós que não conseguiram alterar suas chaves. O sistema tentará automaticamente o processo em qualquer nó que não tenha sua chave alterada. Se o processo terminar com alguns nós ainda não tendo uma chave alterada, o botão **Repetir** será exibido.

   Se a atualização da chave falhar para um ou mais nós:

   a. Reveja as mensagens de erro listadas na tabela.

   b. Resolva os problemas.

   c. Selecione **Repetir**.

      Tentar novamente altera apenas as chaves de acesso SSH nos nós que falharam durante tentativas anteriores de alteração de chave.

5. Depois que as chaves de acesso SSH tiverem sido alteradas para todos os nós, exclua o Primeiro pacote de recuperação que você baixou.

6. Opcionalmente, selecione **MAINTENANCE** > **System** > **Recovery package** para transferir uma cópia adicional do novo Recovery Package.

Use a federação de identidade

O uso da federação de identidade torna a configuração de grupos e usuários mais rápida e permite que os usuários façam login no StorageGRID usando credenciais familiares.

Configure a federação de identidade para o Grid Manager

Você pode configurar a federação de identidade no Gerenciador de Grade se quiser que os grupos de administração e usuários sejam gerenciados em outro sistema, como ative Directory, Azure ative Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você está usando o ative Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.

Se pretender utilizar um serviço LDAP v3 que não esteja listado, contacte o suporte técnico.

- Se você pretende usar o OpenLDAP, você deve configurar o servidor OpenLDAP. Diretrizes para configurar um servidor OpenLDAPConsulte .
- Se você planeja habilitar o logon único (SSO), revisou o "requisitos e considerações para logon único".
- Se você planeja usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade está usando TLS 1,2 ou 1,3. "Cifras suportadas para conexões TLS de saída"Consulte .

Sobre esta tarefa

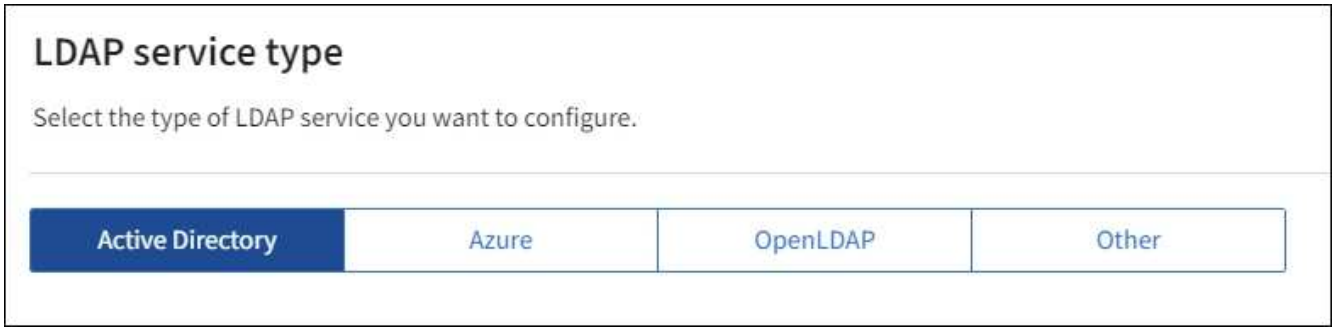
Você pode configurar uma fonte de identidade para o Gerenciador de Grade se quiser importar grupos de outro sistema, como ative Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Você pode importar os seguintes tipos de grupos:

- Grupos de administração. Os usuários nos grupos de administração podem entrar no Gerenciador de Grade e executar tarefas, com base nas permissões de gerenciamento atribuídas ao grupo.
- Grupos de usuários de locatários que não usam sua própria fonte de identidade. Os usuários em grupos de inquilinos podem entrar no Gerenciador de inquilinos e executar tarefas, com base nas permissões atribuídas ao grupo no Gerenciador de inquilinos. "Crie uma conta de locatário"Consulte e "Use uma conta de locatário" para obter detalhes.

Introduza a configuração

Passos

1. Selecione **CONFIGURATION** > **access control** > **Identity Federation**.
2. Selecione **Ativar federação de identidade**.
3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.



Selecione **Other** para configurar valores para um servidor LDAP que use o Oracle Directory Server.

4. Se você selecionou **Other**, preencha os campos na seção atributos LDAP. Caso contrário, vá para a próxima etapa.
   - **Nome exclusivo do usuário**: O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `uid` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `uid`.
   - **UUID de usuário**: O nome do atributo que contém o identificador exclusivo permanente de um usuário LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.

- **Group Unique Name**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `cn` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `cn`.
- **Group UUID**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.

5. Para todos os tipos de serviço LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias na secção Configurar servidor LDAP.
   - **Nome de host**: O nome de domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
   - **Port**: A porta usada para se conetar ao servidor LDAP.

     > A porta padrão para STARTTLS é 389 e a porta padrão para LDAPS é 636. No entanto, você pode usar qualquer porta desde que seu firewall esteja configurado corretamente.

   - **Nome de usuário**: O caminho completo do nome distinto (DN) para o usuário que se conetará ao servidor LDAP.

     No ative Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

     O usuário especificado deve ter permissão para listar grupos e usuários e para acessar os seguintes atributos:

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`
     - `cn`
     - `memberOf` ou `isMemberOf`
     - **Ative Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, E `userPrincipalName`
     - **Azure**: `accountEnabled` E. `userPrincipalName`

   - **Senha**: A senha associada ao nome de usuário.

     > Se você alterar a senha no futuro, você deve atualizá-la nesta página.

   - **Group base DN**: O caminho completo do nome distinto (DN) para uma subárvore LDAP que você deseja pesquisar grupos. No exemplo do ative Directory (abaixo), todos os grupos cujo Nome distinto é relativo ao DN base (DC-StorageGRID,DC-com) podem ser usados como grupos federados.

     > Os valores **Group unique name** devem ser exclusivos dentro do **Group base DN** a que pertencem.

   - **DN da base do usuário**: O caminho completo do nome distinto (DN) de uma subárvore LDAP que você deseja pesquisar por usuários.

> Os valores **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN da base de usuários** a que pertencem.

- **Bind username format** (opcional): O padrão de username padrão StorageGRID deve ser usado se o padrão não puder ser determinado automaticamente.

  É recomendado fornecer **Bind username format** porque pode permitir que os usuários façam login se o StorageGRID não conseguir vincular-se à conta de serviço.

  Introduza um destes padrões:

  - **Padrão UserPrincipalName (ative Directory e Azure)**: `[USERNAME]@example.com`
  - * Padrão de nome de logon de nível inferior (ative Directory e Azure)*: `example\[USERNAME]`
  - * Padrão de nome distinto *: `CN=[USERNAME],CN=Users,DC=example,DC=com`

    Inclua **[USERNAME]** exatamente como escrito.

6. Na seção Transport Layer Security (TLS), selecione uma configuração de segurança.
   - **Use STARTTLS**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para ative Directory, OpenLDAP ou outro, mas esta opção não é suportada para o Azure.
   - **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar essa opção para o Azure.
   - **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido. Esta opção não é suportada para o Azure.

     > O uso da opção **não usar TLS** não é suportado se o servidor do ative Directory forçar a assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

7. Se você selecionou STARTTLS ou LDAPS, escolha o certificado usado para proteger a conexão.
   - **Use o certificado CA do sistema operacional**: Use o certificado CA de grade padrão instalado no sistema operacional para proteger conexões.
   - **Use certificado CA personalizado**: Use um certificado de segurança personalizado.

     Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

Teste a conexão e salve a configuração

Depois de introduzir todos os valores, tem de testar a ligação antes de poder guardar a configuração. O StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato de nome de usuário de vinculação, se você tiver fornecido uma.

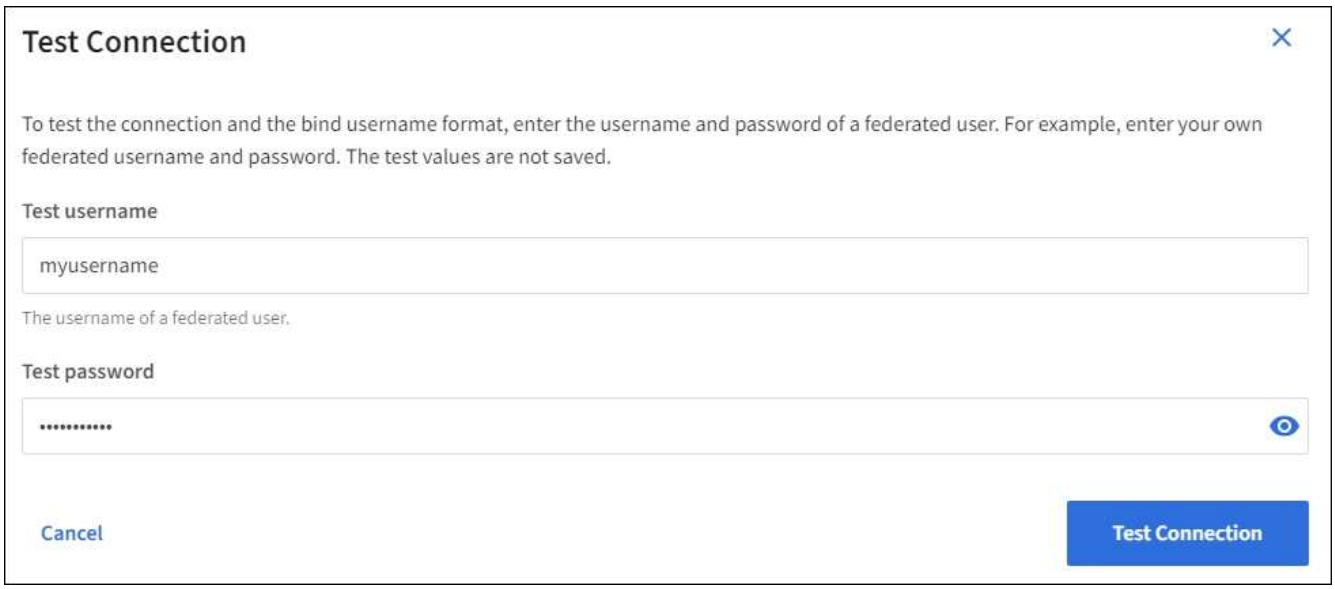
Passos

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
   - É apresentada uma mensagem "Test Connection successful" (testar ligação bem-sucedida) se as definições de ligação forem válidas. Selecione **Save** (Guardar) para guardar a configuração.

- É apresentada uma mensagem "não foi possível estabelecer ligação de teste" se as definições da ligação forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.

3. Se você tiver fornecido um formato de nome de usuário do BIND, insira o nome de usuário e a senha de um usuário federado válido.

   Por exemplo, insira seu próprio nome de usuário e senha. Não inclua carateres especiais no nome de usuário, como em ou /.



   - É apresentada uma mensagem "Test Connection successful" (testar ligação bem-sucedida) se as definições de ligação forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem de erro é exibida se as configurações de conexão, o formato de nome de usuário de ligação ou o nome de usuário de teste e a senha forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar a sincronização com a fonte de identidade

O sistema StorageGRID sincroniza periodicamente grupos federados e usuários da origem da identidade. Você pode forçar o início da sincronização se quiser ativar ou restringir as permissões de usuário o mais rápido possível.

Passos

1. Vá para a página de federação de identidade.
2. Selecione **servidor de sincronização** na parte superior da página.

   O processo de sincronização pode demorar algum tempo, dependendo do ambiente.

   O alerta **Falha na sincronização da federação de identidade** é acionado se houver um problema na sincronização de grupos federados e usuários da origem da identidade.

Desativar a federação de identidade

Você pode desativar temporariamente ou permanentemente a federação de identidade para grupos e usuários. Quando a federação de identidade está desativada, não há comunicação entre o StorageGRID e a

fonte de identidade. No entanto, todas as configurações que você configurou são mantidas, permitindo que você reative facilmente a federação de identidade no futuro.

Sobre esta tarefa

Antes de desativar a federação de identidade, você deve estar ciente do seguinte:

- Os utilizadores federados não poderão iniciar sessão.
- Os usuários federados que estiverem conetados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a origem da identidade não ocorrerá e os alertas não serão gerados para contas que não tenham sido sincronizadas.
- A caixa de seleção **Ativar federação de identidade** será desativada se o logon único (SSO) estiver definido como **ativado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. "Desative o logon único"Consulte .

Passos

1. Vá para a página de federação de identidade.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.

Diretrizes para configurar um servidor OpenLDAP

Se você quiser usar um servidor OpenLDAP para federação de identidade, você deve configurar configurações específicas no servidor OpenLDAP.

> Para fontes de identidade que não são ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso S3 aos usuários que estão desativados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 para o usuário ou remova o usuário de todos os grupos.

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para a manutenção da associação de grupo reverso no "Documentação do OpenLDAP: Guia do administrador da versão 2,4".

Indexação

Você deve configurar os seguintes atributos OpenLDAP com as palavras-chave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Além disso, certifique-se de que os campos mencionados na ajuda do Nome de usuário sejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção da associação de grupo reverso no "Documentação do OpenLDAP: Guia do administrador da versão 2,4".

Gerenciar grupos de administradores

Você pode criar grupos de administração para gerenciar as permissões de segurança para um ou mais usuários de administração. Os usuários devem pertencer a um grupo para ter acesso ao sistema StorageGRID.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Crie um grupo de administração

Os grupos de administração permitem determinar quais usuários podem acessar quais recursos e operações no Gerenciador de Grade e na API de Gerenciamento de Grade.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Access Control** > **Admin Groups**.
2. Selecione **criar grupo**.

Escolha um tipo de grupo

Você pode criar um grupo local ou importar um grupo federado.

- Crie um grupo local se quiser atribuir permissões a usuários locais.
- Crie um grupo federado para importar usuários da origem da identidade.

Grupo local

Passos

1. Selecione **local group**.
2. Introduza um nome de apresentação para o grupo, que pode atualizar posteriormente, conforme necessário. Por exemplo, "usuários de manutenção" ou "Administradores de ILM".
3. Introduza um nome exclusivo para o grupo, que não pode atualizar mais tarde.
4. Selecione **continuar**.

Grupo federado

Passos

1. Selecione **Federated Group**.
2. Introduza o nome do grupo que pretende importar, exatamente como aparece na origem de identidade configurada.
   - Para o ative Directory e Azure, use o sAMAccountName.
   - Para OpenLDAP, use o CN (Nome Comum).
   - Para outro LDAP, use o nome exclusivo apropriado para o servidor LDAP.
3. Selecione **continuar**.

Gerenciar permissões de grupo

Passos

1. Para **modo de acesso**, selecione se os usuários do grupo podem alterar as configurações e executar operações no Gerenciador de Grade e na API de Gerenciamento de Grade ou se eles só podem exibir configurações e recursos.
   - **Leitura-escrita** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar quaisquer operações no Gerenciador de Grade ou na API de Gerenciamento de Grade. Os usuários locais só de leitura podem alterar suas próprias senhas.

   > Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

2. Selecione um ou mais "permissões do grupo de administração".

   Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes ao grupo não poderão entrar no StorageGRID.

3. Se estiver criando um grupo local, selecione **continuar**. Se você estiver criando um grupo federado, selecione **criar grupo** e **concluir**.

Adicionar utilizadores (apenas grupos locais)

Passos

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.

Se ainda não tiver criado utilizadores locais, pode guardar o grupo sem adicionar utilizadores. Pode adicionar este grupo ao utilizador na página utilizadores. "Gerenciar usuários"Consulte para obter detalhes.

2. Selecione **criar grupo** e **concluir**.

Exibir e editar grupos de administração

Você pode exibir detalhes de grupos existentes, modificar um grupo ou duplicar um grupo.

- Para exibir informações básicas de todos os grupos, revise a tabela na página grupos.
- Para exibir todos os detalhes de um grupo específico ou editar um grupo, use o menu **ações** ou a página de detalhes.

Tarefa	Menu ações	Página de detalhes
Ver detalhes do grupo	a. Selecione a caixa de verificação para o grupo. b. Selecione **ações** > **Exibir detalhes do grupo**.	Selecione o nome do grupo na tabela.
Editar nome de exibição (apenas grupos locais)	a. Selecione a caixa de verificação para o grupo. b. Selecione **ações** > **Editar nome do grupo**. c. Introduza o novo nome. d. Selecione **Salvar alterações**.	a. Selecione o nome do grupo para exibir os detalhes. b. Selecione o ícone de edição . c. Introduza o novo nome. d. Selecione **Salvar alterações**.
Editar o modo de acesso ou permissões	a. Selecione a caixa de verificação para o grupo. b. Selecione **ações** > **Exibir detalhes do grupo**. c. Opcionalmente, altere o modo de acesso do grupo. d. Opcionalmente, selecione ou "permissões do grupo de administração"desmarque . e. Selecione **Salvar alterações**.	a. Selecione o nome do grupo para exibir os detalhes. b. Opcionalmente, altere o modo de acesso do grupo. c. Opcionalmente, selecione ou "permissões do grupo de administração"desmarque . d. Selecione **Salvar alterações**.

Duplicar um grupo

Passos

1. Selecione a caixa de verificação para o grupo.
2. Selecione **ações** > **grupo duplicado**.
3. Conclua o assistente de grupo duplicado.

Eliminar um grupo

Você pode excluir um grupo de administração quando quiser remover o grupo do sistema e remover todas as permissões associadas ao grupo. A exclusão de um grupo de administração remove todos os usuários do grupo, mas não exclui os usuários.

Passos

1. Na página grupos, marque a caixa de seleção para cada grupo que deseja remover.
2. Selecione **ações** > **Excluir grupo**.
3. Selecione **Excluir grupos**.

Permissões do grupo de administração

Ao criar grupos de usuários admin, você seleciona uma ou mais permissões para controlar o acesso a recursos específicos do Gerenciador de Grade. Em seguida, você pode atribuir cada usuário a um ou mais desses grupos de administração para determinar quais tarefas o usuário pode executar.

Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes a esse grupo não poderão entrar no Gerenciador de Grade ou na API de Gerenciamento de Grade.

Por padrão, qualquer usuário que pertença a um grupo que tenha pelo menos uma permissão pode executar as seguintes tarefas:

- Faça login no Gerenciador de Grade
- Visualizar o painel de instrumentos
- Exibir as páginas de nós
- Ver alertas atuais e resolvidos
- Alterar sua própria senha (somente usuários locais)
- Visualize determinadas informações fornecidas nas páginas Configuração e Manutenção

Interação entre permissões e modo de acesso

Para todas as permissões, a configuração **modo de acesso** do grupo determina se os usuários podem alterar configurações e executar operações ou se eles podem exibir somente as configurações e recursos relacionados. Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

As seções a seguir descrevem as permissões que você pode atribuir ao criar ou editar um grupo de administradores. Qualquer funcionalidade não mencionada explicitamente requer a permissão **Root Access**.

Acesso à raiz

Essa permissão fornece acesso a todos os recursos de administração de grade.

Altere a senha raiz do locatário

Essa permissão fornece acesso à opção **alterar senha de root** na página de locatários, permitindo que você controle quem pode alterar a senha para o usuário raiz local do locatário. Essa permissão também é usada para migrar chaves S3 quando o recurso de importação de chaves S3 estiver ativado. Os usuários que não têm essa permissão não podem ver a opção **alterar senha de root**.

Para conceder acesso à página de locatários, que contém a opção **alterar senha de root**, atribua também a permissão **Contas de locatário**.

Configuração da página de topologia de grade

Esta permissão fornece acesso às guias Configuração na página **SUPPORT** > **Tools** > **Grid topology**.

A página de topologia de Grade foi obsoleta e será removida em uma versão futura.

ILM

Esta permissão fornece acesso às seguintes opções de menu **ILM**:

- Regras
- Políticas
- Etiquetas de política
- Pools de armazenamento
- Classes de armazenamento
- Regiões
- Pesquisa de metadados de objetos

Os usuários devem ter as permissões **outras configurações de grade** e **Configuração de página de topologia de grade** para gerenciar as notas de armazenamento.

Manutenção

Os usuários devem ter a permissão Manutenção para usar estas opções:

- **CONFIGURAÇÃO** > **controlo de acesso**:
  - Senhas de grade
- **CONFIGURAÇÃO** > **rede**:
  - S3 nomes de domínio de endpoint
- **MANUTENÇÃO** > **tarefas**:
  - Descomissionar
  - Expansão
  - Verificação de existência do objeto
  - Recuperação
- **MANUTENÇÃO** > **sistema**:
  - Pacote de recuperação
  - Atualização de software
- **SUPORTE** > **Ferramentas**:
  - Registos

Os usuários que não têm a permissão Manutenção podem visualizar, mas não editar, estas páginas:

- **MANUTENÇÃO** > **rede**:
  - Servidores DNS
  - Rede de rede
  - Servidores NTP
- **MANUTENÇÃO** > **sistema**:
  - Licença
- **CONFIGURAÇÃO** > **rede**:
  - S3 nomes de domínio de endpoint
- **CONFIGURAÇÃO** > **Segurança**:
  - Certificados
- **CONFIGURAÇÃO** > **Monitoramento**:
  - Servidor de auditoria e syslog

Gerenciar alertas

Essa permissão fornece acesso a opções de gerenciamento de alertas. Os usuários devem ter essa permissão para gerenciar silêncios, notificações de alerta e regras de alerta.

Consulta de métricas

Esta permissão fornece acesso a:

- **SUPORTE** > **Ferramentas** > **métricas** página
- Consultas de métricas personalizadas do Prometheus usando a seção **Metrics** da API Grid Management
- Cartões de painel do Grid Manager que contêm métricas

Pesquisa de metadados de objetos

Esta permissão fornece acesso à página **ILM** > **Object metadata lookup**.

Outra configuração de grade

Esta permissão fornece acesso a opções de configuração de grade adicionais.

> Para ver essas opções adicionais, os usuários também devem ter a permissão **Grid topology page Configuration**.

- **ILM**:
  - Classes de armazenamento
- **CONFIGURAÇÃO** > **sistema**:
- **SUPORTE** > **outro**:
  - Custo da ligação

Administrador do dispositivo de storage

Esta permissão fornece:

- Acesso ao Gerenciador de sistemas e-Series SANtricity em dispositivos de storage por meio do Gerenciador de Grade.
- Capacidade de executar tarefas de solução de problemas e manutenção na guia Gerenciar unidades para dispositivos que suportam essas operações.

Contas de inquilino

Essa permissão permite:

- Acesse a página de locatários, onde você pode criar, editar e remover contas de locatários
- Ver políticas de classificação de tráfego existentes
- Exibir cartões de painel do Grid Manager que contêm detalhes do locatário

Gerenciar usuários

Você pode exibir usuários locais e federados. Você também pode criar usuários locais e atribuí-los a grupos de administração locais para determinar quais recursos do Gerenciador de Grade esses usuários podem acessar.

Antes de começar

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

Crie um usuário local

Você pode criar um ou mais usuários locais e atribuir cada usuário a um ou mais grupos locais. As permissões do grupo controlam quais recursos do Gerenciador de Grade e da API de Gerenciamento de Grade o usuário pode acessar.

Você pode criar somente usuários locais. Use a fonte de identidade externa para gerenciar usuários e grupos federados.

O Gerenciador de Grade inclui um usuário local predefinido, chamado "root". Não é possível remover o usuário raiz.

> Se o logon único (SSO) estiver ativado, os usuários locais não poderão fazer login no StorageGRID.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Access Control** > **Admin Users**.
2. Selecione **criar usuário**.

Introduza as credenciais do utilizador

Passos

1. Introduza o nome completo do utilizador, um nome de utilizador exclusivo e uma palavra-passe.
2. Opcionalmente, selecione **Sim** se esse usuário não tiver acesso ao Gerenciador de Grade ou à API de Gerenciamento de Grade.

3. Selecione **continuar**.

Atribuir a grupos

Passos

1. Opcionalmente, atribua o usuário a um ou mais grupos para determinar as permissões do usuário.

   Se ainda não tiver criado grupos, pode guardar o utilizador sem selecionar grupos. Você pode adicionar esse usuário a um grupo na página grupos.

   Se um usuário pertencer a vários grupos, as permissões serão cumulativas. "Gerenciar grupos de administradores"Consulte para obter detalhes.

2. Selecione **Create user** e selecione **Finish**.

Ver e editar utilizadores locais

Você pode exibir detalhes de usuários locais e federados existentes. Você pode modificar um usuário local para alterar o nome completo, a senha ou a associação de grupo do usuário. Você também pode impedir temporariamente que um usuário acesse o Gerenciador de Grade e a API de Gerenciamento de Grade.

Só pode editar utilizadores locais. Use a fonte de identidade externa para gerenciar usuários federados.

- Para exibir informações básicas para todos os usuários locais e federados, revise a tabela na página usuários.
- Para visualizar todos os detalhes de um usuário específico, editar um usuário local ou alterar a senha de um usuário local, use o menu **ações** ou a página de detalhes.

  Todas as edições são aplicadas na próxima vez que o usuário sair e, em seguida, voltar a entrar no Gerenciador de Grade.

  Os usuários locais podem alterar suas próprias senhas usando a opção **alterar senha** no banner do Gerenciador de Grade.

Tarefa	Menu ações	Página de detalhes
Ver detalhes do utilizador	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**.	Selecione o nome do usuário na tabela.
Editar nome completo (somente usuários locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Editar nome completo**. c. Introduza o novo nome. d. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione o ícone de edição . c. Introduza o novo nome. d. Selecione **Salvar alterações**.

Tarefa	Menu ações	Página de detalhes
Negar ou permitir acesso à StorageGRID	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia Acesso. d. Selecione **Sim** para impedir que o usuário faça login no Gerenciador de Grade ou na API de Gerenciamento de Grade, ou selecione **não** para permitir que o usuário faça login. e. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Acesso. c. Selecione **Sim** para impedir que o usuário faça login no Gerenciador de Grade ou na API de Gerenciamento de Grade, ou selecione **não** para permitir que o usuário faça login. d. Selecione **Salvar alterações**.
Alterar palavra-passe (apenas utilizadores locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia Senha. d. Introduza uma nova palavra-passe. e. Selecione **alterar palavra-passe**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Senha. c. Introduza uma nova palavra-passe. d. Selecione **alterar palavra-passe**.
Alterar grupos (somente usuários locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia grupos. d. Opcionalmente, selecione o link após um nome de grupo para exibir os detalhes do grupo em uma nova guia do navegador. e. Selecione **Editar grupos** para selecionar grupos diferentes. f. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia grupos. c. Opcionalmente, selecione o link após um nome de grupo para exibir os detalhes do grupo em uma nova guia do navegador. d. Selecione **Editar grupos** para selecionar grupos diferentes. e. Selecione **Salvar alterações**.

Duplicar um usuário

Você pode duplicar um usuário existente para criar um novo usuário com as mesmas permissões.

Passos

1. Selecione a caixa de verificação para o utilizador.
2. Selecione **ações** > **usuário duplicado**.
3. Conclua o assistente de usuário duplicado.

Eliminar um utilizador

Você pode excluir um usuário local para remover permanentemente esse usuário do sistema.

Não é possível excluir o usuário raiz.

Passos

1. Na página usuários, marque a caixa de seleção para cada usuário que deseja remover.
2. Selecione **ações** > **Excluir usuário**.
3. Selecione **Eliminar utilizador**.

Usar logon único (SSO)

Configurar o logon único

Quando o logon único (SSO) está ativado, os usuários só podem acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de gerenciamento de grade ou a API de gerenciamento de locatário se suas credenciais forem autorizadas usando o processo de login SSO implementado pela sua organização. Os usuários locais não podem entrar no StorageGRID.

Como o single sign-on funciona

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0).

Antes de ativar o SSO (logon único), verifique como os processos de login e logout do StorageGRID são afetados quando o SSO está ativado.

Inicie sessão quando o SSO estiver ativado

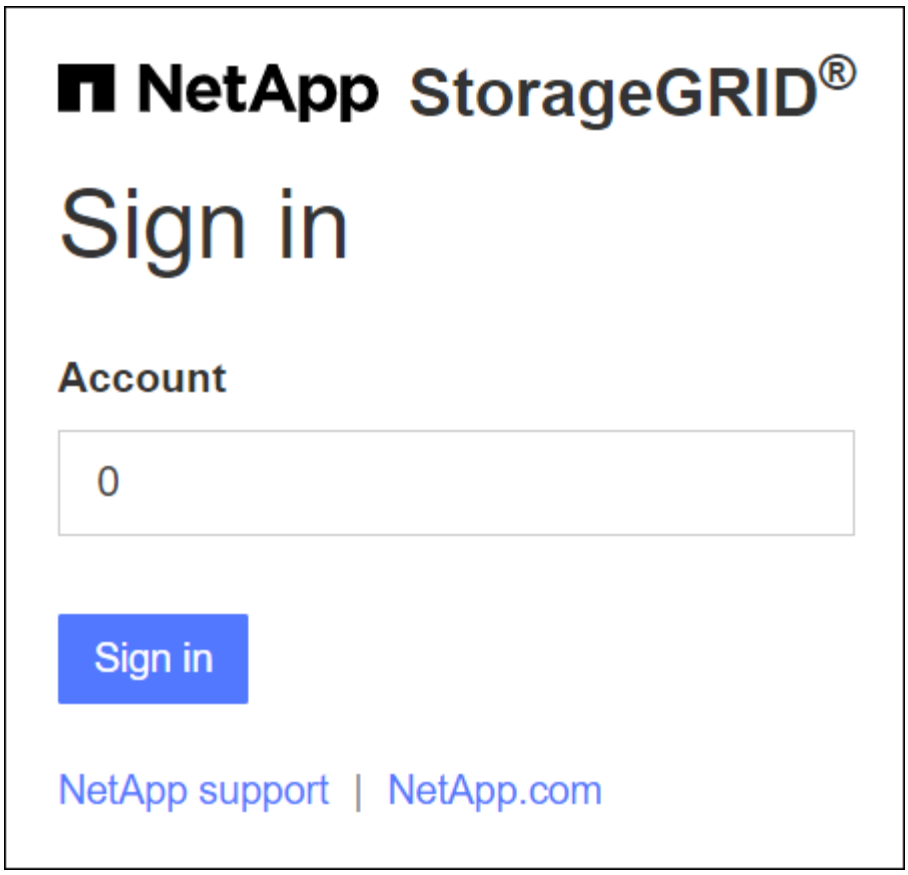
Quando o SSO está ativado e você entra no StorageGRID, você é redirecionado para a página SSO da sua organização para validar suas credenciais.

Passos

1. Insira o nome de domínio totalmente qualificado ou o endereço IP de qualquer nó de administrador do StorageGRID em um navegador da Web.

   É apresentada a página de início de sessão do StorageGRID.

   - Se esta for a primeira vez que você acessou o URL neste navegador, será solicitado um ID de conta:

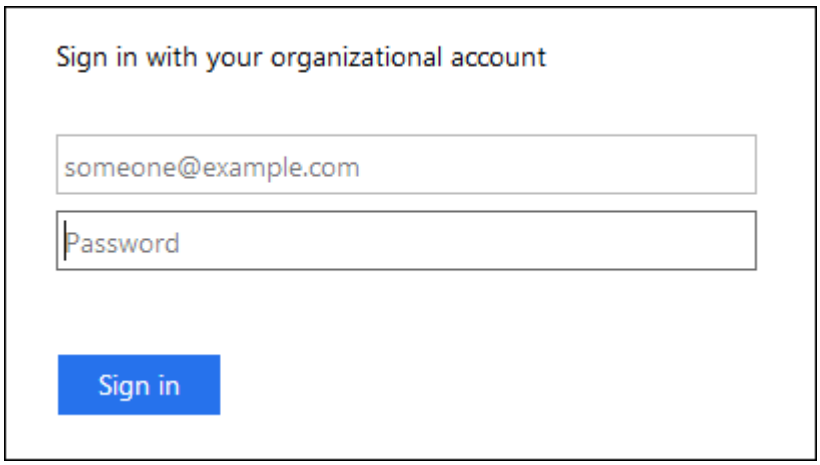


- Se você acessou anteriormente o Gerenciador de Grade ou o Gerente do Locatário, será solicitado que você selecione uma conta recente ou insira um ID de conta:

A página de login do StorageGRID não é exibida quando você insere o URL completo de uma conta de locatário (ou seja, um nome de domínio totalmente qualificado ou endereço IP seguido de `/?accountId=20-digit-account-id`). Em vez disso, você será imediatamente redirecionado para a página de login SSO da sua organização, onde você pode Inicie sessão com as suas credenciais SSO.

2. Indique se deseja acessar o Gerenciador de Grade ou o Gerenciador de Locatário:
   - Para acessar o Gerenciador de Grade, deixe o campo **ID de conta** em branco, digite **0** como ID de conta ou selecione **Gerenciador de Grade** se ele aparecer na lista de contas recentes.
   - Para acessar o Gerenciador do Locatário, insira o ID da conta do locatário de 20 dígitos ou selecione um locatário pelo nome se ele aparecer na lista de contas recentes.
3. Selecione **entrar**

   O StorageGRID redireciona você para a página de login SSO da sua organização. Por exemplo:



4. Faça login com suas credenciais SSO.

   Se suas credenciais SSO estiverem corretas:

   a. O provedor de identidade (IDP) fornece uma resposta de autenticação ao StorageGRID.
   b. O StorageGRID valida a resposta de autenticação.
   c. Se a resposta for válida e você pertencer a um grupo federado com permissões de acesso ao StorageGRID, você estará conetado ao Gerenciador de Grade ou ao Gerenciador de Locatário, dependendo da conta selecionada.

   Se a conta de serviço estiver inacessível, você ainda poderá fazer login, contanto que você seja um usuário existente que pertença a um grupo federado com permissões de acesso ao StorageGRID.

5. Opcionalmente, acesse outros nós de administração ou acesse o Gerenciador de grade ou o Gerenciador de locatário, se você tiver permissões adequadas.

   Você não precisa reinserir suas credenciais SSO.

Sair quando o SSO estiver ativado

Quando o SSO está ativado para o StorageGRID, o que acontece quando você sai depende do que você está conetado e de onde você está se saindo.

Passos

1. Localize o link **Sair** no canto superior direito da interface do usuário.
2. Selecione **Sair**.

   É apresentada a página de início de sessão do StorageGRID. A lista suspensa **Recent Accounts** (Contas recentes) é atualizada para incluir o **Grid Manager** ou o nome do locatário, para que você possa acessar essas interfaces de usuário mais rapidamente no futuro.

Se você estiver conetado a…	E você sai de…	Você está logado fora de…
Grid Manager em um ou mais nós de administração	Grid Manager em qualquer nó de administração	Grid Manager em todos os nós de administração **Observação:** se você usar o Azure para SSO, pode levar alguns minutos para ser desconetado de todos os nós de administração.
Gerenciador de locatários em um ou mais nós de administração	Gerente de locatário em qualquer nó de administrador	Gerenciador de locatários em todos os nós de administração
Tanto o Grid Manager quanto o Tenant Manager	Gerenciador de grade	Apenas o Grid Manager. Você também deve sair do Gerenciador do Locatário para sair do SSO.

A tabela resume o que acontece quando você sai se estiver usando uma única sessão do navegador. Se você estiver conetado ao StorageGRID em várias sessões do navegador, será necessário sair de todas as sessões do navegador separadamente.

Requisitos e considerações para logon único

Antes de ativar o logon único (SSO) para um sistema StorageGRID, revise os requisitos e considerações.

Requisitos do provedor de identidade

O StorageGRID oferece suporte aos seguintes provedores de identidade SSO (IDP):

- Serviço de Federação do ative Directory (AD FS)
- Azure ative Directory (Azure AD)
- PingFederate

Você deve configurar a federação de identidade para o seu sistema StorageGRID antes de poder configurar um provedor de identidade SSO. O tipo de serviço LDAP que você usa para controles de federação de

identidade que tipo de SSO você pode implementar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Ative Directory	• Ative Directory • Azure • PingFederate
Azure	Azure

Requisitos do AD FS

Você pode usar qualquer uma das seguintes versões do AD FS:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> O Windows Server 2016 deve estar usando o "Atualização do KB3201845", ou superior.

Requisitos adicionais

- Transport Layer Security (TLS) 1,2 ou 1,3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Considerações para o Azure

Se você usar o Azure como o tipo SSO e os usuários tiverem nomes principais de usuário que não usam o sAMAccountName como prefixo, problemas de login podem ocorrer se o StorageGRID perder sua conexão com o servidor LDAP. Para permitir que os utilizadores iniciem sessão, tem de restaurar a ligação ao servidor LDAP.

Requisitos de certificado do servidor

Por padrão, o StorageGRID usa um certificado de interface de gerenciamento em cada nó de administrador para proteger o acesso ao Gerenciador de Grade, ao Gerenciador de locatário, à API de gerenciamento de grade e à API de gerenciamento de locatário. Quando você configura confiança de parte confiável (AD FS), aplicativos empresariais (Azure) ou conexões de provedor de serviços (PingFederate) para StorageGRID, você usa o certificado de servidor como o certificado de assinatura para solicitações StorageGRID.

Se ainda não "configurado um certificado personalizado para a interface de gerenciamento"o fez, deve fazê-lo agora. Quando você instala um certificado de servidor personalizado, ele é usado para todos os nós de administração e você pode usá-lo em todos os trusts de partes dependentes do StorageGRID, aplicativos empresariais ou conexões SP.

> O uso do certificado de servidor padrão de um nó de administrador em uma conexão de confiança de parte confiável, aplicativo empresarial ou SP não é recomendado. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de iniciar sessão no nó recuperado, tem de atualizar a confiança de parte fidedigna, a aplicação empresarial ou a ligação SP com o novo certificado.

Você pode acessar o certificado de servidor de um nó de administrador fazendo login no shell de comando do nó e indo para `/var/local/mgmt-api` o diretório. Um certificado de servidor personalizado é `custom-server.crt` nomeado . O certificado de servidor padrão do nó é `server.crt` nomeado .

Requisitos portuários

O logon único (SSO) não está disponível nas portas do Gerenciador de Grade restrito ou do Gerenciador de locatário. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único. "Controle o acesso no firewall externo"Consulte .

Confirme se os usuários federados podem entrar

Antes de ativar o logon único (SSO), você deve confirmar que pelo menos um usuário federado pode entrar no Gerenciador de Grade e entrar no Gerenciador de locatários para quaisquer contas de locatário existentes.

Antes de começar

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

Passos

1. Se houver contas de inquilino existentes, confirme que nenhum dos inquilinos está usando sua própria fonte de identidade.

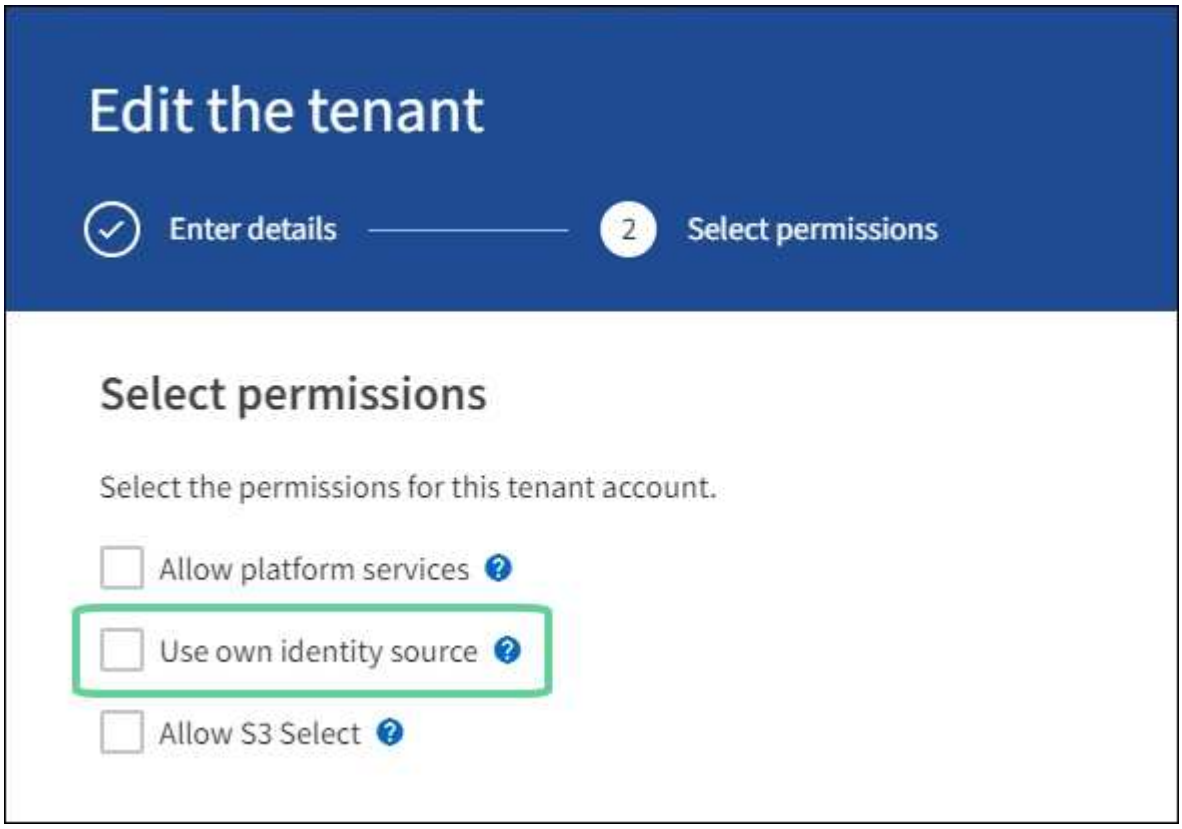
   Quando você ativa o SSO, uma fonte de identidade configurada no Gerenciador de locatário é substituída pela origem de identidade configurada no Gerenciador de Grade. Os usuários pertencentes à fonte de identidade do locatário não poderão mais entrar a menos que tenham uma conta com a fonte de identidade do Gerenciador de Grade.

   a. Inicie sessão no Gestor do Locatário para cada conta de inquilino.
   b. Selecione **GERENCIAMENTO DE ACESSO** > **federação de identidade**.
   c. Confirme se a caixa de verificação **Ativar federação de identidade** não está selecionada.
   d. Se estiver, confirme se os grupos federados que possam estar em uso para essa conta de locatário não são mais necessários, desmarque a caixa de seleção e selecione **Salvar**.

2. Confirme se um usuário federado pode acessar o Gerenciador de Grade:
   a. No Gerenciador de Grade, selecione **CONFIGURATION** > **Access Control** > **Admin Groups**.
   b. Certifique-se de que pelo menos um grupo federado tenha sido importado da origem de identidade do ative Directory e de que tenha sido atribuída a permissão de acesso raiz.
   c. Terminar sessão.
   d. Confirme que você pode fazer login novamente no Gerenciador de Grade como um usuário no grupo federado.
3. Se houver contas de locatário existentes, confirme se um usuário federado que tenha permissão de acesso root pode entrar:
   a. No Gerenciador de Grade, selecione **TENANTS**.
   b. Selecione a conta de locatário e selecione **ações** > **Editar**.

c. Na guia Inserir detalhes, selecione **continuar**.

d. Se a caixa de seleção **Use own Identity source** estiver selecionada, desmarque a caixa e selecione **Save**.



É apresentada a página do locatário.

a. Selecione a conta de locatário, selecione **entrar** e faça login na conta de locatário como usuário raiz local.

b. No Gerenciador do Locatário, selecione **GERENCIAMENTO DE ACESSO** > **grupos**.

c. Certifique-se de que pelo menos um grupo federado do Gerenciador de Grade recebeu a permissão de acesso raiz para esse locatário.

d. Terminar sessão.

e. Confirme que você pode fazer login novamente no locatário como um usuário no grupo federado.

Informações relacionadas

- "Requisitos e considerações para logon único"
- "Gerenciar grupos de administradores"
- "Use uma conta de locatário"

Use o modo sandbox

Você pode usar o modo sandbox para configurar e testar o logon único (SSO) antes de habilitá-lo para todos os usuários do StorageGRID. Depois que o SSO estiver ativado, você poderá retornar ao modo sandbox sempre que precisar alterar ou testar novamente a configuração.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Você configurou a federação de identidade para o seu sistema StorageGRID.
- Para a federação de identidade **tipo de serviço LDAP**, você selecionou o ative Directory ou o Azure, com base no provedor de identidade SSO que você planeja usar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Ative Directory	• Ative Directory • Azure • PingFederate
Azure	Azure

Sobre esta tarefa

Quando o SSO está ativado e um usuário tenta entrar em um nó de administrador, o StorageGRID envia uma solicitação de autenticação para o provedor de identidade SSO. Por sua vez, o provedor de identidade SSO envia uma resposta de autenticação de volta ao StorageGRID, indicando se a solicitação de autenticação foi bem-sucedida. Para solicitações bem-sucedidas:

- A resposta do ative Directory ou PingFederate inclui um identificador universal único (UUID) para o usuário.
- A resposta do Azure inclui um Nome Principal de Usuário (UPN).

Para permitir que o StorageGRID (o provedor de serviços) e o provedor de identidade SSO se comuniquem com segurança sobre solicitações de autenticação de usuário, você deve configurar certas configurações no StorageGRID. Em seguida, você deve usar o software do provedor de identidade SSO para criar uma confiança de parte confiável (AD FS), aplicativo empresarial (Azure) ou provedor de serviços (PingFederate) para cada nó de administração. Finalmente, você deve retornar ao StorageGRID para ativar o SSO.

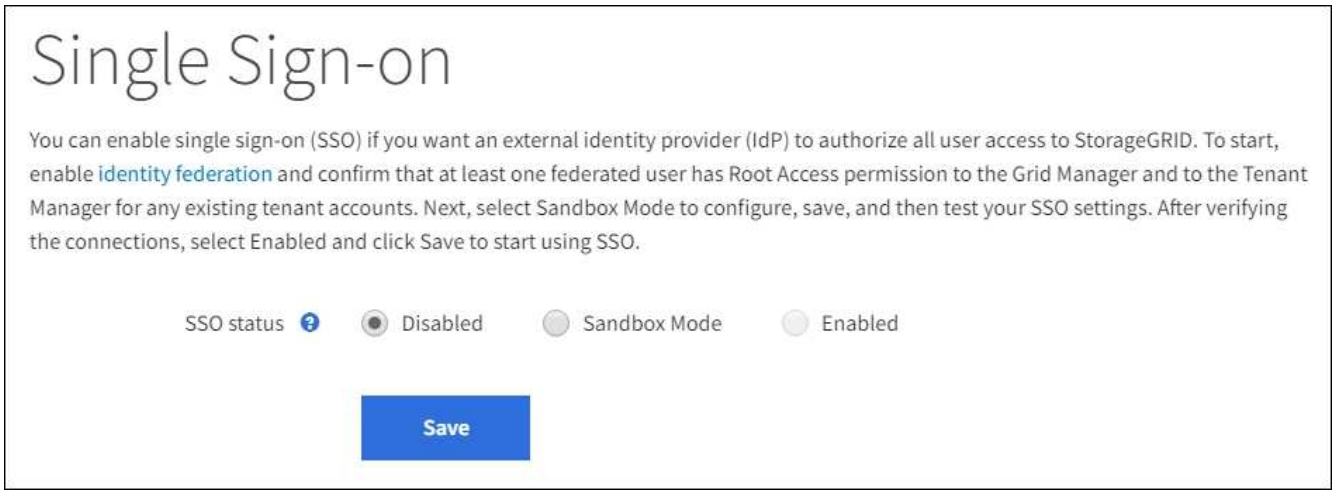
O modo Sandbox facilita a execução desta configuração de back-and-forth e testar todas as suas configurações antes de ativar o SSO. Quando você está usando o modo sandbox, os usuários não podem entrar usando SSO.

Acesse o modo sandbox

Passos

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.

   A página Single Sign-On (Início de sessão único) é exibida, com a opção **Disabled** selecionada.



Se as opções de Status SSO não aparecerem, confirme se você configurou o provedor de identidade como a origem de identidade federada. "Requisitos e considerações para logon único"Consulte .

2. Selecione **Sandbox Mode**.

   A seção Provedor de identidade é exibida.

Insira os detalhes do provedor de identidade

Passos

1. Selecione o **SSO type** na lista suspensa.
2. Preencha os campos na seção Provedor de identidade com base no tipo SSO selecionado.

Ative Directory

a. Digite o nome do serviço **Federation** para o provedor de identidade, exatamente como aparece no ative Directory Federation Service (AD FS).

> Para localizar o nome do serviço de federação, vá para Gerenciador do Windows Server. Selecione **Ferramentas** > **Gerenciamento do AD FS**. No menu Ação, selecione **Editar Propriedades do Serviço de Federação**. O Nome do Serviço de Federação é apresentado no segundo campo.

b. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta a solicitações StorageGRID.

- **Use o certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

  Se você selecionar essa configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, "Reinicie o serviço mgmt-api nos nós de administração"imediatamente e testar se há um SSO bem-sucedido no Gerenciador de Grade.

c. Na seção parte dependente, especifique o **identificador de parte dependente** para StorageGRID. Esse valor controla o nome que você usa para cada confiança de parte confiável no AD FS.

- Por exemplo, se sua grade tiver apenas um nó Admin e você não antecipar a adição de mais nós Admin no futuro, digite `SG` ou `StorageGRID`.
- Se sua grade incluir mais de um nó Admin, inclua a cadeia `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que mostra o identificador de parte confiável para cada nó Admin em seu sistema, com base no nome do host do nó.

> Você deve criar uma confiança de parte confiável para cada nó de administrador no seu sistema StorageGRID. Ter uma confiança de parte confiável para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

d. Selecione **Guardar**.

Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

Azure

a. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de

identidade enviar informações de configuração SSO em resposta a solicitações StorageGRID.

- **Use o certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

  Se você selecionar essa configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, "Reinicie o serviço mgmt-api nos nós de administração"imediatamente e testar se há um SSO bem-sucedido no Gerenciador de Grade.

b. Na seção aplicativo empresarial, especifique o **Nome do aplicativo empresarial** para StorageGRID. Esse valor controla o nome que você usa para cada aplicativo corporativo no Azure AD.

- Por exemplo, se sua grade tiver apenas um nó Admin e você não antecipar a adição de mais nós Admin no futuro, digite `SG` ou `StorageGRID`.
- Se sua grade incluir mais de um nó Admin, inclua a cadeia `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que mostra um nome de aplicativo corporativo para cada nó Admin em seu sistema, com base no nome do host do nó.

> Você deve criar um aplicativo empresarial para cada nó de administração no sistema StorageGRID. Ter um aplicativo corporativo para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

c. Siga as etapas em "Crie aplicativos empresariais no Azure AD" para criar um aplicativo corporativo para cada nó de administração listado na tabela.

d. No Azure AD, copie o URL de metadados da federação para cada aplicativo corporativo. Em seguida, cole esse URL no campo **URL de metadados de Federação** correspondente no StorageGRID.

e. Depois de copiar e colar um URL de metadados de federação para todos os nós de administração, selecione **Salvar**.

   Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

PingFederate

a. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta a solicitações StorageGRID.

- **Use o certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a

conexão.

Se você selecionar essa configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, "Reinicie o serviço mgmt-api nos nós de administração"imediatamente e testar se há um SSO bem-sucedido no Gerenciador de Grade.

b. Na seção Fornecedor de Serviços (SP), especifique o **ID de conexão SP** para StorageGRID. Esse valor controla o nome que você usa para cada conexão SP no PingFederate.

- Por exemplo, se sua grade tiver apenas um nó Admin e você não antecipar a adição de mais nós Admin no futuro, digite `SG` ou `StorageGRID`.
- Se sua grade incluir mais de um nó Admin, inclua a cadeia `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que mostra o ID de conexão do SP para cada nó de administrador no sistema, com base no nome do host do nó.

> Você deve criar uma conexão SP para cada nó de administração no sistema StorageGRID. Ter uma conexão SP para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

c. Especifique o URL de metadados de federação para cada nó Admin no campo **URL de metadados de Federação**.

Use o seguinte formato:

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

d. Selecione **Guardar**.

Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

Configurar trusts de terceiros confiáveis, aplicativos empresariais ou conexões SP

Quando a configuração é salva, o aviso de confirmação do modo Sandbox é exibido. Este aviso confirma que o modo sandbox está agora ativado e fornece instruções de visão geral.

O StorageGRID pode permanecer no modo sandbox enquanto necessário. No entanto, quando **modo Sandbox** está selecionado na página de logon único, o SSO é desativado para todos os usuários do StorageGRID. Somente usuários locais podem fazer login.

Siga estas etapas para configurar as trusts de parte confiável (ative Directory), aplicativos empresariais completos (Azure) ou configurar conexões SP (PingFederate).

Ative Directory

Passos

1. Vá para Serviços de Federação do ative Directory (AD FS).
2. Crie uma ou mais confianças de parte confiáveis para o StorageGRID, usando cada identificador de parte confiável mostrado na tabela na página de logon único do StorageGRID.

   Você deve criar uma confiança para cada nó Admin mostrado na tabela.

   Para obter instruções, vá "Criar confiança de parte confiável no AD FS"para .

Azure

Passos

1. Na página de logon único para o nó Admin ao qual você está conetado atualmente, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para qualquer outro nó Admin na sua grade, repita estas etapas:
   a. Faça login no nó.
   b. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Vá para o Portal do Azure.
4. Siga as etapas em "Crie aplicativos empresariais no Azure AD" para carregar o arquivo de metadados SAML para cada nó Admin em seu aplicativo corporativo do Azure correspondente.

PingFederate

Passos

1. Na página de logon único para o nó Admin ao qual você está conetado atualmente, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para qualquer outro nó Admin na sua grade, repita estas etapas:
   a. Faça login no nó.
   b. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Vá para PingFederate.
4. "Crie uma ou mais conexões de provedor de serviços (SP) para o StorageGRID". Use o ID de conexão do SP para cada nó de administrador (mostrado na tabela na página de logon único do StorageGRID) e os metadados SAML que você baixou para esse nó de administrador.

   Você deve criar uma conexão SP para cada nó de administrador mostrado na tabela.

Testar conexões SSO

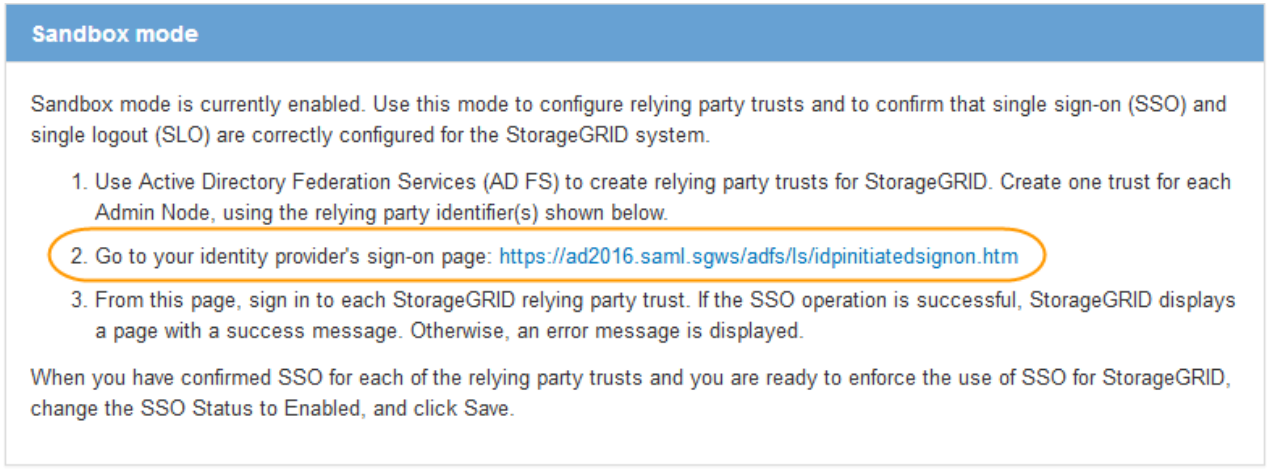
Antes de aplicar o uso de logon único para todo o sistema StorageGRID, você deve confirmar que o logon único e o logout único estão configurados corretamente para cada nó de administração.

Ative Directory

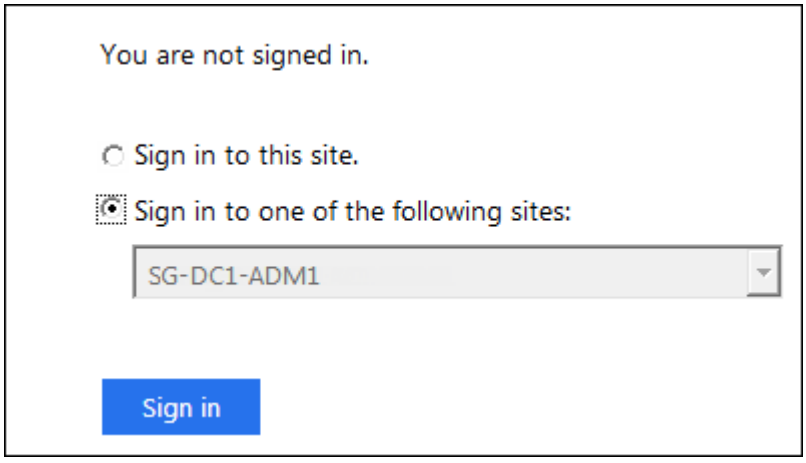
Passos

1. Na página de logon único do StorageGRID, localize o link na mensagem do modo Sandbox.

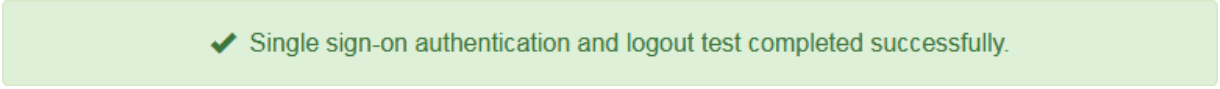
   O URL é derivado do valor inserido no campo **Nome do serviço de Federação**.



2. Selecione o link ou copie e cole o URL em um navegador para acessar a página de logon do provedor de identidade.
3. Para confirmar que você pode usar o SSO para entrar no StorageGRID, selecione **entrar em um dos seguintes sites**, selecione o identificador de parte confiável para seu nó de administrador principal e selecione **entrar**.



4. Introduza o seu nome de utilizador federado e a palavra-passe.
   - Se as operações de login e logout SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.



   - Se a operação SSO não for bem-sucedida, será exibida uma mensagem de erro. Corrija o problema, limpe os cookies do navegador e tente novamente.
5. Repita estas etapas para verificar a conexão SSO para cada nó Admin na grade.

Azure

Passos

1. Vá para a página de logon único no portal do Azure.
2. Selecione **Teste este aplicativo**.
3. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

     ✔ Single sign-on authentication and logout test completed successfully.

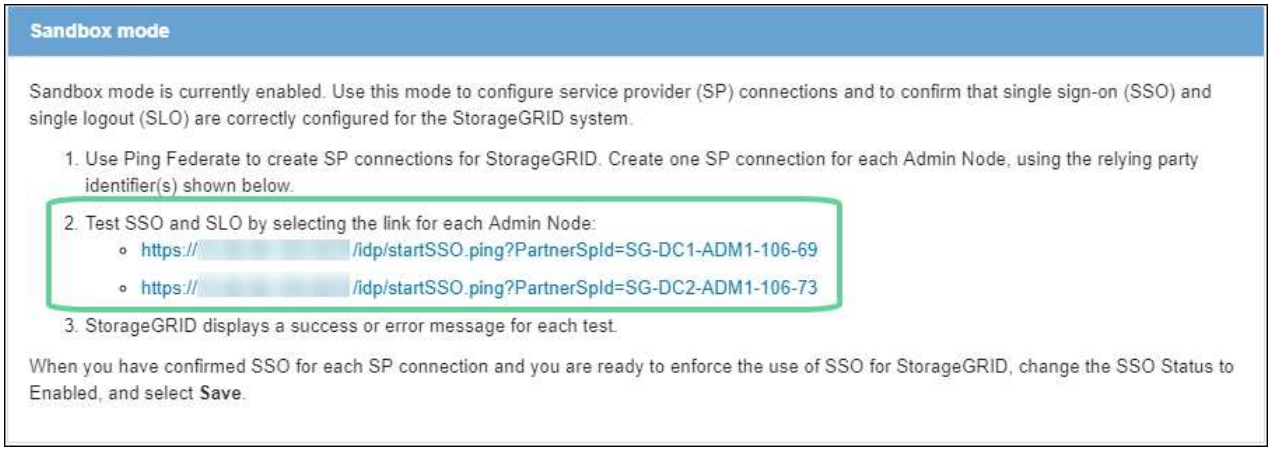
   - Se a operação SSO não for bem-sucedida, será exibida uma mensagem de erro. Corrija o problema, limpe os cookies do navegador e tente novamente.
4. Repita estas etapas para verificar a conexão SSO para cada nó Admin na grade.

PingFederate

Passos

1. Na página de logon único do StorageGRID, selecione o primeiro link na mensagem do modo Sandbox.

   Selecione e teste um link de cada vez.



2. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Se a operação SSO não for bem-sucedida, será exibida uma mensagem de erro. Corrija o problema, limpe os cookies do navegador e tente novamente.
3. Selecione o próximo link para verificar a conexão SSO para cada nó Admin na grade.

   Se você vir uma mensagem Página expirada, selecione o botão **voltar** no seu navegador e reenvie suas credenciais.

Ative o logon único

Quando você confirmar que pode usar o SSO para fazer login em cada nó de administrador, você pode ativar o SSO para todo o seu sistema StorageGRID.

> Quando o SSO está ativado, todos os usuários devem usar o SSO para acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de Gerenciamento de Grade e a API de Gerenciamento de Locatário. Os usuários locais não podem mais acessar o StorageGRID.

Passos

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
2. Altere o Status SSO para **Enabled**.
3. Selecione **Guardar**.
4. Reveja a mensagem de aviso e selecione **OK**.

   O início de sessão único está agora ativado.

> Se você estiver usando o Portal do Azure e acessar o StorageGRID do mesmo computador que usa para acessar o Azure, verifique se o usuário do Portal do Azure também é um usuário autorizado do StorageGRID (um usuário em um grupo federado que foi importado para o StorageGRID) ou faça logout do Portal do Azure antes de tentar entrar no StorageGRID.

Criar confiança de parte confiável no AD FS

Você deve usar os Serviços de Federação do ative Directory (AD FS) para criar uma confiança de parte confiável para cada nó de administração em seu sistema. Você pode criar trusts confiáveis de parte usando comandos do PowerShell, importando metadados SAML do StorageGRID ou inserindo os dados manualmente.

Antes de começar

- Você configurou o logon único para o StorageGRID e selecionou **AD FS** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. "Use o modo sandbox"Consulte .
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de entidade dependente para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos nós de administração na página de logon único do StorageGRID.

> Você deve criar uma confiança de parte confiável para cada nó de administrador no seu sistema StorageGRID. Ter uma confiança de parte confiável para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

- Você tem experiência em criar confiança de parte confiável no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in Gerenciamento do AD FS e pertence ao grupo Administradores.
- Se você estiver criando a confiança de parte confiável manualmente, você tem o certificado personalizado que foi carregado para a interface de gerenciamento do StorageGRID ou sabe como fazer login em um nó de administrador a partir do shell de comando.

Sobre esta tarefa

Estas instruções aplicam-se ao Windows Server 2016 AD FS. Se você estiver usando uma versão diferente do AD FS, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Crie uma confiança de parte confiável usando o Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais trusts de parte confiáveis.

Passos

1. No menu Iniciar do Windows, selecione o ícone do PowerShell com o botão direito e selecione **Executar como Administrador**.
2. No prompt de comando do PowerShell, digite o seguinte comando:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Para `Admin_Node_Identifier`, insira o Identificador de parte dependente para o nó Admin, exatamente como aparece na página Início de sessão único. Por exemplo, `SG-DC1-ADM1`.
   - Para `Admin_Node_FQDN`, introduza o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)
3. No Gerenciador do Windows Server, selecione **Ferramentas** > **Gerenciamento do AD FS**.

   A ferramenta de gerenciamento do AD FS é exibida.
4. Selecione **AD FS** > **confiar em parts**.

   É apresentada a lista de confianças de partes dependentes.
5. Adicione uma Política de Controle de Acesso à confiança da entidade dependente recém-criada:
   a. Localize a confiança de quem confia que você acabou de criar.
   b. Clique com o botão direito do rato na fidedignidade e selecione **Editar política de controlo de acesso**.
   c. Selecione uma política de controlo de acesso.
   d. Selecione **aplicar** e **OK**
6. Adicione uma Política de emissão de reclamação à recém-criada confiança da parte dependente:
   a. Localize a confiança de quem confia que você acabou de criar.
   b. Clique com o botão direito do rato na confiança e selecione **Editar política de emissão de reclamação**.
   c. Selecione **Adicionar regra**.
   d. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **Avançar**.
   e. Na página Configurar regra, insira um nome de exibição para essa regra.

      Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

f. Para o Attribute Store, selecione **ative Directory**.

g. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID** ou selecione **User-Principal-Name**.

h. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.

i. Selecione **Finish** e **OK**.

7. Confirme se os metadados foram importados com sucesso.

a. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.

b. Confirme se os campos nas guias **Endpoints**, **Identificadores** e **assinatura** estão preenchidos.

Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou insira os valores manualmente.

8. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.

9. Quando terminar, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. "Use o modo Sandbox"Consulte para obter instruções.

Crie uma confiança de parte confiável importando metadados de federação

Você pode importar os valores de cada confiança de parte confiável acessando os metadados SAML para cada nó de administração.

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e **Gerenciamento do AD FS**.

2. Em ações, selecione **Adicionar confiança de parte dependente**.

3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e selecione **Iniciar**.

4. Selecione **Importar dados sobre a parte dependente publicada on-line ou em uma rede local**.

5. Em **Endereço de metadados de Federação (nome do host ou URL)**, digite o local dos metadados SAML para este nó de administração:

`https://Admin_Node_FQDN/api/saml-metadata`

Para *`Admin_Node_FQDN`*, introduza o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

6. Conclua o assistente confiar na parte confiável, salve a confiança da parte confiável e feche o assistente.

> Ao inserir o nome de exibição, use o Identificador de parte confiável para o nó Admin, exatamente como ele aparece na página de logon único no Gerenciador de Grade. Por exemplo, `SG-DC1-ADM1`.

7. Adicionar uma regra de reclamação:

a. Clique com o botão direito do rato na confiança e selecione **Editar política de emissão de reclamação**.

b. Selecione **Adicionar regra**:

c. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **Avançar**.

d. Na página Configurar regra, insira um nome de exibição para essa regra.

   Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

e. Para o Attribute Store, selecione **ative Directory**.

f. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID** ou selecione **User-Principal-Name**.

g. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.

h. Selecione **Finish** e **OK**.

8. Confirme se os metadados foram importados com sucesso.

   a. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.

   b. Confirme se os campos nas guias **Endpoints**, **Identificadores** e **assinatura** estão preenchidos.

      Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou insira os valores manualmente.

9. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.

10. Quando terminar, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. "Use o modo Sandbox"Consulte para obter instruções.

Crie uma confiança de parte confiável manualmente

Se você optar por não importar os dados para as partes confiáveis, você poderá inserir os valores manualmente.

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e **Gerenciamento do AD FS**.
2. Em ações, selecione **Adicionar confiança de parte dependente**.
3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e selecione **Iniciar**.
4. Selecione **Digite os dados sobre a parte que depende manualmente** e selecione **Next**.
5. Conclua o assistente confiança da parte dependente:

   a. Introduza um nome de apresentação para este nó de administração.

      Para obter consistência, use o Identificador de parte confiável para o nó Admin, exatamente como ele aparece na página de logon único no Gerenciador de Grade. Por exemplo, `SG-DC1-ADM1`.

   b. Ignore a etapa para configurar um certificado de criptografia de token opcional.

   c. Na página Configurar URL, marque a caixa de seleção **Ativar suporte para o protocolo SAML 2,0 WebSSO**.

   d. Digite o URL do endpoint do serviço SAML para o nó Admin:

`https://Admin_Node_FQDN/api/saml-response`

Para *Admin_Node_FQDN*, introduza o nome de domínio totalmente qualificado para o nó Admin. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

e. Na página Configurar Identificadores, especifique o Identificador da parte de dependência para o mesmo nó de administração:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, insira o Identificador de parte dependente para o nó Admin, exatamente como aparece na página Início de sessão único. Por exemplo, `SG-DC1-ADM1`.

f. Revise as configurações, salve a confiança da parte confiável e feche o assistente.

A caixa de diálogo Editar política de emissão de reclamação é exibida.

> Se a caixa de diálogo não for exibida, clique com o botão direito do Mouse no Trust e selecione **Editar política de emissão de reclamação**.

6. Para iniciar o assistente de regra de reclamação, selecione **Adicionar regra**:
   a. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **Avançar**.
   b. Na página Configurar regra, insira um nome de exibição para essa regra.

      Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

   c. Para o Attribute Store, selecione **ative Directory**.
   d. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID** ou selecione **User-Principal-Name**.
   e. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
   f. Selecione **Finish** e **OK**.
7. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.
8. Na guia **Endpoints**, configure o endpoint para logout único (SLO):
   a. Selecione **Adicionar SAML**.
   b. Selecione **Endpoint Type** > **SAML Logout**.
   c. Selecione **Binding** > **Redirect**.
   d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste nó Admin:

      `https://Admin_Node_FQDN/api/saml-logout`

   Para *Admin_Node_FQDN*, introduza o nome de domínio totalmente qualificado do nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

a. Selecione **OK**.

9. Na guia **assinatura**, especifique o certificado de assinatura para essa confiança de parte confiável:
   a. Adicione o certificado personalizado:
      - Se tiver o certificado de gestão personalizado que carregou no StorageGRID, selecione esse certificado.
      - Se você não tiver o certificado personalizado, faça login no Admin Node, vá para `/var/local/mgmt-api` o diretório do Admin Node e adicione o `custom-server.crt` arquivo de certificado.

        O uso do certificado padrão do Admin Node (`server.crt`) não é recomendado. Se o nó Admin falhar, o certificado padrão será regenerado quando você recuperar o nó e você precisará atualizar a confiança da parte confiável.

   b. Selecione **aplicar** e **OK**.

      As propriedades da parte dependente são salvas e fechadas.

10. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.
11. Quando terminar, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. "Use o modo sandbox"Consulte para obter instruções.

Crie aplicativos empresariais no Azure AD

Você usa o Azure AD para criar um aplicativo corporativo para cada nó de administrador no sistema.

Antes de começar

- Você começou a configurar o logon único para o StorageGRID e selecionou **Azure** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. "Use o modo sandbox"Consulte .
- Você tem o **Nome do aplicativo Enterprise** para cada nó Admin no seu sistema. Você pode copiar esses valores da tabela de detalhes do nó de administrador na página de logon único do StorageGRID.

  Você deve criar um aplicativo empresarial para cada nó de administração no sistema StorageGRID. Ter um aplicativo corporativo para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

- Você tem experiência em criar aplicativos empresariais no Azure ative Directory.
- Você tem uma conta do Azure com uma assinatura ativa.
- Você tem uma das seguintes funções na conta do Azure: Administrador Global, Administrador de aplicativos em nuvem, Administrador de aplicativos ou proprietário do responsável do serviço.

Acesse o Azure AD

Passos

1. Inicie sessão no "Portal do Azure".

2. Navegue até "Azure ative Directory".
3. "Aplicações empresariais"Selecione .

Crie aplicativos empresariais e salve a configuração SSO do StorageGRID

Para salvar a configuração SSO para o Azure no StorageGRID, você deve usar o Azure para criar um aplicativo corporativo para cada nó de administração. Você copiará os URLs de metadados da federação do Azure e os colará nos campos **URL de metadados da Federação** correspondentes na página de logon único do StorageGRID.

Passos

1. Repita as etapas a seguir para cada nó Admin.
   a. No painel aplicativos do Azure Enterprise, selecione **novo aplicativo**.
   b. Selecione **Crie seu próprio aplicativo**.
   c. Para o nome, insira o **Nome do aplicativo da empresa** que você copiou da tabela de detalhes do nó de administrador na página de logon único do StorageGRID.
   d. Deixe o botão de opção **integrar qualquer outro aplicativo que você não encontrar na galeria (não galeria)** selecionado.
   e. Selecione **criar**.
   f. Selecione o link **Get Started** no **2. Configure a caixa Single Sign On** (Início de sessão único) ou selecione o link **Single Sign-On** (Início de sessão único) na margem esquerda.
   g. Selecione a caixa **SAML**.
   h. Copie o URL de metadados de Federação de aplicativos*, que você pode encontrar em **Etapa 3 certificado de assinatura SAML**.
   i. Vá para a página de logon único do StorageGRID e cole o URL no campo **URL de metadados da Federação** que corresponde ao nome do aplicativo **empresa** que você usou.
2. Depois de colar um URL de metadados de federação para cada nó de administrador e fazer todas as outras alterações necessárias na configuração SSO, selecione **Salvar** na página de logon único do StorageGRID.

Faça o download dos metadados SAML para cada nó de administração

Depois que a configuração SSO for salva, você pode baixar um arquivo de metadados SAML para cada nó de administrador no sistema StorageGRID.

Passos

1. Repita estas etapas para cada nó Admin.
   a. Inicie sessão no StorageGRID a partir do nó de administração.
   b. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   c. Selecione o botão para baixar os metadados SAML para esse nó Admin.
   d. Salve o arquivo, que você carregará no Azure AD.

Carregue metadados SAML para cada aplicação empresarial

Depois de baixar um arquivo de metadados SAML para cada nó de administrador do StorageGRID, execute as seguintes etapas no Azure AD:

Passos

1. Retorne ao Portal do Azure.
2. Repita estes passos para cada aplicação empresarial:

   > Talvez seja necessário atualizar a página aplicativos empresariais para ver os aplicativos adicionados anteriormente na lista.

   a. Vá para a página Propriedades do aplicativo corporativo.
   b. Defina **atribuição necessária** como **não** (a menos que você queira configurar atribuições separadamente).
   c. Aceda à página de início de sessão único.
   d. Conclua a configuração SAML.
   e. Selecione o botão **Upload metadata file** e selecione o arquivo de metadados SAML que você baixou para o Admin Node correspondente.
   f. Depois que o arquivo for carregado, selecione **Save** e, em seguida, selecione **X** para fechar o painel. Você será retornado à página Configurar logon único com SAML.
3. Siga os passos em "Use o modo sandbox" para testar cada aplicação.

Crie conexões de provedor de serviços (SP) no PingFederate

Você usa o PingFederate para criar uma conexão de provedor de serviços (SP) para cada nó de administrador no seu sistema. Para acelerar o processo, você importará os metadados SAML do StorageGRID.

Antes de começar

- Você configurou o logon único para o StorageGRID e selecionou **Ping federate** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. "Use o modo sandbox"Consulte .
- Você tem o **ID de conexão SP** para cada nó de administrador no sistema. Você pode encontrar esses valores na tabela de detalhes dos nós de administração na página de logon único do StorageGRID.
- Você baixou os **metadados SAML** para cada nó Admin no seu sistema.
- Você tem experiência em criar conexões SP no servidor PingFederate.
- Você tem o "Guia de referência do administrador" para PingFederate Server. A documentação do PingFederate fornece instruções detalhadas passo a passo e explicações.
- Você tem o "Permissão de administrador" para PingFederate Server.

Sobre esta tarefa

Estas instruções resumem como configurar o PingFederate Server versão 10,3 como um provedor SSO para o StorageGRID. Se você estiver usando outra versão do PingFederate, talvez seja necessário adaptar essas instruções. Consulte a documentação do PingFederate Server para obter instruções detalhadas sobre o seu lançamento.

Complete pré-requisitos no PingFederate

Antes de criar as conexões SP que você usará para o StorageGRID, você deve concluir as tarefas de pré-requisito no PingFederate. Você usará as informações desses pré-requisitos quando configurar as conexões SP.

Criar armazenamento de dados

Se você ainda não o fez, crie um armazenamento de dados para conetar o PingFederate ao servidor LDAP do AD FS. Use os valores usados "configurando a federação de identidade"no StorageGRID.

- * Tipo*: Diretório (LDAP)
- **Tipo LDAP**: Ative Directory
- **Nome do atributo binário**: Insira **objectGUID** na guia atributos binários LDAP exatamente como mostrado.

Criar validador de credenciais de senha

Se você ainda não o fez, crie um validador de credenciais de senha.

- **Type**: LDAP Username Password Credential Validator
- **Armazenamento de dados**: Selecione o armazenamento de dados que você criou.
- **Base de pesquisa**: Insira informações do LDAP (por exemplo,
- **Filtro de pesquisa**: SAMAccountName
- **Escopo**: Subárvore

Criar instância de adaptador IDP

Se você ainda não o fez, crie uma instância de adaptador IDP.

Passos

1. Aceda a **Autenticação** > **integração** > **adaptadores IDP**.
2. Selecione **criar nova instância**.
3. Na guia tipo, selecione **HTML form IDP Adapter**.
4. Na guia adaptador IDP, selecione **Adicionar uma nova linha a 'Validadores de credenciais'**.
5. Selecione o validador de credenciais de senha que você criou.
6. Na guia Adapter Attributes (atributos do adaptador), selecione o atributo **username** para **pseudônimo**.
7. Selecione **Guardar**.

Criar ou importar certificado de assinatura[[certificado de assinatura]]

Se ainda não o fez, crie ou importe o certificado de assinatura.

Passos

1. Aceda a **Security** > **Signing & Decryption Keys & Certificates**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP no PingFederate

Quando você cria uma conexão SP no PingFederate, importa os metadados SAML que você baixou do StorageGRID para o nó Admin. O arquivo de metadados contém muitos dos valores específicos que você precisa.

Você deve criar uma conexão SP para cada nó de administração no sistema StorageGRID, para que os usuários possam fazer login e sair com segurança de qualquer nó. Use estas instruções para criar a primeira conexão SP. Em seguida, aceda a Crie conexões SP adicionais para criar quaisquer ligações adicionais de que necessita.

Escolha o tipo de conexão SP

Passos

1. Aceda a **aplicações** > **integração** > **ligações SP**.
2. Selecione **criar conexão**.
3. Selecione **não utilize um modelo para esta ligação**.
4. Selecione **Browser SSO Profiles** e **SAML 2,0** como protocolo.

Importar metadados do SP

Passos

1. Na guia Importar metadados, selecione **Arquivo**.
2. Escolha o arquivo de metadados SAML que você baixou na página de logon único do StorageGRID para o nó de administração.
3. Revise o Resumo de metadados e as informações fornecidas na guia informações gerais.

   O ID da entidade do Parceiro e o Nome da conexão são definidos como ID de conexão StorageGRID SP. (Por exemplo, 10.96.105.200-DC1-ADM1-105-200). O URL base é o IP do nó de administração do StorageGRID.

4. Selecione **seguinte**.

Configure o SSO do navegador IDP

Passos

1. Na guia SSO do navegador, selecione **Configurar SSO do navegador**.
2. Na guia perfis SAML, selecione as opções **SSO iniciado por SP**, **SLO inicial por SP**, **SSO iniciado por IDP** e **SLO** iniciado por IDP.
3. Selecione **seguinte**.
4. Na guia Assertion Lifetime, não faça alterações.
5. Na guia criação de asserções, selecione **Configurar criação de asserções**.
   a. Na guia Mapeamento de identidade, selecione **Standard**.
   b. Na guia Contrato de Atributo, use o **SAML_SUBJECT** como Contrato de Atributo e o formato de nome não especificado que foi importado.
6. Para estender o contrato, selecione **Excluir** para remover `urn:oid` o , que não é usado.

Instância do adaptador de mapa

Passos

1. Na guia Mapeamento de origem de autenticação, selecione **Mapear nova instância de adaptador**.
2. Na guia instância do adaptador, selecione o instância do adaptador que você criou.

3. Na guia método de mapeamento, selecione **recuperar atributos adicionais de um armazenamento de dados**.
4. Na guia origem do atributo e Pesquisa de usuário, selecione **Adicionar origem do atributo**.
5. Na guia armazenamento de dados, forneça uma descrição e selecione o armazenamento de dados que você adicionou.
6. Na guia Pesquisa de diretório LDAP:
   - Digite o **DN base**, que deve corresponder exatamente ao valor inserido no StorageGRID para o servidor LDAP.
   - Para o escopo de pesquisa, selecione **subtree**.
   - Para a classe Objeto raiz, procure e adicione um destes atributos: **ObjectGUID** ou **userPrincipalName**.
7. Na guia tipos de codificação de atributos binários LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia filtro LDAP, digite **sAMAccountName**.
9. Na guia execução do contrato de atributo, selecione **LDAP (attribute)** na lista suspensa origem e selecione **objectGUID** ou **userPrincipalName** na lista suspensa valor.
10. Revise e salve a fonte do atributo.
11. Na guia origem do atributo de salvamento de falha, selecione **Abortar a transação SSO**.
12. Reveja o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configure as definições do protocolo

Passos

1. Na guia **conexão SP** > **SSO do navegador** > **Configurações do protocolo**, selecione **Configurar configurações do protocolo**.
2. Na guia URL do Serviço ao Consumidor de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para vinculação e `/api/saml-response` URL do ponto final).
3. Na guia URLs de serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para vinculação e `/api/saml-logout` para URL de ponto final.
4. Na guia ligações SAML permitidas, desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são obrigatórios.
5. Na guia Política de assinatura, deixe as caixas de seleção **Require Authn Requests to be signed** e **Always Sign Assertion** selecionadas.
6. Na guia Diretiva de criptografia, selecione **nenhum**.
7. Reveja o resumo e selecione **Concluído** para guardar as definições do protocolo.
8. Revise o resumo e selecione **Concluído** para salvar as configurações de SSO do navegador.

Configurar credenciais

Passos

1. Na guia conexão SP, selecione **credenciais**.
2. Na guia credenciais, selecione **Configurar credenciais**.
3. Selecione o certificado de assinatura que você criou ou importou.

4. Selecione **Next** para ir para **Manage Signature Verification Settings**.
   a. Na guia Trust Model (modelo de confiança), selecione **Unancored** (sem ancoragem).
   b. Na guia certificado de verificação de assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID.
5. Reveja os ecrãs de resumo e selecione **Guardar** para guardar a ligação SP.

Crie conexões SP adicionais

Você pode copiar a primeira conexão SP para criar as conexões SP necessárias para cada nó de administração na grade. Você carrega novos metadados para cada cópia.

> As conexões do SP para diferentes nós de administração usam configurações idênticas, com exceção do ID da entidade do parceiro, URL base, ID da conexão, nome da conexão, verificação de assinatura e URL de resposta do SLO.

Passos

1. Selecione **Ação** > **Copiar** para criar uma cópia da conexão SP inicial para cada nó de administração adicional.
2. Introduza a ID da ligação e o nome da ligação para a cópia e selecione **Guardar**.
3. Escolha o arquivo de metadados correspondente ao nó Admin:
   a. Selecione **Ação** > **Atualizar com metadados**.
   b. Selecione **escolha Arquivo** e carregue os metadados.
   c. Selecione **seguinte**.
   d. Selecione **Guardar**.
4. Resolva o erro devido ao atributo não utilizado:
   a. Selecione a nova ligação.
   b. Selecione **Configure Browser SSO > Configure Assertion creation > Attribute Contract**.
   c. Exclua a entrada para **urn:oid**.
   d. Selecione **Guardar**.

Desative o logon único

Você pode desativar o logon único (SSO) se não quiser mais usar essa funcionalidade. Você deve desativar o logon único antes de desativar a federação de identidade.

Antes de começar

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

Passos

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.

   É apresentada a página Single Sign-on (Início de sessão único).

2. Selecione a opção **Disabled** (Desativado).

3. Selecione **Guardar**.

   É apresentada uma mensagem de aviso indicando que os utilizadores locais poderão iniciar sessão.

4. Selecione **OK**.

   Na próxima vez que você entrar no StorageGRID, a página de login do StorageGRID será exibida e você deverá inserir o nome de usuário e a senha de um usuário do StorageGRID local ou federado.

Desative e reative temporariamente o logon único para um nó de administração

Talvez você não consiga entrar no Gerenciador de Grade se o sistema de logon único (SSO) estiver inativo. Nesse caso, você pode desativar e reativar temporariamente o SSO para um nó de administrador. Para desativar e reativar o SSO, você deve acessar o shell de comando do nó.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Você tem o `Passwords.txt` arquivo.
- Você sabe a senha para o usuário raiz local.

Sobre esta tarefa

Depois de desativar o SSO para um nó Admin, você pode entrar no Gerenciador de Grade como o usuário raiz local. Para proteger seu sistema StorageGRID, você deve usar o shell de comando do nó para reativar o SSO no nó Admin assim que você sair.

> A desativação do SSO para um nó Admin não afeta as configurações de SSO para quaisquer outros nós Admin na grade. A caixa de seleção **Ativar SSO** na página de logon único no Gerenciador de Grade permanece selecionada e todas as configurações SSO existentes são mantidas, a menos que você as atualize.

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.
   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 comando:`disable-saml`

   Uma mensagem indica que o comando se aplica somente a esse nó Admin.

3. Confirme que você deseja desativar o SSO.

   Uma mensagem indica que o logon único está desativado no nó.

4. Em um navegador da Web, acesse o Gerenciador de Grade no mesmo nó Admin.

   A página de login do Gerenciador de Grade agora é exibida porque o SSO foi desativado.

5. Inicie sessão com a raiz do nome de utilizador e a palavra-passe do utilizador raiz local.
6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração SSO:
   a. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   b. Altere as configurações de SSO incorretas ou desatualizadas.
   c. Selecione **Guardar**.

      Selecionar **Save** na página Single Sign-On (Início de sessão único) reativa automaticamente o SSO para toda a grelha.

7. Se você desativou o SSO temporariamente porque precisava acessar o Gerenciador de Grade por algum outro motivo:
   a. Execute qualquer tarefa ou tarefas que você precisa executar.
   b. Selecione **Sair** e feche o Gerenciador de Grade.
   c. Reative o SSO no nó Admin. Você pode executar uma das seguintes etapas:

      - Execute o seguinte comando: `enable-saml`

        Uma mensagem indica que o comando se aplica somente a esse nó Admin.

      Confirme se você deseja ativar o SSO.

   Uma mensagem indica que o logon único está ativado no nó.

      - Reinicie o nó da grade: `reboot`
8. A partir de um navegador da Web, acesse o Gerenciador de Grade a partir do mesmo nó Admin.
9. Confirme se a página de login do StorageGRID é exibida e que você deve inserir suas credenciais SSO para acessar o Gerenciador de Grade.

Use a federação de grade

O que é a federação de grade?

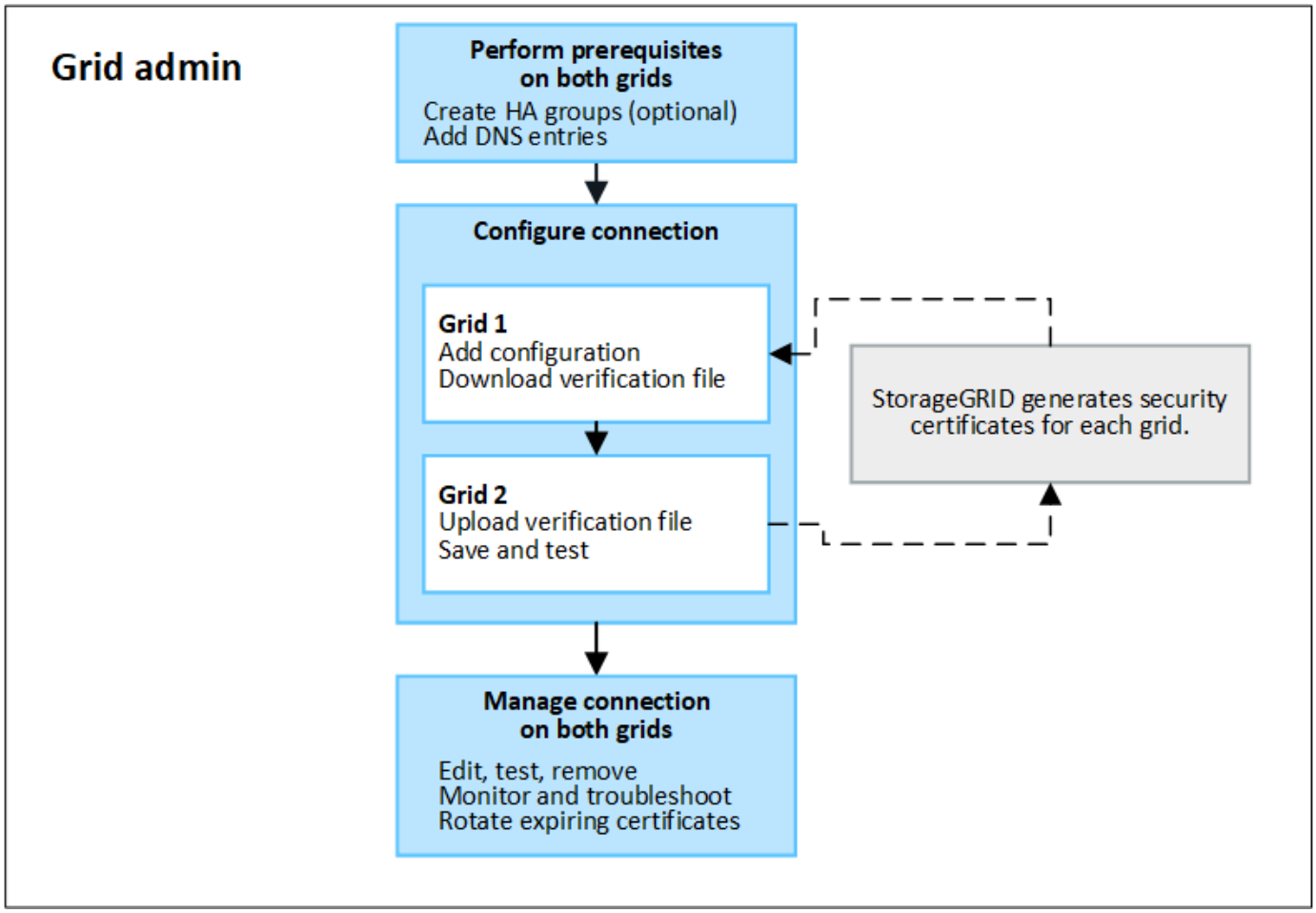
Você pode usar a federação de grade para clonar locatários e replicar seus objetos entre dois sistemas StorageGRID para recuperação de desastres.

O que é uma conexão de federação de grade?

Uma conexão de federação de grade é uma conexão bidirecional, confiável e segura entre os nós de administrador e gateway em dois sistemas StorageGRID.

Fluxo de trabalho para federação de grade

O diagrama de fluxo de trabalho resume as etapas para configurar uma conexão de federação de grade entre duas grades.



Considerações e requisitos para conexões de federação de grade

- As grades usadas para federação de grade devem estar executando versões do StorageGRID que são idênticas ou não têm mais de uma diferença de versão principal entre elas.

  Para obter detalhes sobre os requisitos de versão, consulte o "Notas de lançamento".

- Uma grade pode ter uma ou mais conexões de federação de grade para outras grades. Cada conexão de federação de grade é independente de quaisquer outras conexões. Por exemplo, se o Grid 1 tiver uma conexão com o Grid 2 e uma segunda conexão com o Grid 3, não haverá conexão implícita entre o Grid 2 e o Grid 3.
- As conexões de federação de grade são bidirecionais. Após a conexão ser estabelecida, você pode monitorar e gerenciar a conexão a partir de qualquer grade.
- Deve existir pelo menos uma ligação de federação de grelha antes de poder utilizar "clone de conta" ou "replicação entre grade".

Requisitos de rede e endereço IP

- As conexões de federação de grade podem ocorrer na rede de grade, na rede de administração ou na rede de cliente.
- Uma conexão de federação de grade coneta uma grade a outra grade. A configuração para cada grade especifica um ponto de extremidade de federação de grade na outra grade que consiste em nós de administrador, nós de gateway ou ambos.
- A prática recomendada é conetar "Grupos de alta disponibilidade (HA)" os nós Gateway e Admin em cada

grade. O uso de grupos de HA ajuda a garantir que as conexões de federação de grade permaneçam on-line se os nós ficarem indisponíveis. Se a interface ativa em qualquer um dos grupos HA falhar, a conexão poderá usar uma interface de backup.

- Não é recomendável criar uma conexão de federação de grade que use o endereço IP de um único nó de administrador ou nó de gateway. Se o nó ficar indisponível, a conexão de federação de grade também ficará indisponível.
- "Replicação entre grade" De objetos requer que os nós de storage em cada grade possam acessar os nós de administrador e gateway configurados na outra grade. Para cada grade, confirme se todos os nós de storage têm uma rota de largura de banda alta como nós de administrador ou nós de gateway usados para a conexão.

Use FQDNs para equilibrar a conexão de carga

Para um ambiente de produção, use nomes de domínio totalmente qualificados (FQDNs) para identificar cada grade na conexão. Em seguida, crie as entradas de DNS apropriadas, da seguinte forma:

- O FQDN para a Grade 1 mapeou um ou mais endereços IP virtuais (VIP) para grupos de HA na Grade 1 ou para o endereço IP de um ou mais nós de Admin ou Gateway na Grade 1.
- O FQDN para a Grade 2 mapeou um ou mais endereços VIP para a Grade 2 ou para o endereço IP de um ou mais nós de Admin ou Gateway na Grade 2.

Quando você usa várias entradas de DNS, as solicitações para usar a conexão são balanceadas de carga, da seguinte forma:

- As entradas DNS que mapeiam para os endereços VIP de vários grupos de HA são balanceadas de carga entre os nós ativos nos grupos de HA.
- As entradas DNS que mapeiam para os endereços IP de vários nós de administração ou nós de gateway são balanceadas de carga entre os nós mapeados.

Requisitos portuários

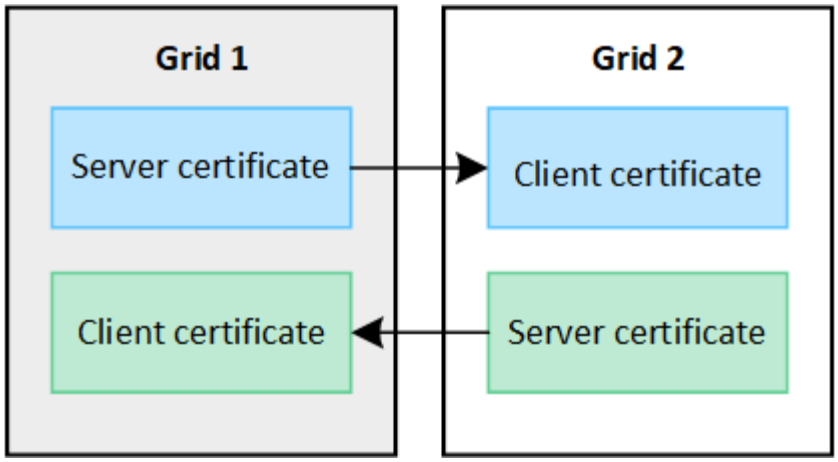
Ao criar uma conexão de federação de grade, você pode especificar qualquer número de porta não utilizado de 23000 a 23999. Ambas as grades nesta conexão usarão a mesma porta.

Você deve garantir que nenhum nó em qualquer grade use essa porta para outras conexões.

Requisitos de certificado

Quando você configura uma conexão de federação de grade, o StorageGRID gera automaticamente quatro certificados SSL:

- Certificados de servidor e cliente para autenticar e criptografar informações enviadas da grade 1 para a grade 2
- Certificados de servidor e cliente para autenticar e criptografar informações enviadas da grade 2 para a grade 1



Por padrão, os certificados são válidos por 730 dias (2 anos). Quando esses certificados estiverem próximos da data de expiração, o alerta **Expiration of Grid Federation certificate** lembra que você deve girar os certificados, o que você pode fazer usando o Grid Manager.

> Se os certificados em qualquer uma das extremidades da conexão expirarem, a conexão deixará de funcionar. A replicação de dados ficará pendente até que os certificados sejam atualizados.

Saiba mais

- "Crie conexões de federação de grade"
- "Gerenciar conexões de federação de grade"
- "Solucionar erros de federação de grade"

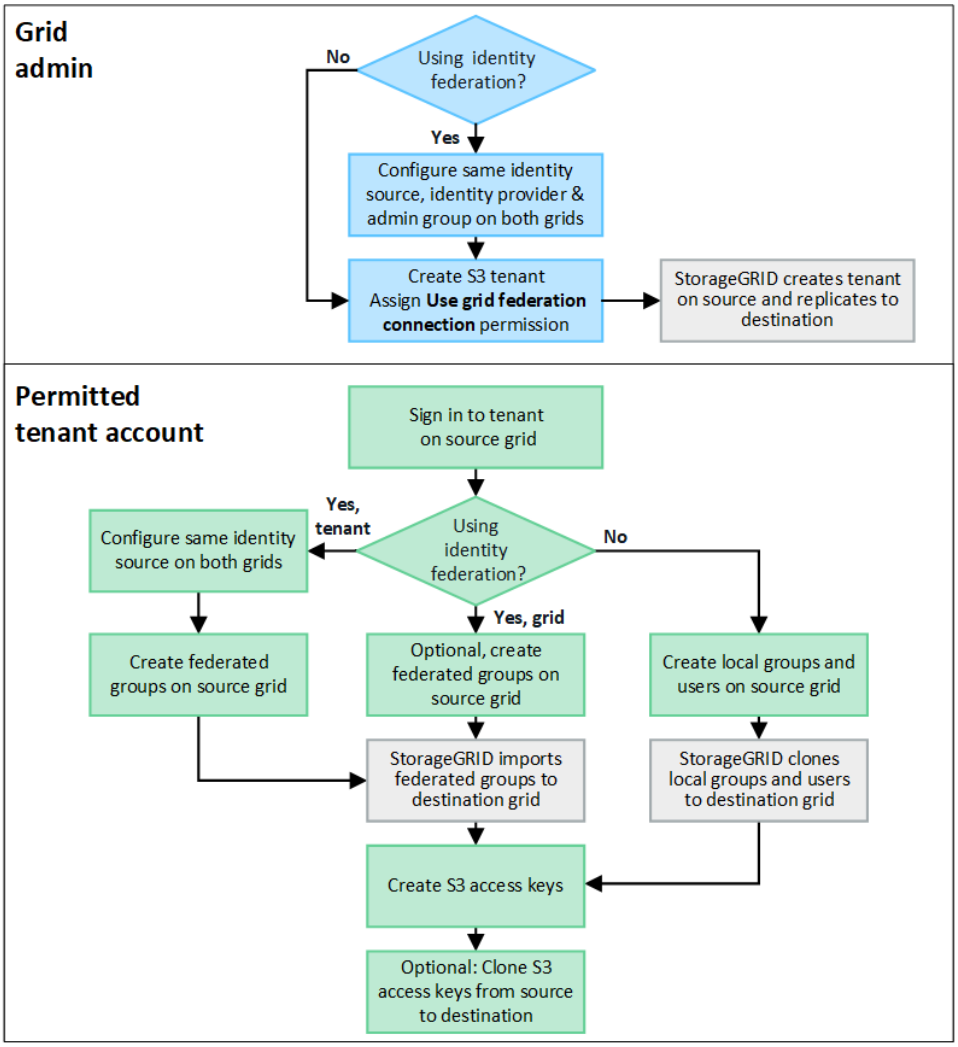
O que é o clone de conta?

O clone de conta é a replicação automática de uma conta de locatário, grupos de locatários, usuários de locatários e, opcionalmente, chaves de acesso S3 entre os sistemas StorageGRID em um "conexão de federação de grade".

O clone de conta é necessário para "replicação entre grade"o . Clonar informações de conta de um sistema StorageGRID de origem para um sistema StorageGRID de destino garante que usuários e grupos de locatários possam acessar os buckets e objetos correspondentes em qualquer grade.

Fluxo de trabalho para clone de conta

O diagrama de fluxo de trabalho mostra as etapas que administradores de grade e locatários permitidos executarão para configurar o clone de conta. Estas etapas são executadas após o "a conexão de federação de grade está configurada".



Fluxo de trabalho de administração de grade

As etapas que os administradores de grade executam dependem se os sistemas StorageGRID na "conexão de federação de grade"federação usar logon único (SSO) ou identidade.

Configurar SSO para o clone de conta (opcional)

Se qualquer um dos sistemas StorageGRID na conexão de federação de grade usar SSO, ambas as grades devem usar SSO. Antes de criar as contas de locatário para federação de grade, os administradores de grade para as grades de origem e destino do locatário devem executar essas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grades. "Use a federação de identidade"Consulte .
2. Configure o mesmo provedor de identidade SSO (IDP) para ambas as grades. "Configurar o logon único"Consulte .
3. "Crie o mesmo grupo de administração" em ambas as grades importando o mesmo grupo federado.

   Ao criar o locatário, você selecionará esse grupo para ter a permissão de acesso raiz inicial para as contas de locatário de origem e destino.

Se esse grupo de administração não existir em ambas as grades antes de criar o locatário, o locatário não será replicado para o destino.

Configurar federação de identidade em nível de grade para o clone de conta (opcional)

Se um dos sistemas StorageGRID usar federação de identidade sem SSO, ambas as grades devem usar federação de identidade. Antes de criar as contas de locatário para federação de grade, os administradores de grade para as grades de origem e destino do locatário devem executar essas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grades. "Use a federação de identidade"Consulte .
2. Opcionalmente, se um grupo federado tiver permissão de acesso raiz inicial para as contas de locatário de origem e destino, "crie o mesmo grupo de administração" em ambas as grades importando o mesmo grupo federado.

   Se você atribuir permissão de acesso root a um grupo federado que não existe em ambas as grades, o locatário não será replicado para a grade de destino.

3. Se você não quiser que um grupo federado tenha permissão de acesso raiz inicial para ambas as contas, especifique uma senha para o usuário raiz local.

Crie uma conta de locatário S3 permitida

Depois de configurar opcionalmente o SSO ou a federação de identidade, um administrador de grade executa essas etapas para determinar quais locatários podem replicar objetos de bucket para outros sistemas StorageGRID.

Passos

1. Determine qual grade você deseja ser a grade de origem do locatário para operações de clone de conta.

   A grade onde o locatário é originalmente criado é conhecida como *source grid* do locatário. A grade onde o locatário é replicado é conhecida como *grade de destino* do locatário.

2. Nessa grade, crie uma nova conta de locatário do S3 ou edite uma conta existente.
3. Atribua a permissão **Use Grid Federation Connection**.
4. Se a conta de locatário gerenciar seus próprios usuários federados, atribua a permissão **Use own Identity source**.

   Se essa permissão for atribuída, as contas de locatário de origem e destino deverão configurar a mesma fonte de identidade antes de criar grupos federados. Os grupos federados adicionados ao locatário de origem não podem ser clonados para o locatário de destino, a menos que ambas as grades usem a mesma fonte de identidade.

5. Selecione uma conexão de federação de grade específica.
6. Salve o locatário novo ou modificado.

   Quando um novo locatário com a permissão **usar conexão de federação de grade** é salvo, o StorageGRID cria automaticamente uma réplica desse locatário na outra grade, da seguinte forma:

   - Ambas as contas de inquilino têm o mesmo ID de conta, nome, cota de armazenamento e permissões atribuídas.

- Se você selecionou um grupo federado para ter permissão de acesso root para o locatário, esse grupo será clonado para o locatário de destino.
- Se você selecionou um usuário local para ter permissão de acesso root para o locatário, esse usuário será clonado para o locatário de destino. No entanto, a senha para esse usuário não é clonada.

Para obter detalhes, "Gerenciar locatários permitidos para federação de grade"consulte .

Fluxo de trabalho de conta de locatário permitido

Depois que um locatário com a permissão **usar conexão de federação de grade** for replicado para a grade de destino, as contas de locatário permitidas podem executar essas etapas para clonar grupos de locatários, usuários e chaves de acesso S3.

Passos

1. Faça login na conta do locatário na grade de origem do locatário.
2. Se permitido, configure a federação de identificação nas contas de locatário de origem e destino.
3. Crie grupos e usuários no locatário de origem.

   Quando novos grupos ou usuários são criados no locatário de origem, o StorageGRID os clonará automaticamente para o locatário de destino, mas nenhuma clonagem ocorre do destino de volta para a origem.

4. Crie S3 chaves de acesso.
5. Opcionalmente, clone chaves de acesso S3 do locatário de origem para o locatário de destino.

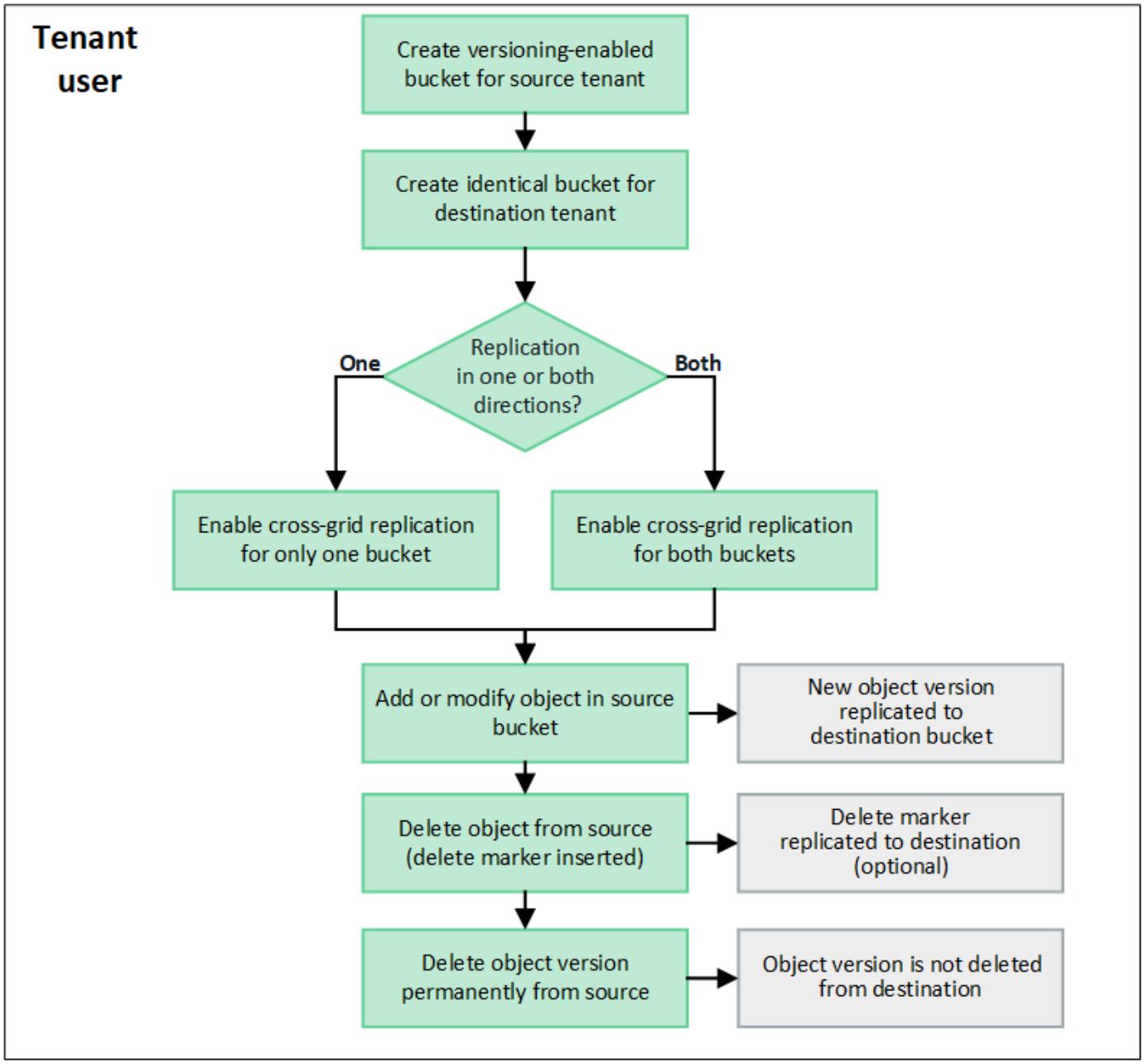
Para obter detalhes sobre o fluxo de trabalho permitido da conta de locatário e saber como grupos, usuários e chaves de acesso S3 são clonados, "Clonar grupos de locatários e usuários"consulte e "Clonar chaves de acesso S3 usando a API".

O que é replicação entre redes?

A replicação entre grade é a replicação automática de objetos entre buckets S3 selecionados em dois sistemas StorageGRID que estão conetados em um "conexão de federação de grade". "Clone de conta" é necessário para replicação entre grades.

Fluxo de trabalho para replicação entre grades

O diagrama de fluxo de trabalho resume as etapas para configurar a replicação entre grades entre intervalos em duas grades.



Requisitos para replicação entre grades

Se uma conta de locatário tiver a permissão **usar conexão de federação de grade** para usar um ou mais "conexões de federação de grade", um usuário de locatário com permissão de acesso root poderá criar buckets idênticos nas contas de locatário correspondentes em cada grade. Estes baldes:

- Deve ter o mesmo nome, mas pode ter regiões diferentes
- Deve ter o controle de versão habilitado
- Tem de ter o bloqueio de objetos S3 desativado
- Deve estar vazio

Depois que ambos os buckets tiverem sido criados, a replicação entre grades pode ser configurada para um ou ambos os buckets.

Saiba mais

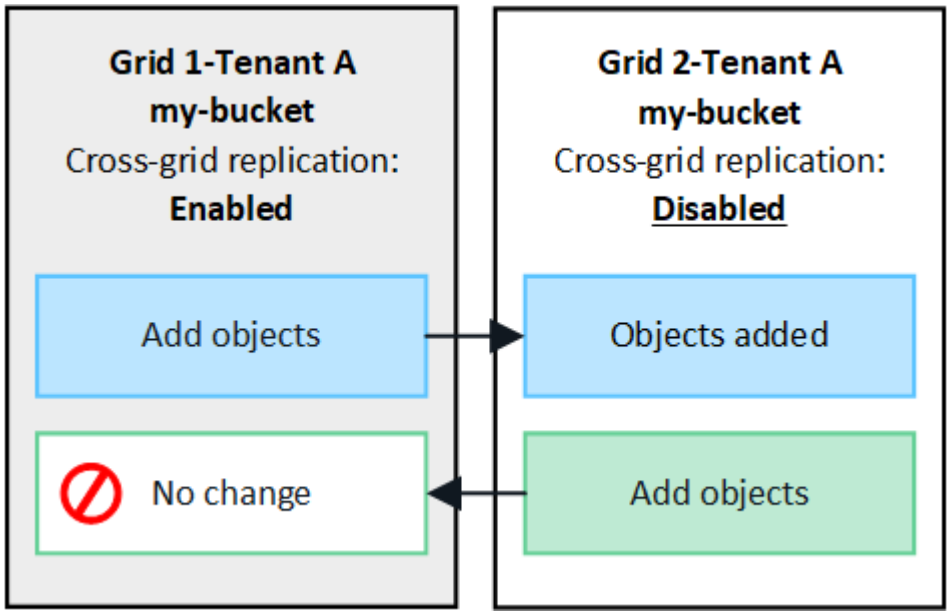
"Gerenciar a replicação entre grades"

Como a replicação entre redes funciona

A replicação entre grades pode ser configurada para ocorrer em uma direção ou em ambas as direções.

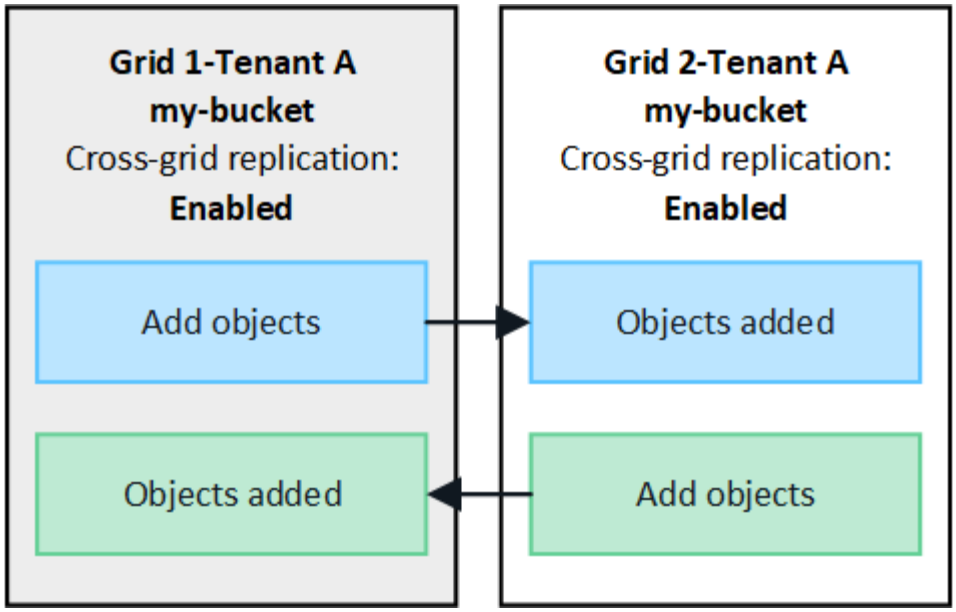
Replicação em uma direção

Se você habilitar a replicação entre grade para um bucket em apenas uma grade, os objetos adicionados a esse bucket (o bucket de origem) serão replicados para o bucket correspondente na outra grade (o bucket de destino). No entanto, os objetos adicionados ao intervalo de destino não são replicados de volta para a origem. Na figura, a replicação de grade cruzada é ativada para `my-bucket` da grade 1 para a grade 2, mas não é ativada na outra direção.



Replicação em ambas as direções

Se você habilitar a replicação entre grade para o mesmo bucket em ambas as grades, os objetos adicionados a qualquer bucket serão replicados para a outra grade. Na figura, a replicação em grade cruzada é ativada para `my-bucket` em ambas as direções.



O que acontece quando os objetos são ingeridos?

Quando um cliente S3 adiciona um objeto a um bucket que tem replicação entre grades ativada, o seguinte acontece:

1. O StorageGRID replica automaticamente o objeto do bucket de origem para o bucket de destino. O tempo para executar essa operação de replicação em segundo plano depende de vários fatores, incluindo o número de outras operações de replicação pendentes.

   O cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação GetObject ou HeadObject. A resposta inclui um cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores: O cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação GetObject ou HeadObject. A resposta inclui um cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grelha	Estado da replicação
Fonte	• **COMPLETED**: A replicação foi bem-sucedida para todas as conexões de grade. • **PENDENTE**: O objeto não foi replicado para pelo menos uma conexão de grade. • **FAILURE**: A replicação não está pendente para qualquer conexão de grade e pelo menos uma falha permanente. Um usuário deve resolver o erro.
Destino	• RÉPLICA*: O objeto foi replicado a partir da grade de origem.

   > O StorageGRID não suporta o `x-amz-replication-status` colhedor.

2. O StorageGRID usa as políticas de ILM ativas de cada grade para gerenciar os objetos, assim como qualquer outro objeto. Por exemplo, Objeto A na Grade 1 pode ser armazenado como duas cópias replicadas e retido para sempre, enquanto a cópia do Objeto A que foi replicado para a Grade 2 pode ser

armazenada usando codificação de apagamento 2-1 e excluída após três anos.

O que acontece quando os objetos são excluídos?

Conforme descrito "Eliminar fluxo de dados"no , o StorageGRID pode excluir um objeto por qualquer um destes motivos:

- O cliente S3 emite uma solicitação de exclusão.
- Um usuário do Tenant Manager seleciona a "Excluir objetos no bucket" opção para remover todos os objetos de um bucket.
- O bucket tem uma configuração de ciclo de vida, que expira.
- O último período de tempo na regra ILM para o objeto termina, e não há mais colocações especificadas.

Quando o StorageGRID exclui um objeto devido a uma operação Excluir objetos na operação de bucket, expiração do ciclo de vida do bucket ou expiração do posicionamento do ILM, o objeto replicado nunca é excluído da outra grade em uma conexão de federação de grade. No entanto, os marcadores de exclusão adicionados ao bucket de origem por exclusões do cliente S3 podem ser replicados opcionalmente para o bucket de destino.

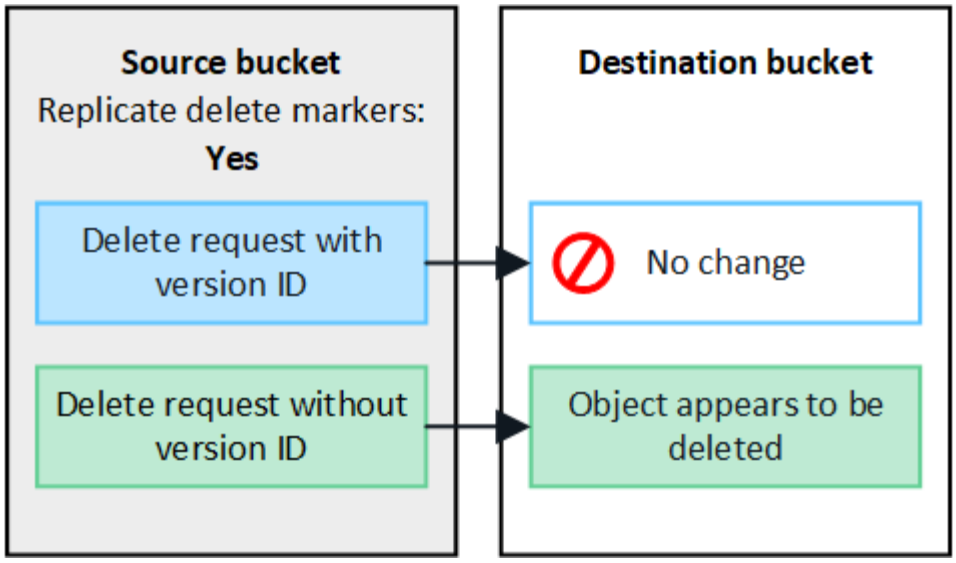
Para entender o que acontece quando um cliente S3 exclui objetos de um bucket que tem replicação entre grade ativada, revise como os clientes S3 excluem objetos de buckets que têm o controle de versão ativado, da seguinte forma:

- Se um cliente S3 emitir uma solicitação de exclusão que inclua um ID de versão, essa versão do objeto será removida permanentemente. Nenhum marcador de eliminação é adicionado ao balde.
- Se um cliente S3 emitir uma solicitação de exclusão que não inclua um ID de versão, o StorageGRID não exclui nenhuma versão de objeto. Em vez disso, ele adiciona um marcador de exclusão ao intervalo. O marcador de exclusão faz com que o StorageGRID atue como se o objeto fosse excluído:
  - Uma solicitação GetObject sem um ID de versão falhará `404 No Object Found`
  - Uma solicitação GetObject com um ID de versão válido será bem-sucedida e retornará a versão do objeto solicitada.

Quando um cliente S3 exclui um objeto de um bucket que tem replicação entre grade ativada, o StorageGRID determina se deve replicar a solicitação de exclusão para o destino, da seguinte forma:

- Se a solicitação de exclusão incluir um ID de versão, essa versão do objeto será removida permanentemente da grade de origem. No entanto, o StorageGRID não replica solicitações de exclusão que incluem um ID de versão, portanto, a mesma versão do objeto não é excluída do destino.
- Se a solicitação de exclusão não incluir um ID de versão, o StorageGRID poderá, opcionalmente, replicar o marcador de exclusão, com base na configuração da replicação entre grade para o bucket:
  - Se você optar por replicar marcadores de exclusão (padrão), um marcador de exclusão será adicionado ao intervalo de origem e replicado ao intervalo de destino. Na verdade, o objeto parece ser excluído em ambas as grades.
  - Se você optar por não replicar marcadores de exclusão, um marcador de exclusão será adicionado ao intervalo de origem, mas não será replicado para o intervalo de destino. Com efeito, os objetos que são excluídos na grade de origem não são excluídos na grade de destino.

Na figura, **Replicate DELETE markers** foi definido como **Yes** quando "a replicação entre redes foi ativada". Excluir solicitações para o bucket de origem que inclua um ID de versão não excluirá objetos do bucket de destino. Excluir solicitações para o bucket de origem que não inclua um ID de versão aparecerão para excluir objetos no bucket de destino.



Se você quiser manter as exclusões de objetos sincronizadas entre grades, crie correspondentes "Configurações do ciclo de vida do S3" para os buckets em ambas as grades.

Como os objetos criptografados são replicados

Quando você usa replicação entre grade para replicar objetos entre grades, é possível criptografar objetos individuais, usar criptografia de bucket padrão ou configurar criptografia em toda a grade. Você pode adicionar, modificar ou remover configurações padrão de intervalo ou criptografia em toda a grade antes ou depois de ativar a replicação entre grade para um bucket.

Para criptografar objetos individuais, você pode usar SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID) ao adicionar os objetos ao bucket de origem. Use o `x-amz-server-side-encryption` cabeçalho da solicitação e `AES256` especifique . "Use a criptografia do lado do servidor"Consulte .

O uso do SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente) não é suportado para replicação entre grades. A operação de ingestão falhará.

Para usar a criptografia padrão para um bucket, use uma solicitação PutBucketEncryption e defina o `SSEAlgorithm` parâmetro como `AES256`. A criptografia no nível do bucket aplica-se a quaisquer objetos ingeridos sem o `x-amz-server-side-encryption` cabeçalho da solicitação. "Operações em baldes"Consulte .

Para usar criptografia no nível da grade, defina a opção **Stored Object Encryption** como **AES-256**. A criptografia no nível da grade se aplica a quaisquer objetos que não sejam criptografados no nível do bucket ou que sejam ingeridos sem o `x-amz-server-side-encryption` cabeçalho da solicitação. "Configure as opções de rede e objeto"Consulte .

SSE não suporta AES-128. Se a opção **Stored Object Encryption** estiver ativada para a grade de origem usando a opção **AES-128**, o uso do algoritmo AES-128 não será propagado para o objeto replicado. Em vez disso, o objeto replicado usará o intervalo padrão do destino ou a configuração de criptografia em nível de grade, se disponível.

Ao determinar como criptografar objetos de origem, o StorageGRID aplica estas regras:

1. Use o `x-amz-server-side-encryption` cabeçalho de ingestão, se presente.
2. Se um cabeçalho de ingestão não estiver presente, use a configuração de criptografia padrão do intervalo, se configurado.
3. Se uma configuração de intervalo não estiver configurada, use a configuração de criptografia em toda a grade, se configurada.
4. Se uma configuração em toda a grade não estiver presente, não criptografe o objeto de origem.

Ao determinar como criptografar objetos replicados, o StorageGRID aplica essas regras nesta ordem:

1. Use a mesma criptografia que o objeto de origem, a menos que esse objeto use criptografia AES-128.
2. Se o objeto de origem não estiver criptografado ou usar AES-128, use a configuração de criptografia padrão do bucket de destino, se configurado.
3. Se o intervalo de destino não tiver uma configuração de criptografia, use a configuração de criptografia em toda a grade do destino, se configurada.
4. Se uma configuração em toda a grade não estiver presente, não criptografe o objeto de destino.

PutObjectTagging e DeleteObjectTagging não são suportados

As solicitações PutObjectTagging e DeleteObjectTagging não são suportadas para objetos em buckets que têm replicação entre grade ativada.

Se um cliente S3 emitir uma solicitação PutObjectTagging ou DeleteObjectTagging, `501 Not Implemented` será retornado. A mensagem é `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`.

Como os objetos segmentados são replicados

O tamanho máximo do segmento da grade de origem aplica-se a objetos replicados na grade de destino. Quando os objetos são replicados para outra grade, a configuração **tamanho máximo do segmento** (**CONFIGURATION** > **System** > **Storage options**) da grade de origem será usada em ambas as grades. Por exemplo, suponha que o tamanho máximo do segmento para a grade de origem seja de 1 GB, enquanto o tamanho máximo do segmento da grade de destino é de 50 MB. Se você ingerir um objeto de 2 GB na grade de origem, esse objeto será salvo como dois segmentos de 1 GB. Ele também será replicado para a grade de destino como dois segmentos de 1 GB, mesmo que o tamanho máximo do segmento da grade seja de 50 MB.

Compare a replicação entre redes e a replicação do CloudMirror

À medida que você começar a usar a federação de grade, revise as semelhanças e as diferenças entre "replicação entre grade" e o "Serviço de replicação do StorageGRID CloudMirror".

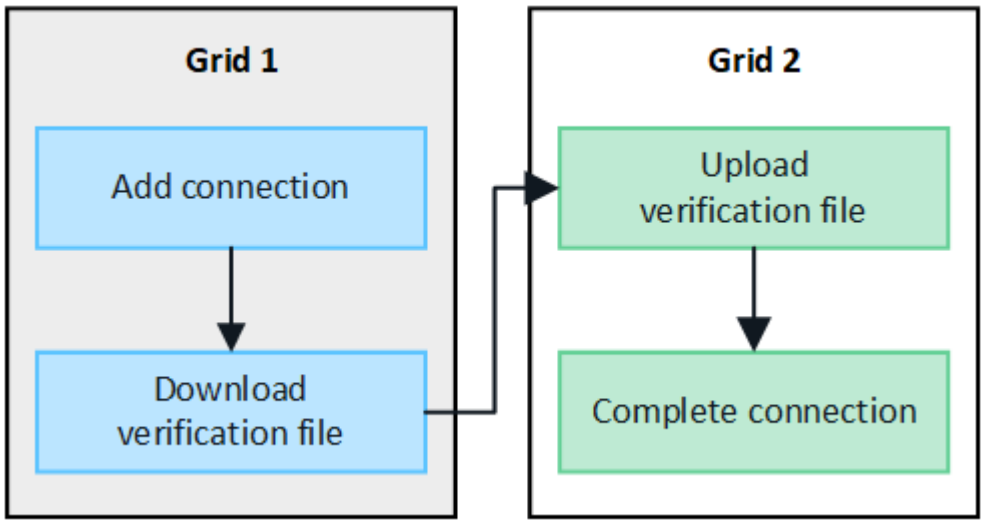
	Replicação entre grade	Serviço de replicação do CloudMirror
Qual é o objetivo principal?	Um sistema StorageGRID atua como um sistema de recuperação de desastres. Os objetos em um bucket podem ser replicados entre as grades em uma ou ambas as direções.	Permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket externo do S3 (destino). A replicação do CloudMirror cria uma cópia independente de um objeto em uma infraestrutura S3 independente. Essa cópia independente não é usada como backup, mas muitas vezes processada na nuvem.
Como é configurado?	1. Configure uma conexão de federação de grade entre duas grades. 2. Adicione novas contas de inquilino, que são clonadas automaticamente para a outra grade. 3. Adicione novos grupos de inquilinos e usuários, que também são clonados. 4. Crie buckets correspondentes em cada grade e permita que a replicação entre grade ocorra em uma ou ambas as direções.	1. Um usuário de locatário configura a replicação do CloudMirror definindo um endpoint do CloudMirror (endereço IP, credenciais, etc.) usando o Gerenciador do Tenant ou a API S3. 2. Qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o endpoint do CloudMirror.
Quem é responsável por montá-lo?	• Um administrador de grade configura a conexão e os locatários. • Os usuários do locatário configuram os grupos, usuários, chaves e buckets.	Normalmente, um usuário locatário.
Qual é o destino?	Um bucket S3 correspondente e idêntico no outro sistema StorageGRID na conexão de federação de grade.	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3). • Google Cloud Platform (GCP)
O controle de versão do objeto é necessário?	Sim, os buckets de origem e destino devem ter o controle de versão de objetos habilitado.	Não, a replicação do CloudMirror suporta qualquer combinação de buckets não versionados e versionados na origem e no destino.
O que faz com que os objetos sejam movidos para o destino?	Os objetos são replicados automaticamente quando são adicionados a um bucket que tem replicação entre grade ativada.	Os objetos são replicados automaticamente quando são adicionados a um bucket que foi configurado com um endpoint do CloudMirror. Os objetos que existiam no bucket de origem antes do bucket ser configurado com o endpoint do CloudMirror não são replicados, a menos que sejam modificados.

	Replicação entre grade	Serviço de replicação do CloudMirror
Como os objetos são replicados?	A replicação entre grade cria objetos com controle de versão e replica o ID da versão do bucket de origem para o bucket de destino. Isso permite que a ordem da versão seja mantida em ambas as grades.	A replicação do CloudMirror não requer buckets habilitados para controle de versão, portanto, o CloudMirror só pode manter o pedido de uma chave em um site. Não há garantias de que o pedido será mantido para pedidos para um objeto em local diferente.
E se um objeto não puder ser replicado?	O objeto está na fila para replicação, sujeito aos limites de armazenamento de metadados.	O objeto está na fila para replicação, sujeito aos limites dos serviços da plataforma ("Recomendações para o uso de serviços de plataforma"consulte).
Os metadados do sistema do objeto são replicados?	Sim, quando um objeto é replicado para a outra grade, seus metadados do sistema também são replicados. Os metadados serão idênticos em ambas as grades.	Não, quando um objeto é replicado para o bucket externo, seus metadados do sistema são atualizados. Os metadados diferem entre locais, dependendo do tempo de ingestão e do comportamento da infraestrutura independente do S3.
Como os objetos são recuperados?	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação para o bucket em qualquer grade.	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação para StorageGRID ou para o destino S3. Por exemplo, suponha que você use a replicação do CloudMirror para espelhar objetos em uma organização parceira. O parceiro pode usar seus próprios aplicativos para ler ou atualizar objetos diretamente do destino S3. Não é necessário utilizar o StorageGRID.
O que acontece se um objeto for excluído?	• As solicitações de exclusão que incluem um ID de versão nunca são replicadas para a grade de destino. • Excluir solicitações que não incluem um ID de versão adicionam um marcador de exclusão ao bucket de origem, que pode ser replicado opcionalmente para a grade de destino. • Se a replicação entre grades for configurada para apenas uma direção, os objetos no intervalo de destino podem ser excluídos sem afetar a origem.	Os resultados variam de acordo com o estado de versionamento dos intervalos de origem e destino (que não precisam ser os mesmos): • Se ambos os buckets forem versionados, uma solicitação de exclusão adicionará um marcador de exclusão em ambos os locais. • Se apenas o intervalo de origem for versionado, uma solicitação de exclusão adicionará um marcador de exclusão à origem, mas não ao destino. • Se nenhum intervalo for versionado, uma solicitação de exclusão excluirá o objeto da origem, mas não do destino. Da mesma forma, os objetos no intervalo de destino podem ser excluídos sem afetar a origem.

Crie conexões de federação de grade

Você pode criar uma conexão de federação de grade entre dois sistemas StorageGRID se quiser clonar detalhes do locatário e replicar dados de objeto.

Como mostrado na figura, a criação de uma conexão de federação de grade inclui etapas em ambas as grades. Você adiciona a conexão em uma grade e a completa na outra grade. Você pode começar a partir de qualquer grade.



Antes de começar

- Você revisou o "considerações e requisitos" para configurar conexões de federação de grade.
- Se você planeja usar nomes de domínio totalmente qualificados (FQDNs) para cada grade em vez de endereços IP ou VIP, você sabe quais nomes usar e confirmou que o servidor DNS para cada grade tem as entradas apropriadas.
- Você está usando um "navegador da web suportado".
- Você tem permissão de acesso raiz e a senha de provisionamento para ambas as grades.

Adicionar ligação

Execute estas etapas em um dos dois sistemas StorageGRID.

Passos

1. Faça login no Gerenciador de Grade a partir do nó Admin primário em qualquer grade.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione **Adicionar conexão**.
4. Introduza os detalhes da ligação.

Campo	Descrição
Nome da ligação	Um nome exclusivo para ajudá-lo a reconhecer esta conexão, por exemplo, "Grid 1-Grid 2".

Campo	Descrição
FQDN ou IP para esta grade	Uma das seguintes opções: • O FQDN da grade em que você está conetado atualmente • Um endereço VIP de um grupo HA nesta grelha • Um endereço IP de um nó de administrador ou nó de gateway nesta grade. O IP pode estar em qualquer rede que a grade de destino possa alcançar.
Porta	A porta que pretende utilizar para esta ligação. Pode introduzir qualquer número de porta não utilizado de 23000 a 23999. Ambas as grades nesta conexão usarão a mesma porta. Você deve garantir que nenhum nó em qualquer grade use essa porta para outras conexões.
Certificado dias válidos para esta grade	O número de dias que deseja que os certificados de segurança para essa grade na conexão sejam válidos. O valor padrão é de 730 dias (2 anos), mas você pode inserir qualquer valor de 1 a 762 dias. O StorageGRID gera automaticamente certificados de cliente e servidor para cada grade quando você salva a conexão.
Frase-passe de aprovisionamento para esta grelha	A senha de provisionamento para a grade à qual você está conetado.
FQDN ou IP para a outra grade	Uma das seguintes opções: • O FQDN da grade à qual você deseja se conetar • Um endereço VIP de um grupo HA na outra grade • Um endereço IP de um nó de administrador ou nó de gateway na outra grade. O IP pode estar em qualquer rede que a grade de origem possa alcançar.

5. Selecione **Salvar e continuar**.
6. Para a etapa Download do arquivo de verificação, selecione **Download do arquivo de verificação**.

   Depois que a conexão for concluída na outra grade, você não poderá mais baixar o arquivo de verificação de qualquer grade.

7. Localize o arquivo baixado (*`connection-name`*`.grid-federation`) e salve-o em um local seguro.

   Este arquivo contém segredos (mascarados como *****) e outros detalhes sensíveis e deve ser armazenado e transmitido com segurança.

8. Selecione **Fechar** para retornar à página de federação de Grade.
9. Confirme se a nova ligação é apresentada e que o seu **Estado da ligação** é **a aguardar ligação**.

10. Forneça o *connection-name*`.grid-federation` arquivo ao administrador de grade para a outra grade.

Ligação completa

Execute estas etapas no sistema StorageGRID ao qual você está se conetando (a outra grade).

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione **carregar ficheiro de verificação** para aceder à página carregar.
4. Selecione **carregar ficheiro de verificação**. Em seguida, procure e selecione o arquivo que foi baixado da primeira grade (*connection-name*`.grid-federation`).

   São apresentados os detalhes da ligação.

5. Opcionalmente, insira um número diferente de dias válidos para os certificados de segurança para esta grade. A entrada **Certificate Valid Days** (dias válidos do certificado*) é padrão para o valor inserido na primeira grade, mas cada grade pode usar datas de expiração diferentes.

   Em geral, use o mesmo número de dias para os certificados em ambos os lados da conexão.

   > Se os certificados em qualquer uma das extremidades da conexão expirarem, a conexão parará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

6. Insira a senha de provisionamento para a grade à qual você está conetado no momento.
7. Selecione **Salvar e testar**.

   Os certificados são gerados e a conexão é testada. Se a conexão for válida, uma mensagem de sucesso será exibida e a nova conexão será listada na página de federação de Grade. O **Estado da ligação** será **ligado**.

   Se uma mensagem de erro for exibida, solucione quaisquer problemas. "Solucionar erros de federação de grade"Consulte .

8. Vá para a página de federação de Grade na primeira grade e atualize o navegador. Confirme se o **Estado da ligação** é agora **ligado**.
9. Depois que a conexão for estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

   Se editar esta ligação, será criado um novo ficheiro de verificação. O arquivo original não pode ser reutilizado.

Depois de terminar

- Reveja as considerações para "gerenciamento de inquilinos permitidos".
- "Crie uma ou mais novas contas de inquilino", Atribua a permissão **Use Grid Federation Connection** e selecione a nova conexão.
- "Gerencie a conexão" conforme necessário. Você pode editar valores de conexão, testar uma conexão, girar certificados de conexão ou remover uma conexão.

- "Monitorize a ligação" Como parte de suas atividades normais de monitoramento do StorageGRID.
- "Solucionar problemas da conexão", incluindo a resolução de quaisquer alertas e erros relacionados ao clone de conta e replicação entre grades.

Gerenciar conexões de federação de grade

O gerenciamento de conexões de federação de grade entre sistemas StorageGRID inclui edição de detalhes de conexão, rotação de certificados, remoção de permissões de locatário e remoção de conexões não utilizadas.

Antes de começar

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

Editar uma conexão de federação de grade

Você pode editar uma conexão de federação de grade entrando no nó de administração principal em qualquer grade da conexão. Depois de fazer alterações na primeira grade, você deve baixar um novo arquivo de verificação e enviá-lo para a outra grade.

> Enquanto a conexão está sendo editada, as solicitações de replicação entre redes ou clone de conta continuarão a usar as configurações de conexão existentes. Todas as edições feitas na primeira grade são salvas localmente, mas não são usadas até que tenham sido carregadas na segunda grade, salvas e testadas.

Comece a editar a ligação

Passos

1. Faça login no Gerenciador de Grade a partir do nó Admin primário em qualquer grade.
2. Selecione **NÓS** e confirme se todos os outros nós de administrador do sistema estão online.

> Quando você edita uma conexão de federação de grade, o StorageGRID tenta salvar um arquivo de "configuração de candidato" em todos os nós de administração na primeira grade. Se esse arquivo não puder ser salvo em todos os nós de administração, uma mensagem de aviso será exibida quando você selecionar **Salvar e testar**.

3. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
4. Edite os detalhes da conexão usando o menu **ações** na página de federação de Grade ou a página de detalhes de uma conexão específica. Consulte "Crie conexões de federação de grade" para saber o que introduzir.

Menu ações

a. Selecionar o botão do rádio para a ligação.
b. Selecione **ações** > **Editar**.
c. Introduza as novas informações.

Página de detalhes

a. Selecione um nome de ligação para apresentar os respetivos detalhes.
b. Selecione **Editar**.
c. Introduza as novas informações.

5. Insira a senha de provisionamento para a grade à qual você está conetado.
6. Selecione **Salvar e continuar**.

   Os novos valores são salvos, mas eles não serão aplicados à conexão até que você tenha carregado o novo arquivo de verificação na outra grade.

7. Selecione **Transferir ficheiro de verificação**.

   Para transferir este ficheiro posteriormente, aceda à página de detalhes da ligação.

8. Localize o arquivo baixado (*connection-name*`.grid-federation`) e salve-o em um local seguro.

   O arquivo de verificação contém segredos e deve ser armazenado e transmitido com segurança.

9. Selecione **Fechar** para retornar à página de federação de Grade.
10. Confirme se o **Status da conexão** é **Pending edit**.

    Se o status da conexão for diferente de **conectado** quando você começou a editar a conexão, ela não mudará para **Pending edit**.

11. Forneça o *connection-name*`.grid-federation` arquivo ao administrador de grade para a outra grade.

Termine a edição da conexão

Termine a edição da conexão carregando o arquivo de verificação na outra grade.

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione **carregar ficheiro de verificação** para aceder à página de carregamento.
4. Selecione **carregar ficheiro de verificação**. Em seguida, procure e selecione o arquivo que foi baixado da primeira grade.
5. Insira a senha de provisionamento para a grade à qual você está conetado no momento.
6. Selecione **Salvar e testar**.

Se a conexão puder ser estabelecida usando os valores editados, uma mensagem de sucesso será exibida. Caso contrário, é apresentada uma mensagem de erro. Revise a mensagem e solucione quaisquer problemas.

7. Feche o assistente para retornar à página de federação de Grade.
8. Confirme se o **Estado da ligação** é **ligado**.
9. Vá para a página de federação de Grade na primeira grade e atualize o navegador. Confirme se o **Estado da ligação** é agora **ligado**.
10. Depois que a conexão for estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

Teste uma conexão de federação de grade

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Teste a conexão usando o menu **ações** na página de federação de Grade ou a página de detalhes para uma conexão específica.

Menu ações

a. Selecionar o botão do rádio para a ligação.

b. Selecione **ações** > **Teste**.

Página de detalhes

a. Selecione um nome de ligação para apresentar os respetivos detalhes.

b. Selecione **Test Connection**.

4. Reveja o estado da ligação:

Estado da ligação	Descrição
Ligado	Ambas as grades estão conetadas e se comunicando normalmente.
Erro	A conexão está em um estado de erro. Por exemplo, um certificado expirou ou um valor de configuração não é mais válido.
Edição pendente	Você editou a conexão nesta grade, mas a conexão ainda está usando a configuração existente. Para concluir a edição, carregue o novo arquivo de verificação para a outra grade.
A aguardar ligação	Você configurou a conexão nesta grade, mas a conexão não foi concluída na outra grade. Baixe o arquivo de verificação desta grade e faça o upload para a outra grade.
Desconhecido	A conexão está em um estado desconhecido, possivelmente por causa de um problema de rede ou um nó off-line.

5. Se o status da conexão for **Error**, resolva quaisquer problemas. Em seguida, selecione **Test Connection** novamente para confirmar que o problema foi corrigido.

gire certificados de conexão

Cada conexão de federação de grade usa quatro certificados SSL gerados automaticamente para proteger a conexão. Quando os dois certificados de cada grade estiverem próximos da data de expiração, o alerta **Expiration of Grid Federation certificate** lembra que você deve girar os certificados.

> Se os certificados em qualquer uma das extremidades da conexão expirarem, a conexão parará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

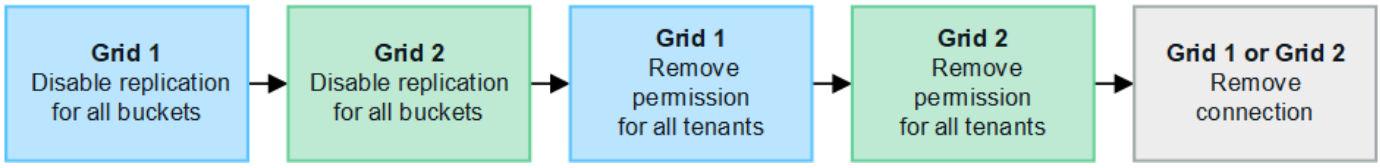
Passos

1. Faça login no Gerenciador de Grade a partir do nó Admin primário em qualquer grade.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Em qualquer guia da página de federação de Grade, selecione o nome da conexão para exibir seus detalhes.
4. Selecione a guia **certificados**.
5. Selecione **Rotate certificates** (rodar certificados).
6. Especifique quantos dias os novos certificados devem ser válidos.
7. Insira a senha de provisionamento para a grade à qual você está conetado.
8. Selecione **Rotate certificates** (rodar certificados).
9. Conforme necessário, repita estas etapas na outra grade na conexão.

   Em geral, use o mesmo número de dias para os certificados em ambos os lados da conexão.

Remova uma conexão de federação de grade

Você pode remover uma conexão de federação de grade de qualquer grade na conexão. Como mostrado na figura, você deve executar etapas de pré-requisito em ambas as grades para confirmar que a conexão não está sendo usada por nenhum locatário em qualquer grade.



Antes de remover uma conexão, observe o seguinte:

- A remoção de uma conexão não exclui nenhum item que já tenha sido copiado entre grades. Por exemplo, usuários de locatários, grupos e objetos que existem em ambas as grades não são excluídos de qualquer grade quando a permissão do locatário é removida. Se você quiser excluir esses itens, você deve excluí-los manualmente de ambas as grades.
- Quando você remove uma conexão, quaisquer objetos que estejam pendentes de replicação (ingeridos mas ainda não replicados para a outra grade) terão sua replicação permanentemente falhada.

Desative a replicação para todos os buckets do locatário

Passos

1. A partir de qualquer grade, entre no Gerenciador de Grade a partir do nó Admin primário.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione o nome da ligação para apresentar os respetivos detalhes.
4. Na guia **allowed tenants** (inquilinos permitidos), determine se a conexão está sendo usada por quaisquer inquilinos.
5. Se algum inquilino estiver listado, instrua todos os inquilinos para que "desative a replicação entre redes"todos os seus buckets em ambas as grades na conexão.

> Não é possível remover a permissão **usar conexão de federação de grade** se qualquer bucket de locatário tiver replicação entre grade ativada. Cada conta de locatário deve desativar a replicação entre grade para seus buckets em ambas as grades.

Remova a permissão para cada locatário

Depois que a replicação entre grades for desativada para todos os buckets do locatário, remova a permissão **Use Grid Federation** de todos os locatários em ambas as grades.

Passos

1. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
2. Selecione o nome da ligação para apresentar os respetivos detalhes.
3. Para cada locatário na guia **inquilinos permitidos**, remova a permissão **usar conexão de federação de grade** de cada locatário. "Gerenciar locatários permitidos"Consulte .
4. Repita estes passos para os inquilinos permitidos na outra grelha.

Remova a conexão

Passos

1. Quando nenhum inquilino em qualquer grade estiver usando a conexão, selecione **Remover**.
2. Reveja a mensagem de confirmação e selecione **Remover**.
   - Se a conexão puder ser removida, uma mensagem de sucesso será exibida. A conexão de federação de grade agora é removida de ambas as grades.
   - Se a conexão não puder ser removida (por exemplo, ela ainda está em uso ou há um erro de conexão), uma mensagem de erro será exibida. Você pode fazer um dos seguintes procedimentos:
     - Resolva o erro (recomendado). "Solucionar erros de federação de grade"Consulte .
     - Retire a ligação à força. Consulte a próxima seção.

Remova uma conexão de federação de grade pela força

Se necessário, você pode forçar a remoção de uma conexão que não tenha o status **conectado**.

A remoção forçada apenas elimina a ligação da grelha local. Para remover completamente a conexão, execute as mesmas etapas em ambas as grades.

Passos

1. Na caixa de diálogo de confirmação, selecione **forçar a remoção**.

   É apresentada uma mensagem de sucesso. Essa conexão de federação de grade não pode mais ser usada. No entanto, os buckets do locatário ainda podem ter a replicação entre grade ativada e algumas cópias de objeto podem já ter sido replicadas entre as grades na conexão.

2. A partir da outra grade na conexão, entre no Gerenciador de Grade do nó Admin principal.
3. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
4. Selecione o nome da ligação para apresentar os respetivos detalhes.
5. Selecione **Remover** e **Sim**.
6. Selecione **forçar a remoção** para remover a conexão desta grade.

Gerenciar os locatários permitidos para a federação de grade

Você pode permitir que as contas de locatário do S3 usem uma conexão de federação de grade entre dois sistemas StorageGRID. Quando os locatários têm permissão para usar uma conexão, etapas especiais são necessárias para editar os detalhes do locatário ou para remover permanentemente a permissão do locatário para usar a conexão.

Antes de começar

- Você está conetado ao Gerenciador de Grade em qualquer grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz" para a grade na qual você está conetado.
- Você "criou uma conexão de federação de grade" tem entre duas grades.
- Analisou os fluxos de trabalho para "clone de conta" e "replicação entre grade".
- Conforme necessário, você já configurou o logon único (SSO) ou identifica a federação para ambas as grades na conexão. "O que é o clone de conta"Consulte .

Crie um locatário permitido

Se você quiser permitir que uma conta de locatário nova ou existente use uma conexão de federação de grade para clone de conta e replicação entre grade, siga as instruções gerais para "Crie um novo locatário do S3" ou "edite uma conta de locatário" e observe o seguinte:

- Você pode criar o locatário a partir de qualquer grade na conexão. A grade onde um locatário é criado é a grade de origem do *locatário*.
- O estado da ligação tem de ser **ligado**.
- Quando o locatário é criado ou editado para ativar a permissão **usar conexão de federação de grade** e, em seguida, salvo na primeira grade, um locatário idêntico é automaticamente replicado para a outra grade. A grade onde o locatário é replicado é a grade de destino do *locatário*.
- Os locatários em ambas as grades terão o mesmo ID de conta, nome, descrição, cota e permissões de 20 dígitos. Opcionalmente, você pode usar o campo **Description** para ajudar a identificar qual é o locatário de origem e qual é o locatário de destino. Por exemplo, essa descrição para um locatário criado na Grade 1 também aparecerá para o locatário replicado para a Grade 2: "Este locatário foi criado na Grade 1."
- Por motivos de segurança, a senha de um usuário raiz local não é copiada para a grade de destino.

Antes que um usuário raiz local possa fazer login no locatário replicado na grade de destino, um administrador de grade para essa grade deve "altere a senha do usuário raiz local".

- Depois que o locatário novo ou editado estiver disponível em ambas as grades, os usuários do locatário podem executar estas operações:
  - Na grade de origem do locatário, crie grupos e usuários locais, que são clonados automaticamente para a grade de destino do locatário. "Clonar grupos de locatários e usuários"Consulte .
  - Crie novas chaves de acesso S3, que podem ser opcionalmente clonadas para a grade de destino do locatário. "Clonar chaves de acesso S3 usando a API"Consulte .
  - Crie buckets idênticos em ambas as grades na conexão e habilite a replicação entre grades em uma direção ou em ambas as direções. "Gerenciar a replicação entre grades"Consulte .

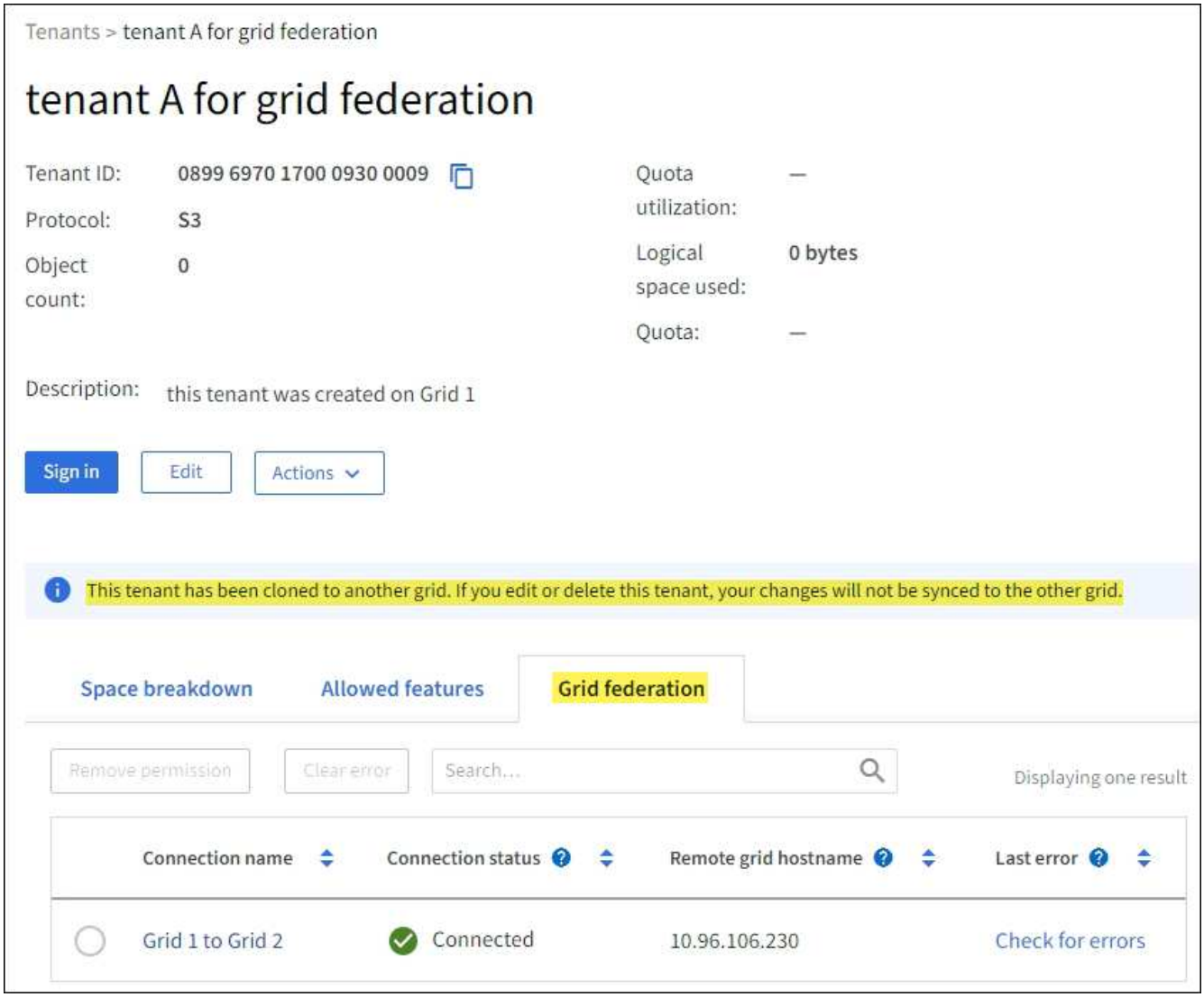
Ver um inquilino permitido

Você pode ver detalhes de um locatário que tem permissão para usar uma conexão de federação de grade.

Passos

1. Selecione **TENANTS**.
2. Na página de locatários, selecione o nome do locatário para exibir a página de detalhes do locatário.

   Se essa for a grade de origem do locatário (ou seja, se o locatário foi criado nessa grade), um banner aparecerá para lembrá-lo de que o locatário foi clonado para outra grade. Se você editar ou excluir esse locatário, suas alterações não serão sincronizadas com a outra grade.



3. Opcionalmente, selecione a guia **Grid Federation** para "monitore a conexão de federação de grade".

Editar um locatário permitido

Se você precisar editar um locatário que tenha a permissão **Use Grid Federation Connection**, siga as instruções gerais para "editando uma conta de locatário" e observe o seguinte:

- Se um locatário tiver a permissão **usar conexão de federação de grade**, você poderá editar os detalhes do locatário de qualquer grade na conexão. No entanto, quaisquer alterações feitas não serão copiadas para a outra grade. Se você quiser manter os detalhes do locatário sincronizados entre grades, você deve fazer as mesmas edições em ambas as grades.
- Você não pode limpar a permissão **usar conexão de federação de grade** quando estiver editando um locatário.
- Você não pode selecionar uma conexão de federação de grade diferente quando estiver editando um locatário.

Excluir um locatário permitido

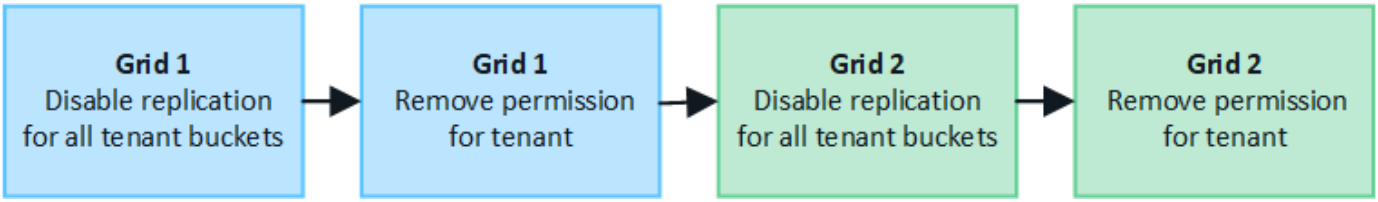
Se você precisar remover um locatário que tenha a permissão **Use Grid Federation Connection**, siga as instruções gerais para "excluindo uma conta de locatário" e observe o seguinte:

- Antes de remover o locatário original na grade de origem, você deve remover todos os buckets da conta na grade de origem.
- Antes de remover o locatário clonado na grade de destino, você deve remover todos os buckets da conta na grade de destino.
- Se você remover o locatário original ou clonado, a conta não poderá mais ser usada para replicação entre grade.
- Se você estiver removendo o locatário original na grade de origem, todos os grupos de locatários, usuários ou chaves clonadas para a grade de destino não serão afetados. Você pode excluir o locatário clonado ou permitir que ele gerencie seus próprios grupos, usuários, chaves de acesso e buckets.
- Se você estiver removendo o locatário clonado na grade de destino, erros de clone ocorrerão se novos grupos ou usuários forem adicionados ao locatário original.

  Para evitar esses erros, remova a permissão do locatário para usar a conexão de federação de grade antes de excluir o locatário dessa grade.

Remove Use grid Federation Connection permission

Para impedir que um locatário use uma conexão de federação de grade, você deve remover a permissão **usar conexão de federação de grade**.



Antes de remover a permissão de um locatário para usar uma conexão de federação de grade, observe o seguinte:

- Não é possível remover a permissão **usar conexão de federação de grade** se qualquer um dos buckets do locatário tiver a replicação entre grade ativada. A conta de locatário deve desativar a replicação entre redes para todos os buckets primeiro.
- A remoção da permissão **usar conexão de federação de grade** não exclui nenhum item que já tenha sido replicado entre grades. Por exemplo, os usuários, grupos e objetos de inquilino que existem em ambas as grades não são excluídos de qualquer grade quando a permissão do locatário é removida. Se você quiser excluir esses itens, você deve excluí-los manualmente de ambas as grades.
- Se você quiser reativar essa permissão com a mesma conexão de federação de grade, exclua esse locatário na grade de destino primeiro; caso contrário, reativar essa permissão resultará em um erro.

> Reativar a permissão **usar conexão de federação de grade** torna a grade local a grade de origem e aciona a clonagem para a grade remota especificada pela conexão de federação de grade selecionada. Se a conta de locatário já existir na grade remota, a clonagem resultará em um erro de conflito.

Antes de começar

- Você está usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz" para ambas as grades.

Desative a replicação para buckets do locatário

Como primeira etapa, desative a replicação entre grade para todos os buckets do locatário.

Passos

1. A partir de qualquer grade, entre no Gerenciador de Grade a partir do nó Admin primário.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione o nome da ligação para apresentar os respetivos detalhes.
4. Na guia **allowed tenants** (inquilinos permitidos), determine se o locatário está usando a conexão.
5. Se o inquilino estiver listado, instrua-o para "desative a replicação entre redes"todos os seus buckets em ambas as grades na conexão.

> Não é possível remover a permissão **usar conexão de federação de grade** se qualquer bucket de locatário tiver replicação entre grade ativada. O locatário deve desativar a replicação entre grade para seus buckets em ambas as grades.

Remover permissão para locatário

Depois que a replicação entre grades for desativada para buckets do locatário, você poderá remover a permissão do locatário para usar a conexão de federação de grade.

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Remova a permissão da página de federação de Grade ou da página de locatários.

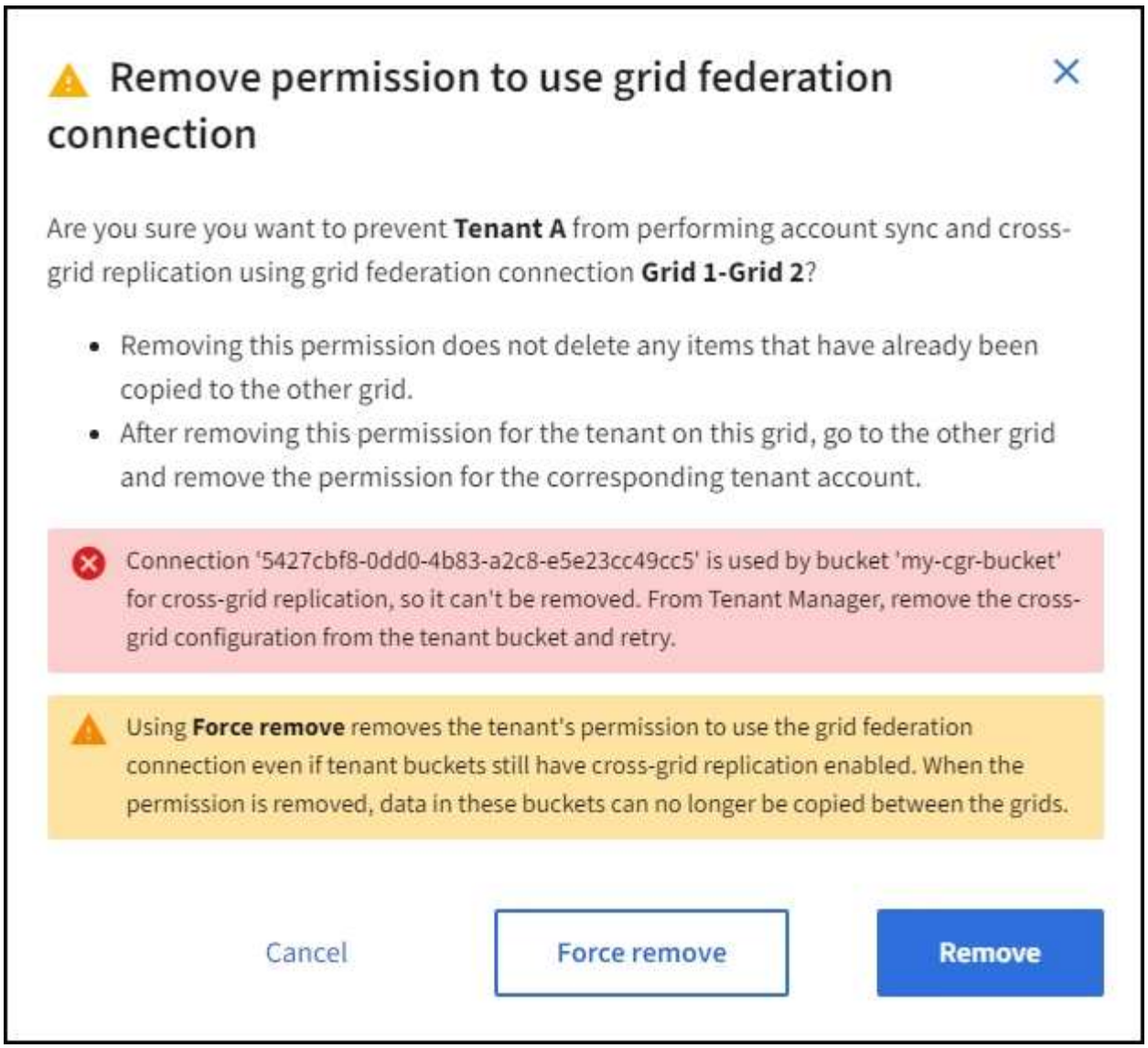
Página de federação de grade

a. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
b. Selecione o nome da ligação para apresentar a respetiva página de detalhes.
c. Na guia **allowed tenants** (inquilinos permitidos), selecione o botão de opção para o locatário.
d. Selecione **Remover permissão**.

Página de inquilinos

a. Selecione **TENANTS**.
b. Selecione o nome do locatário para exibir a página de detalhes.
c. No separador **Grid Federation** (federação de grelha), selecione o botão de opção para a ligação.
d. Selecione **Remover permissão**.

3. Reveja os avisos na caixa de diálogo de confirmação e selecione **Remover**.
   - Se a permissão puder ser removida, você será retornado à página de detalhes e uma mensagem de sucesso será exibida. Esse locatário não pode mais usar a conexão de federação de grade.
   - Se um ou mais buckets de inquilinos ainda tiverem a replicação entre grades ativada, um erro será exibido.



Você pode fazer um dos seguintes procedimentos:

- (Recomendado.) Faça login no Gerenciador do locatário e desative a replicação para cada um dos buckets do locatário. "Gerenciar a replicação entre grades"Consulte . Em seguida, repita as etapas para remover a permissão **Use Grid Connection**.
- Remova a permissão pela força. Consulte a próxima seção.

4. Vá para a outra grade e repita estas etapas para remover a permissão para o mesmo locatário na outra grade.

Remova a permissão pela força

Se necessário, você pode forçar a remoção da permissão de um locatário a usar uma conexão de federação de grade, mesmo se os buckets do locatário tiverem a replicação entre grade ativada.

Antes de remover a permissão de um inquilino por força, observe as considerações gerais[remover a permissão](), bem como estas considerações adicionais:

- Se você remover a permissão **usar conexão de federação de grade** por força, quaisquer objetos que estejam pendentes de replicação para a outra grade (ingeridos, mas ainda não replicados) continuarão a ser replicados. Para evitar que esses objetos em processo atinjam o intervalo de destino, você também

deve remover a permissão do locatário na outra grade.

- Quaisquer objetos ingeridos no intervalo de origem depois de remover a permissão **usar conexão de federação de grade** nunca serão replicados para o intervalo de destino.

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione o nome da ligação para apresentar a respetiva página de detalhes.
4. Na guia **allowed tenants** (inquilinos permitidos), selecione o botão de opção para o locatário.
5. Selecione **Remover permissão**.
6. Reveja os avisos na caixa de diálogo de confirmação e selecione **forçar a remoção**.

   É apresentada uma mensagem de sucesso. Esse locatário não pode mais usar a conexão de federação de grade.

7. Conforme necessário, vá para a outra grade e repita essas etapas para forçar a remoção da permissão para a mesma conta de locatário na outra grade. Por exemplo, você deve repetir essas etapas na outra grade para evitar que objetos em processo atinjam o intervalo de destino.

Solucionar erros de federação de grade

Talvez você precise solucionar alertas e erros relacionados a conexões de federação de grade, clone de conta e replicação entre grade.

alertas e erros de conexão de federação de grade

Você pode receber alertas ou ter erros com suas conexões de federação de grade.

Depois de fazer quaisquer alterações para resolver um problema de conexão, teste a conexão para garantir que o status da conexão retorne a **conectado**. Para obter instruções, "Gerenciar conexões de federação de grade"consulte .

Alerta de falha de conexão de federação de grade

Problema

O alerta **Falha na conexão da federação de grade** foi acionado.

Detalhes

Este alerta indica que a conexão de federação de grade entre as grades não está funcionando.

Ações recomendadas

1. Revise as configurações na página de Federação de Grade para ambas as grades. Confirme se todos os valores estão corretos. "Gerenciar conexões de federação de grade"Consulte .
2. Reveja os certificados utilizados para a ligação. Certifique-se de que não existem alertas para certificados de federação de grade expirados e de que os detalhes de cada certificado são válidos. Consulte as instruções para obter os certificados de conexão rotativos em "Gerenciar conexões de federação de grade".
3. Confirme se todos os nós Admin e Gateway em ambas as grades estão online e disponíveis. Resolva quaisquer alertas que possam estar afetando esses nós e tente novamente.

4. Se você forneceu um nome de domínio totalmente qualificado (FQDN) para a grade local ou remota, confirme se o servidor DNS está on-line e disponível. Consulte "O que é a federação de grade?" para obter informações sobre os requisitos de rede, endereço IP e DNS.

Expiração do alerta de certificado de federação de grade

Problema

O alerta **Expiration of Grid Federation certificate** foi acionado.

Detalhes

Este alerta indica que um ou mais certificados de federação de grade estão prestes a expirar.

Ações recomendadas

Consulte as instruções para obter os certificados de conexão rotativos em "Gerenciar conexões de federação de grade".

Erro ao editar uma conexão de federação de grade

Problema

Ao editar uma conexão de federação de grade, você verá a seguinte mensagem de aviso ao selecionar **Salvar e testar**: "Falha ao criar um arquivo de configuração de candidato em um ou mais nós."

Detalhes

Quando você edita uma conexão de federação de grade, o StorageGRID tenta salvar um arquivo de "configuração de candidato" em todos os nós de administração na primeira grade. Uma mensagem de aviso será exibida se esse arquivo não puder ser salvo em todos os nós de administração, por exemplo, porque um nó de administração está offline.

Ações recomendadas

1. Na grade que você está usando para editar a conexão, selecione **NÓS**.
2. Confirme se todos os nós de administração dessa grade estão online.
3. Se algum nó estiver offline, coloque-o novamente online e tente editar a conexão novamente.

Erros de clone de conta

Não é possível entrar em uma conta de locatário clonada

Problema

Você não pode entrar em uma conta de locatário clonada. A mensagem de erro na página de início de sessão do Gestor do Locatário é "as suas credenciais para esta conta eram inválidas. Tente novamente."

Detalhes

Por motivos de segurança, quando uma conta de locatário é clonada da grade de origem do locatário para a grade de destino do locatário, a senha definida para o usuário raiz local do locatário não é clonada. Da mesma forma, quando um locatário cria usuários locais em sua grade de origem, as senhas de usuário local não são clonadas para a grade de destino.

Ações recomendadas

Antes que o usuário raiz possa fazer login na grade de destino do locatário, um administrador de grade deve primeiro "altere a senha do usuário raiz local" na grade de destino.

Antes que um usuário local clonado possa entrar na grade de destino do locatário, o usuário raiz do locatário

clonado deve adicionar uma senha para o usuário na grade de destino. Para obter instruções, consulte "Gerenciar usuários locais" as instruções para usar o Gerenciador do Locatário.

Locatário criado sem um clone

Problema

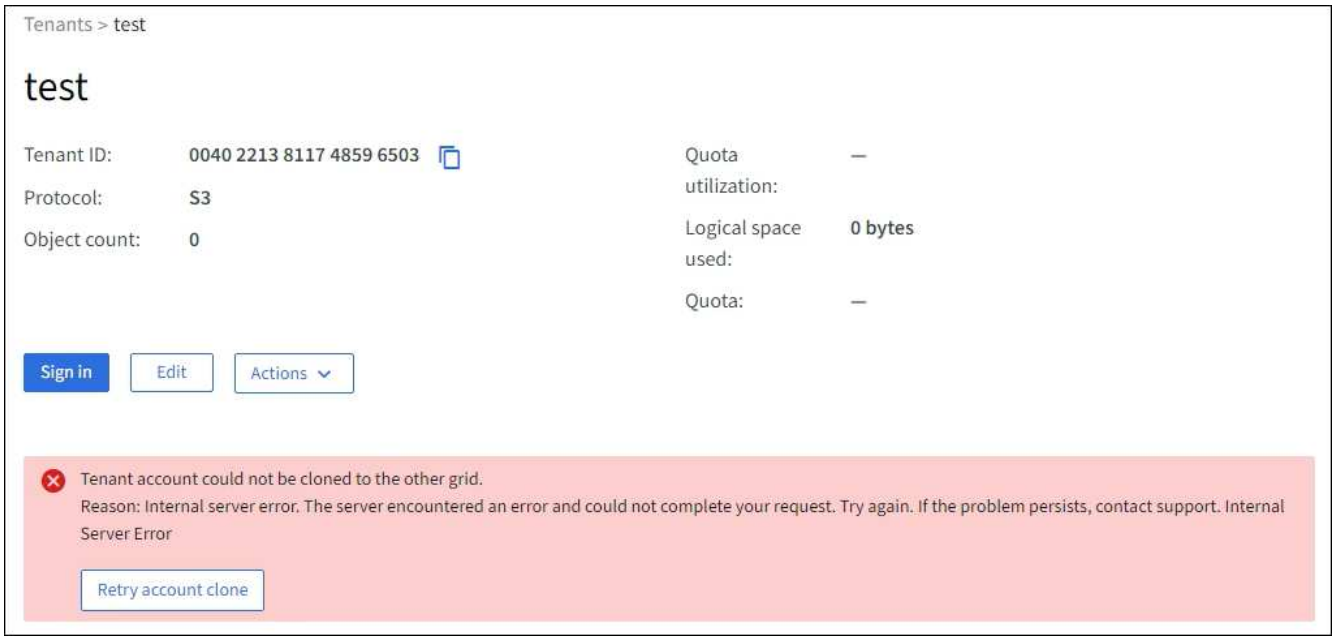
Você verá a mensagem "Tenant created without a clone" após criar um novo locatário com a permissão **Use Grid Federation Connection**.

Detalhes

Esse problema pode ocorrer se as atualizações do status da conexão forem atrasadas, o que pode fazer com que uma conexão não-saudável seja listada como **conectado**.

Ações recomendadas

1. Revise o motivo listado na mensagem de erro e resolva quaisquer problemas de rede ou outros que possam estar impedindo que a conexão funcione. Alertas e erros de conexão de federação de gradeConsulte .
2. Siga as instruções para testar uma conexão de federação de grade em "Gerenciar conexões de federação de grade"para confirmar que o problema foi corrigido.
3. Na grade de origem do locatário, selecione **TENANTS**.
4. Localize a conta de locatário que não foi clonada.
5. Selecione o nome do locatário para exibir a página de detalhes.
6. Selecione **Repetir clone de conta**.



Se o erro tiver sido resolvido, a conta de locatário será clonada para a outra grade.

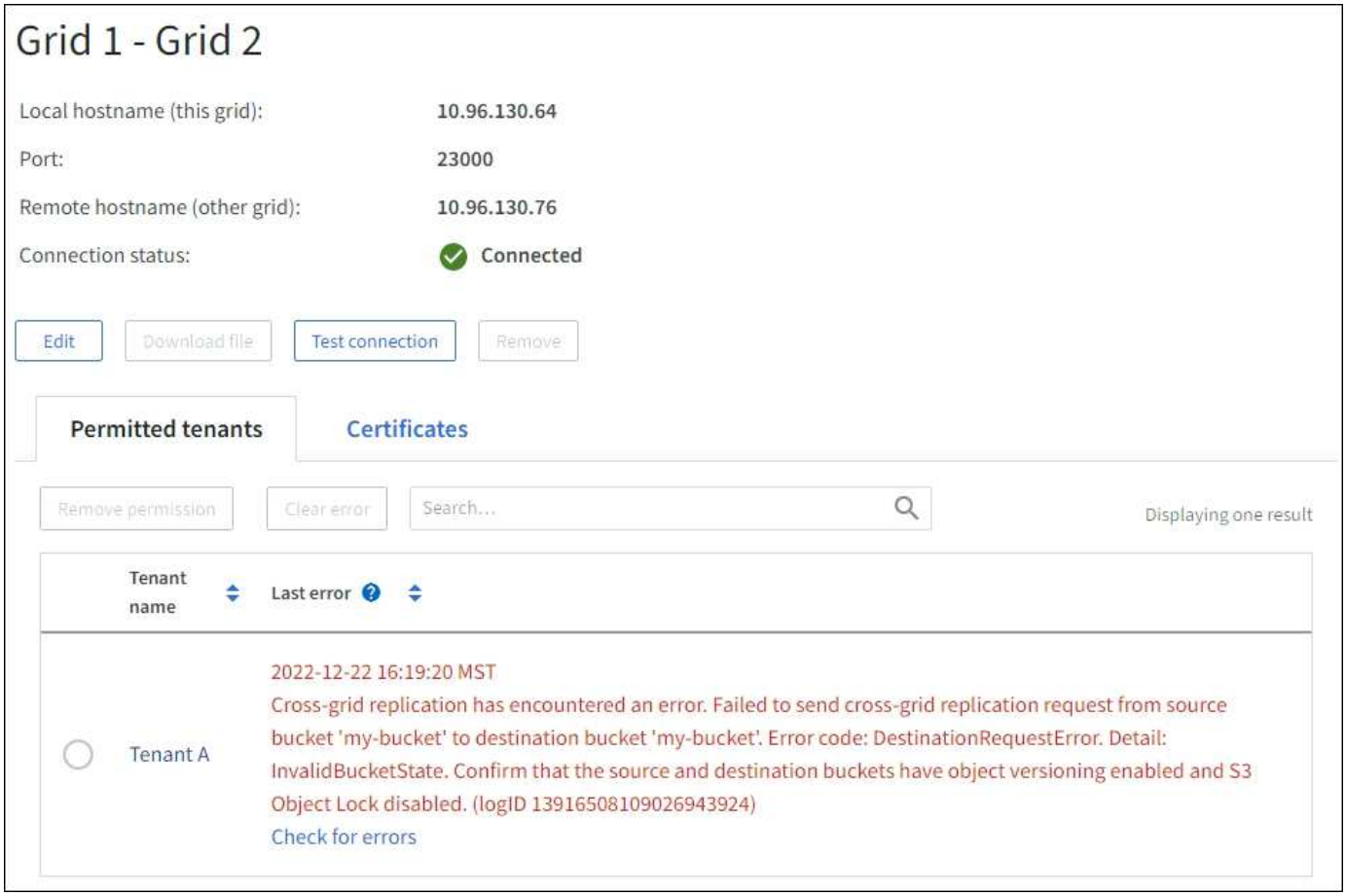
Alertas e erros de replicação entre redes

Último erro mostrado para conexão ou locatário

Problema

Quando "exibindo uma conexão de federação de grade" (ou "gerir os inquilinos permitidos"quando para uma

conexão), você percebe um erro na coluna **último erro** na página de detalhes da conexão. Por exemplo:



Detalhes

Para cada conexão de federação de grade, a coluna **último erro** mostra o erro mais recente a ocorrer, se houver, quando os dados de um locatário estavam sendo replicados para a outra grade. Esta coluna mostra apenas o último erro de replicação entre grelha a ocorrer; os erros anteriores que possam ter ocorrido não serão apresentados. Um erro nesta coluna pode ocorrer por um destes motivos:

- A versão do objeto fonte não foi encontrada.
- O balde de origem não foi encontrado.
- O intervalo de destino foi eliminado.
- O intervalo de destino foi recriado por uma conta diferente.
- O bucket de destino tem controle de versão suspenso.
- O intervalo de destino foi recriado pela mesma conta, mas agora não foi versionado.

Ações recomendadas

Se aparecer uma mensagem de erro na coluna **último erro**, siga estes passos:

1. Reveja o texto da mensagem.
2. Execute quaisquer ações recomendadas. Por exemplo, se o controle de versão foi suspenso no bucket de destino para replicação entre grades, reative o controle de versão desse bucket.
3. Selecione a conta de conexão ou locatário na tabela.
4. Selecione **Clear error**.

5. Selecione **Sim** para limpar a mensagem e atualizar o estado do sistema.
6. Aguarde 5-6 minutos e, em seguida, insira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

> Para garantir que a mensagem de erro seja limpa, aguarde pelo menos 5 minutos após o carimbo de data/hora na mensagem antes de inserir um novo objeto.

> Depois de limpar o erro, um novo **último erro** pode aparecer se os objetos forem ingeridos em um intervalo diferente que também tenha um erro.

7. Para determinar se algum objeto não pôde ser replicado devido ao erro de bucket, "Identificar e tentar novamente operações de replicação com falha"consulte .

Alerta de falha permanente de replicação entre redes

Problema

O alerta **Falha permanente de replicação entre redes** foi acionado.

Detalhes

Esse alerta indica que os objetos de locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer a intervenção do usuário para serem resolvidos. Este alerta é normalmente causado por uma alteração na origem ou no intervalo de destino.

Ações recomendadas

1. Inicie sessão na grelha onde o alerta foi acionado.
2. Aceda a **CONFIGURATION** > **System** > **Grid Federation** e localize o nome da ligação listado no alerta.
3. Na guia inquilinos permitidos, observe a coluna **último erro** para determinar quais contas de locatário têm erros.
4. Para saber mais sobre a falha, consulte as instruções em "Monitorar conexões de federação de grade" para analisar as métricas de replicação entre grades.
5. Para cada conta de locatário afetada:
   a. Consulte as instruções em "Monitorar a atividade do locatário" para confirmar que o locatário não excedeu sua cota na grade de destino para replicação entre grades.
   b. Conforme necessário, aumente a cota do locatário na grade de destino para permitir que novos objetos sejam salvos.
6. Para cada locatário afetado, faça login no Tenant Manager em ambas as grades, para que você possa comparar a lista de buckets.
7. Para cada bucket com replicação entre grades ativada, confirme o seguinte:
   - Há um intervalo correspondente para o mesmo inquilino na outra grade (deve usar o nome exato).
   - Ambos os buckets têm o controle de versão de objetos ativado (o controle de versão não pode ser suspenso em nenhuma grade).
   - Ambos os buckets têm o bloqueio de objeto S3 desativado.
   - Nenhum dos buckets está no estado **Deletando objetos: Somente leitura**.
8. Para confirmar que o problema foi resolvido, consulte as instruções em "Monitorar conexões de federação de grade" para rever as métricas de replicação entre redes ou execute estas etapas:

a. Volte para a página de federação de Grade.

b. Selecione o locatário afetado e selecione **Limpar erro** na coluna **último erro**.

c. Selecione **Sim** para limpar a mensagem e atualizar o estado do sistema.

d. Aguarde 5-6 minutos e, em seguida, insira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

> Para garantir que a mensagem de erro seja limpa, aguarde pelo menos 5 minutos após o carimbo de data/hora na mensagem antes de inserir um novo objeto.

> Pode levar até um dia para que o alerta seja apagado depois que ele for resolvido.

a. Aceda a "Identificar e tentar novamente operações de replicação com falha" para identificar quaisquer objetos ou eliminar marcadores que não foram replicados para a outra grelha e para tentar novamente a replicação conforme necessário.

Alerta de recurso de replicação entre redes indisponível

Problema

O alerta **recurso de replicação entre redes indisponível** foi acionado.

Detalhes

Esse alerta indica que as solicitações de replicação entre grade estão pendentes porque um recurso não está disponível. Por exemplo, pode haver um erro de rede.

Ações recomendadas

1. Monitore o alerta para ver se o problema resolve sozinho.
2. Se o problema persistir, determine se qualquer grade tem um alerta **Falha na conexão de federação de grade** para a mesma conexão ou um alerta **não é possível se comunicar com nó** para um nó. Esse alerta pode ser resolvido quando você resolve esses alertas.
3. Para saber mais sobre a falha, consulte as instruções em "Monitorar conexões de federação de grade" para analisar as métricas de replicação entre grades.
4. Se você não conseguir resolver o alerta, entre em Contato com o suporte técnico.

A replicação entre redes continuará normalmente após o problema ser resolvido.

Identificar e tentar novamente operações de replicação com falha

Depois de resolver o alerta **Falha permanente de replicação entre redes**, você deve determinar se algum objeto ou marcador de exclusão não foi replicado para a outra grade. Em seguida, você pode reingerir esses objetos ou usar a API de Gerenciamento de Grade para repetir a replicação.

O alerta **Falha permanente de replicação entre redes** indica que os objetos do locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer a intervenção do usuário para serem resolvidos. Este alerta é normalmente causado por uma alteração na origem ou no intervalo de destino. Para obter detalhes, "Solucionar erros de federação de grade"consulte .

Determine se algum objeto não pôde ser replicado

Para determinar se algum objeto ou marcador de exclusão não foram replicados para a outra grade, você pode pesquisar mensagens no log de auditoria"CGRR (solicitação de replicação entre grades)". Essa mensagem é adicionada ao log quando o StorageGRID não consegue replicar um objeto, objeto multiparte ou excluir um marcador para o bucket de destino.

Você pode usar o "ferramenta de auditoria-explicação" para traduzir os resultados em um formato mais fácil de ler.

Antes de começar

- Você tem permissão de acesso root.
- Você tem o `Passwords.txt` arquivo.
- Você conhece o endereço IP do nó de administração principal.

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. Procure mensagens CGRR no audit.log e use a ferramenta audit-explain para formatar os resultados.

   Por exemplo, este comando greps para todas as mensagens CGRR nos últimos 30 minutos e usa a ferramenta audit-explain.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   Os resultados do comando serão parecidos com este exemplo, que tem entradas para seis mensagens CGRR. No exemplo, todas as solicitações de replicação entre grades retornavam um erro geral porque o objeto não podia ser replicado. Os três primeiros erros são para operações de "replicar objeto", e os três últimos erros são para operações de "replicar marcador de exclusão".

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Cada entrada contém as seguintes informações:

Campo	Descrição
Solicitação de replicação entre Grade CGRR	O nome da solicitação
locatário	ID da conta do locatário
ligação	O ID da conexão de federação de grade
operação	O tipo de operação de replicação que estava sendo tentada: • replicar objeto • replicar marcador de eliminação • replique objeto multipart
balde	O nome do intervalo
objeto	O nome do objeto
versão	O ID da versão para o objeto

Campo	Descrição
erro	O tipo de erro. Se a replicação entre redes falhou, o erro é "erro geral".

Repetir repetições falhadas

Depois de gerar uma lista de objetos e excluir marcadores que não foram replicados para o bucket de destino e resolver os problemas subjacentes, você pode repetir a replicação de duas maneiras:

- Reingira cada objeto no intervalo de origem.
- Use a API privada de Gerenciamento de Grade, conforme descrito.

Passos

1. Na parte superior do Gerenciador de Grade, selecione o ícone de ajuda e selecione **Documentação da API**.
2. Selecione **vá para a documentação da API privada**.

> Os endpoints da API StorageGRID marcados como "Privado" estão sujeitos a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

3. Na seção **cross-grid-replication-Advanced**, selecione o seguinte endpoint:

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Selecione **Experimente**.
5. Na caixa de texto **body**, substitua a entrada de exemplo para **versionID** por uma ID de versão do audit.log que corresponde a uma solicitação de replicação entre grade e falha.

   Certifique-se de manter as aspas duplas ao redor da string.

6. Selecione **Executar**.
7. Confirme se o código de resposta do servidor é **204**, indicando que o objeto ou marcador de exclusão foi marcado como pendente para replicação entre grade para a outra grade.

> Pendente significa que a solicitação de replicação entre grade foi adicionada à fila interna para processamento.

Monitorar tentativas de replicação

Você deve monitorar as operações de repetição de replicação para garantir que elas sejam concluídas.

> Pode levar várias horas ou mais para que um objeto ou marcador de exclusão seja replicado para a outra grade.

Você pode monitorar as operações de repetição de duas maneiras:

- Use um S3 "HeadObject" ou "GetObject" pedido. A resposta inclui o cabeçalho de resposta específico do

StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grelha	Estado da replicação
Fonte	• **COMPLETED**: A replicação foi bem-sucedida. • **PENDENTE**: O objeto ainda não foi replicado. • **FAILURE**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	• RÉPLICA*: O objeto foi replicado a partir da grade de origem.

- Use a API privada de Gerenciamento de Grade, conforme descrito.

Passos

1. Na seção **cross-grid-replication-Advanced** da documentação da API privada, selecione o seguinte endpoint:

   `GET /private/cross-grid-replication-object-status/{id}`

2. Selecione **Experimente**.
3. Na seção parâmetro, insira o ID da versão que você usou na `cross-grid-replication-retry-failed` solicitação.
4. Selecione **Executar**.
5. Confirme se o código de resposta do servidor é **200**.
6. Revise o status da replicação, que será um dos seguintes:
   - **PENDENTE**: O objeto ainda não foi replicado.
   - **COMPLETED**: A replicação foi bem-sucedida.
   - **FAILED**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.

Gerenciar a segurança

Gerenciar a segurança

Você pode configurar várias configurações de segurança do Gerenciador de Grade para ajudar a proteger seu sistema StorageGRID.

Gerenciar a criptografia

O StorageGRID oferece várias opções para criptografar dados. Você deve "reveja os métodos de encriptação disponíveis"determinar quais atendem aos requisitos de proteção de dados.

Gerenciar certificados

Você pode "configure e gerencie os certificados do servidor" usar para conexões HTTP ou os certificados de cliente usados para autenticar uma identidade de cliente ou usuário no servidor.

Configurar servidores de gerenciamento de chaves

O uso de um "servidor de gerenciamento de chaves" permite proteger os dados do StorageGRID mesmo que um dispositivo seja removido do data center. Depois que os volumes do dispositivo são criptografados, você não pode acessar nenhum dado no dispositivo, a menos que o nó possa se comunicar com o KMS.

> Para usar o gerenciamento de chaves de criptografia, você deve habilitar a configuração **criptografia de nó** para cada dispositivo durante a instalação, antes que o dispositivo seja adicionado à grade.

Gerenciar configurações de proxy

Se você estiver usando serviços de plataforma S3 ou pools de storage em nuvem, poderá configurar um "servidor proxy de storage" entre nós de storage e os pontos de extremidade externos do S3. Se você enviar pacotes do AutoSupport usando HTTPS ou HTTP, poderá configurar um "servidor proxy admin" entre nós de administração e suporte técnico.

Controle firewalls

Para melhorar a segurança do sistema, você pode controlar o acesso aos nós de administração do StorageGRID abrindo ou fechando portas específicas no "firewall externo". Você também pode controlar o acesso à rede a cada nó configurando o respetivo "firewall interno". Você pode impedir o acesso em todas as portas, exceto as necessárias para sua implantação.

Reveja os métodos de encriptação StorageGRID

O StorageGRID oferece várias opções para criptografar dados. Você deve analisar os métodos disponíveis para determinar quais métodos atendem aos requisitos de proteção de dados.

A tabela fornece um resumo de alto nível dos métodos de criptografia disponíveis no StorageGRID.

Opção de criptografia	Como funciona	Aplica-se a
Servidor de gerenciamento de chaves (KMS) no Grid Manager	"configurar um servidor de gerenciamento de chaves"Você para o site StorageGRID e "habilite a criptografia de nó para o dispositivo". Em seguida, um nó de dispositivo se coneta ao KMS para solicitar uma chave de criptografia de chave (KEK). Essa chave criptografa e descriptografa a chave de criptografia de dados (DEK) em cada volume.	Nós de dispositivo que têm **Node Encryption** ativado durante a instalação. Todos os dados no dispositivo são protegidos contra perda física ou remoção do data center. **Nota**: O gerenciamento de chaves de criptografia com um KMS só é suportado para nós de armazenamento e dispositivos de serviços.

Opção de criptografia	Como funciona	Aplica-se a
Página de criptografia de unidade no instalador de dispositivos StorageGRID	Se o dispositivo contiver unidades que suportem criptografia de hardware, você poderá definir uma senha de unidade durante a instalação. Quando você define uma senha de unidade, é impossível para qualquer pessoa recuperar dados válidos de unidades que foram removidas do sistema, a menos que eles saibam a senha. Antes de iniciar a instalação, aceda a **Configurar hardware** > **encriptação da unidade** para definir uma frase-passe de unidade que se aplica a todas as unidades de encriptação automática geridas pela StorageGRID num nó.	Dispositivos que contêm unidades com autocriptografia. Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. A criptografia de unidade não se aplica a unidades gerenciadas pelo SANtricity. Se você tiver um dispositivo de storage com unidades com autocriptografia e controladoras SANtricity, poderá habilitar a segurança da unidade no SANtricity.
Conduza a segurança no Gerenciador de sistemas do SANtricity	Se o recurso Segurança da unidade estiver ativado para o seu dispositivo StorageGRID, você poderá usar "Gerente do sistema da SANtricity" o para criar e gerenciar a chave de segurança. A chave é necessária para aceder aos dados nas unidades seguras.	Dispositivos de storage com unidades Full Disk Encryption (FDE) ou unidades com autocriptografia. Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. Não pode ser usado com alguns dispositivos de armazenamento ou com quaisquer dispositivos de serviços.
Criptografia de objeto armazenado	Você ativa a "Criptografia de objeto armazenado" opção no Gerenciador de Grade. Quando ativado, todos os novos objetos que não são criptografados no nível do bucket ou no nível do objeto são criptografados durante a ingestão.	Dados de objeto S3 recém-ingeridos. Os objetos armazenados existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de bucket do S3	Você emite uma solicitação PutBucketEncryption para ativar a criptografia para o bucket. Todos os novos objetos que não são criptografados no nível do objeto são criptografados durante a ingestão.	Somente dados de objeto S3 recém-ingeridos. A criptografia deve ser especificada para o intervalo. Os objetos bucket existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados. "Operações em baldes"
Criptografia do lado do servidor de objetos S3 (SSE)	Você emite uma solicitação S3 para armazenar um objeto e incluir o `x-amz-server-side-encryption` cabeçalho da solicitação.	Somente dados de objeto S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados. StorageGRID gerencia as chaves. "Use a criptografia do lado do servidor"
Criptografia do lado do servidor de objetos S3 com chaves fornecidas pelo cliente (SSE-C)	Você emite uma solicitação S3 para armazenar um objeto e incluir três cabeçalhos de solicitação. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Somente dados de objeto S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados. As chaves são gerenciadas fora do StorageGRID. "Use a criptografia do lado do servidor"

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de volume externo ou datastore	Você usa um método de criptografia fora do StorageGRID para criptografar um volume ou armazenamento de dados inteiro, se sua plataforma de implantação o suportar.	Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou datastore seja criptografado. Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.
Criptografia de objetos fora do StorageGRID	Você usa um método de criptografia fora do StorageGRID para criptografar dados e metadados de objetos antes que eles sejam ingeridos no StorageGRID.	Somente dados e metadados de objetos (os dados de configuração do sistema não são criptografados). Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados. "Amazon Simple Storage Service - Guia do usuário: Protegendo dados usando criptografia do lado do cliente"

Use vários métodos de criptografia

Dependendo dos seus requisitos, você pode usar mais de um método de criptografia de cada vez. Por exemplo:

- Você pode usar um KMS para proteger os nós do dispositivo e também usar o recurso de segurança da unidade no Gerenciador de sistemas do SANtricity para "criptografar duas vezes" os dados nas unidades com autocriptografia nos mesmos dispositivos.
- Você pode usar um KMS para proteger dados nos nós do dispositivo e também usar a opção de criptografia de objeto armazenado para criptografar todos os objetos quando eles são ingeridos.

Se apenas uma pequena parte de seus objetos exigir criptografia, considere controlar a criptografia no intervalo ou no nível de objeto individual. Ativar vários níveis de criptografia tem um custo de desempenho adicional.

Gerenciar certificados

Gerenciar certificados de segurança

Certificados de segurança são pequenos arquivos de dados usados para criar conexões seguras e confiáveis entre componentes do StorageGRID e entre componentes do StorageGRID e sistemas externos.

O StorageGRID usa dois tipos de certificados de segurança:

- **Certificados de servidor** são necessários quando você usa conexões HTTPS. Os certificados de servidor são usados para estabelecer conexões seguras entre clientes e servidores, autenticando a identidade de um servidor para seus clientes e fornecendo um caminho de comunicação seguro para os dados. O servidor e o cliente têm uma cópia do certificado.
- **Certificados de cliente** autenticam uma identidade de cliente ou usuário no servidor, fornecendo autenticação mais segura do que senhas sozinhas. Os certificados de cliente não encriptam dados.

Quando um cliente se coneta ao servidor usando HTTPS, o servidor responde com o certificado do servidor, que contém uma chave pública. O cliente verifica esse certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão com o servidor usando a mesma chave pública.

O StorageGRID funciona como o servidor para algumas conexões (como o endpoint do balanceador de carga) ou como o cliente para outras conexões (como o serviço de replicação do CloudMirror).

- Certificado padrão de CA de grade*

O StorageGRID inclui uma autoridade de certificação (CA) integrada que gera um certificado interno da CA de grade durante a instalação do sistema. O certificado de CA de grade é usado, por padrão, para proteger o tráfego interno do StorageGRID. Uma autoridade de certificação externa (CA) pode emitir certificados personalizados que são totalmente compatíveis com as políticas de segurança de informações da sua organização. Embora seja possível usar o certificado da CA de Grade para um ambiente que não seja de produção, a prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa. Conexões não protegidas sem certificado também são suportadas, mas não são recomendadas.

- Os certificados de CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser os especificados para verificar conexões de servidor.
- Todos os certificados personalizados devem atender ao "diretrizes de fortalecimento do sistema para certificados de servidor".
- O StorageGRID oferece suporte ao agrupamento de certificados de uma CA em um único arquivo (conhecido como pacote de certificados da CA).

> ⓘ O StorageGRID também inclui certificados de CA do sistema operacional que são os mesmos em todas as grades. Em ambientes de produção, certifique-se de especificar um certificado personalizado assinado por uma autoridade de certificação externa em vez do certificado CA do sistema operacional.

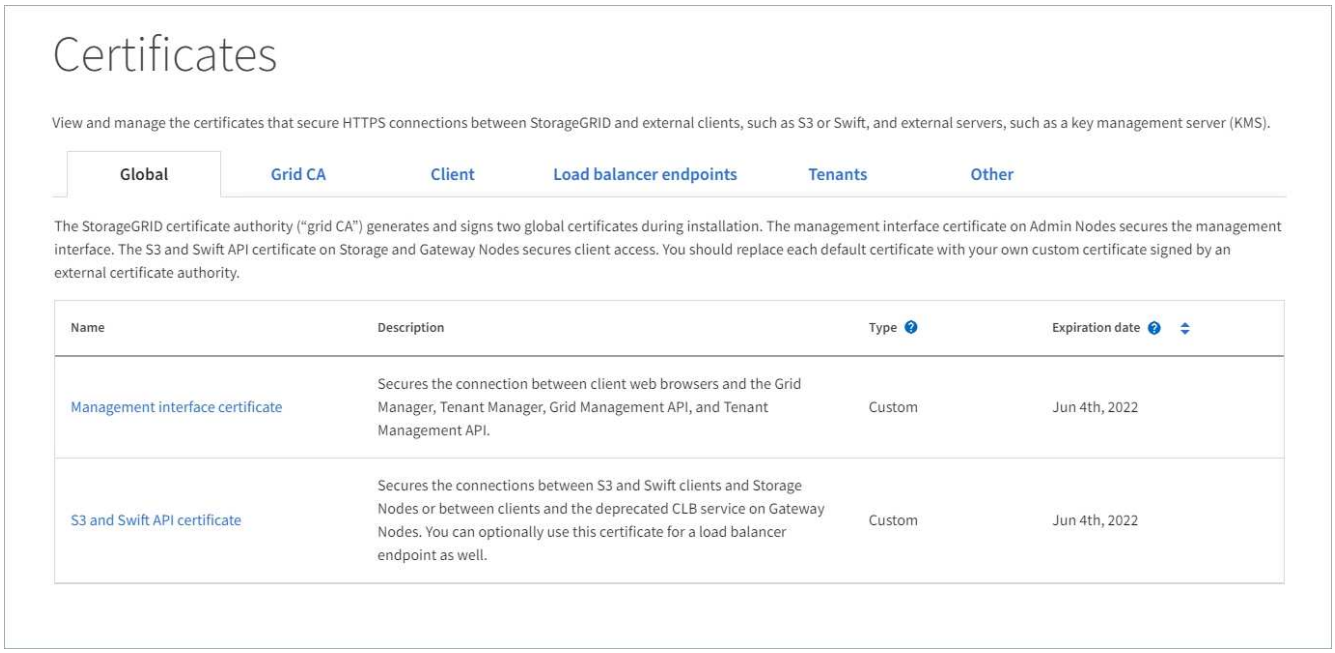
Variantes dos tipos de certificado de servidor e cliente são implementadas de várias maneiras. Você deve ter todos os certificados necessários para sua configuração específica do StorageGRID prontos antes de configurar o sistema.

Acesse certificados de segurança

Você pode acessar informações sobre todos os certificados do StorageGRID em um único local, juntamente com links para o fluxo de trabalho de configuração de cada certificado.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates**.



2. Selecione uma guia na página certificados para obter informações sobre cada categoria de certificado e para acessar as configurações de certificado. Pode aceder a um separador se tiver o "permissão apropriada".

   - * Global*: Protege o acesso à StorageGRID de navegadores da web e clientes de API externos.
   - * Grade CA*: Protege o tráfego interno do StorageGRID.
   - **Cliente**: Protege conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
   - **Terminais do balanceador de carga**: Protege conexões entre clientes S3 e o balanceador de carga StorageGRID.
   - * Inquilinos*: Protege conexões com servidores de federação de identidade ou de endpoints de serviço de plataforma para recursos de armazenamento S3.
   - **Outros**: Protege conexões StorageGRID que exigem certificados específicos.

     Cada guia é descrito abaixo com links para detalhes adicionais do certificado.

Global

Os certificados globais protegem o acesso à StorageGRID a partir de navegadores da Web e clientes externos da API S3. Dois certificados globais são inicialmente gerados pela autoridade de certificação StorageGRID durante a instalação. A prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa.

- Certificado de interface de gerenciamento: Protege as conexões do navegador da Web do cliente às interfaces de gerenciamento do StorageGRID.
- Certificado API S3: Protege as conexões da API do cliente aos nós de storage, nós de administrador e nós de gateway, que os aplicativos clientes S3 usam para carregar e baixar dados de objeto.

As informações sobre os certificados globais instalados incluem:

- **Nome**: Nome do certificado com link para gerenciar o certificado.
- **Descrição**
- **Tipo**: Personalizado ou padrão. Você deve sempre usar um certificado personalizado para melhorar a segurança da grade.
- **Data de expiração**: Se estiver usando o certificado padrão, nenhuma data de expiração será exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade de certificação externa para melhorar a segurança da grade:
  - "Substitua o certificado padrão da interface de gerenciamento gerado pelo StorageGRID" Usado para conexões do Grid Manager e do Tenant Manager.
  - "Substitua o certificado API S3" Usado para conexões do nó de armazenamento e do ponto de extremidade do balanceador de carga (opcional).
- "Restaure o certificado padrão da interface de gerenciamento".
- "Restaure o certificado padrão da API S3".
- "Use um script para gerar um novo certificado de interface de gerenciamento autoassinado".
- Copie ou transfira a "certificado de interface de gerenciamento" ou "Certificado API S3".

CA da grelha

O Certificado CA de grade, gerado pela autoridade de certificação StorageGRID durante a instalação do StorageGRID, protege todo o tráfego interno do StorageGRID.

As informações do certificado incluem a data de validade do certificado e o conteúdo do certificado.

Você pode "Copie ou baixe o certificado da CA de Grade", mas não pode alterá-lo.

Cliente

Certificados de cliente, Gerado por uma autoridade de certificação externa, proteja as conexões entre ferramentas de monitoramento externas e o banco de dados do StorageGRID Prometheus.

A tabela de certificados tem uma linha para cada certificado de cliente configurado e indica se o certificado pode ser usado para acesso ao banco de dados Prometheus, juntamente com a data de validade do certificado.

Você pode:

- "Carregue ou gere um novo certificado de cliente."
- Selecione um nome de certificado para exibir os detalhes do certificado onde você pode:
  - "Altere o nome do certificado do cliente."
  - "Defina a permissão de acesso Prometheus."
  - "Carregue e substitua o certificado do cliente."
  - "Copie ou baixe o certificado do cliente."
  - "Remova o certificado do cliente."
- Selecione **ações** para rapidamente "editar", "fixe", ou "retire" um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los ao mesmo tempo usando **ações** > **Remover**.

Pontos de extremidade do balanceador de carga

Certificados de terminais do balanceador de carga Proteja as conexões entre clientes S3 e o serviço de balanceador de carga StorageGRID em nós de gateway e nós de administração.

A tabela de endpoint do balanceador de carga tem uma linha para cada endpoint do balanceador de carga configurado e indica se o certificado global da API S3 ou um certificado de endpoint do balanceador de carga personalizado está sendo usado para o endpoint. A data de validade de cada certificado também é exibida.

> As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Você pode:

- "Exibir um ponto final do balanceador de carga", incluindo os respetivos detalhes do certificado.
- "Especifique um certificado de endpoint do balanceador de carga para o FabricPool."
- "Use o certificado global da API S3" em vez de gerar um novo certificado de endpoint do balanceador de carga.

Inquilinos

Os locatários podem usar certificados de servidor de federação de identidade ou certificados de endpoint de serviço de plataformaproteger suas conexões com o StorageGRID.

A tabela de locatário tem uma linha para cada locatário e indica se cada locatário tem permissão para usar sua própria fonte de identidade ou serviços de plataforma.

Você pode:

- "Selecione um nome de locatário para iniciar sessão no Gestor de inquilinos"
- "Selecione um nome de locatário para exibir os detalhes da federação de identidade do locatário"
- "Selecione um nome de locatário para visualizar os detalhes dos serviços da plataforma do locatário"
- "Especifique um certificado de endpoint de serviço de plataforma durante a criação do endpoint"

Outros

O StorageGRID usa outros certificados de segurança para fins específicos. Estes certificados são listados pelo seu nome funcional. Outros certificados de segurança incluem:

- Certificados do Cloud Storage Pool
- Certificados de notificação de alerta por e-mail
- Certificados de servidor syslog externos
- Certificados de conexão de federação de grade
- Certificados de federação de identidade
- Certificados de servidor de gerenciamento de chaves (KMS)
- Certificados de logon único

As informações indicam o tipo de certificado que uma função utiliza e as datas de expiração do certificado do servidor e do cliente, conforme aplicável. A seleção de um nome de função abre uma guia do navegador onde você pode exibir e editar os detalhes do certificado.

> Só pode ver e aceder a informações de outros certificados se tiver o "permissão apropriada".

Você pode:

- "Especifique um certificado do Cloud Storage Pool para S3, C2S S3 ou Azure"
- "Especifique um certificado para notificações por e-mail de alerta"
- "Use um certificado para um servidor syslog externo"
- "Girar certificados de conexão de federação de grade"
- "Exibir e editar um certificado de federação de identidade"
- "Carregar certificados de servidor de gerenciamento de chaves (KMS) e cliente"
- "Especifique manualmente um certificado SSO para uma confiança de parte dependente"

Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para as instruções de implementação.

Certificado de interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre navegadores da Web cliente e a interface de gerenciamento do StorageGRID, permitindo que os usuários acessem o Gerenciador de Grade e o Gerenciador de locatário sem avisos de segurança. Este certificado também autentica as conexões da API de Gerenciamento de Grade e da API de Gerenciamento do locatário. Pode utilizar o certificado predefinido criado durante a instalação ou carregar um certificado personalizado.	**CONFIGURATION** > **Security** > **Certificates**, selecione a guia **Global** e, em seguida, selecione **Management interface certificate**	"Configurar certificados de interface de gerenciamento"

Certificado API S3

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras de clientes S3 com um nó de storage e terminais de balanceador de carga (opcional).	**CONFIGURATION** > **Security** > **Certificates**, selecione a guia **Global** e, em seguida, selecione **S3 API certificate**	"Configure os certificados API do S3"

Certificado CA de grade

Consulte Descrição do certificado da CA de Grade padrão.

Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	Instalado em cada cliente, permitindo que o StorageGRID autentique o acesso de cliente externo. • Permite que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas.	**CONFIGURATION** > **Security** > **Certificates** e selecione a guia **Client**	"Configurar certificados de cliente"

Certificado de ponto final do balanceador de carga

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre clientes S3 e o serviço de balanceador de carga StorageGRID em nós de gateway e nós de administração. Você pode fazer upload ou gerar um certificado de balanceador de carga ao configurar um endpoint de balanceador de carga. Os aplicativos clientes usam o certificado do balanceador de carga ao se conetar ao StorageGRID para salvar e recuperar dados de objeto. Você também pode usar uma versão personalizada do certificado global Certificado API S3para autenticar conexões com o serviço Load Balancer. Se o certificado global for usado para autenticar conexões do balanceador de carga, você não precisará carregar ou gerar um certificado separado para cada ponto de extremidade do balanceador de carga. **Nota:** o certificado usado para autenticação do balanceador de carga é o certificado mais usado durante a operação normal do StorageGRID.	**CONFIGURATION** > **Network** > **Load balancer endpoints**	• "Configurar pontos de extremidade do balanceador de carga" • "Crie um ponto de extremidade do balanceador de carga para o FabricPool"

Certificado de endpoint do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um pool de storage de nuvem do StorageGRID para um local de storage externo, como o S3 Glacier ou o storage Microsoft Azure Blob. Um certificado diferente é necessário para cada tipo de provedor de nuvem.	**ILM** > **conjuntos de armazenamento**	"Crie um pool de storage em nuvem"

Certificado de notificação de alerta por e-mail

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre um servidor de e-mail SMTP e o StorageGRID que é usado para notificações de alerta. • Se as comunicações com o servidor SMTP exigirem TLS (Transport Layer Security), você deverá especificar o certificado CA do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.	**ALERTAS** > **Configuração do e-mail**	"Configurar notificações por e-mail para alertas"

Certificado de servidor syslog externo

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão TLS ou RELP/TLS entre um servidor syslog externo que Registra eventos no StorageGRID. **Nota:** não é necessário um certificado de servidor syslog externo para conexões TCP, RELP/TCP e UDP a um servidor syslog externo.	**CONFIGURATION** > **Monitoring** > **servidor de auditoria e syslog**	"Use um servidor syslog externo"

certificado de conexão de federação de grade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentique e criptografe as informações enviadas entre o sistema StorageGRID atual e outra grade em uma conexão de federação de grade.	**CONFIGURATION** > **System** > **Grid Federation**	• "Crie conexões de federação de grade" • "Rode os certificados de ligação"

Certificado de federação de identidade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre o StorageGRID e um provedor de identidade externo, como ative Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidade, que permite que grupos de administração e usuários sejam gerenciados por um sistema externo.	**CONFIGURATION** > **Access Control** > **Identity Federation**	"Use a federação de identidade"

Certificado de servidor de gerenciamento de chaves (KMS)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre o StorageGRID e um servidor de gerenciamento de chaves externo (KMS), que fornece chaves de criptografia para os nós do dispositivo StorageGRID.	**CONFIGURATION** > **Security** > **Key Management Server**	"Adicionar servidor de gerenciamento de chaves (KMS)"

Certificado de endpoint de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão do serviço da plataforma StorageGRID a um recurso de storage S3.	**Gerenciador do Locatário** > **ARMAZENAMENTO (S3)** > **terminais de serviços da plataforma**	"Criar endpoint de serviços de plataforma" "Editar endpoint de serviços de plataforma"

Certificado de logon único (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como AD FS (Serviços de Federação do ative Directory) e StorageGRID usados para solicitações de logon único (SSO).	**CONFIGURATION** > **access control** > **Single sign-on**	"Configurar o logon único"

Exemplos de certificados

Exemplo 1: Serviço do Load Balancer

Neste exemplo, o StorageGRID atua como servidor.

1. Você configura um ponto de extremidade do balanceador de carga e carrega ou gera um certificado de servidor no StorageGRID.
2. Você configura uma conexão de cliente S3 para o endpoint do balanceador de carga e carrega o mesmo certificado para o cliente.
3. Quando o cliente deseja salvar ou recuperar dados, ele se coneta ao endpoint do balanceador de carga usando HTTPS.

4. O StorageGRID responde com o certificado do servidor, que contém uma chave pública e com uma assinatura baseada na chave privada.
5. O cliente verifica esse certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão usando a mesma chave pública.
6. O cliente envia dados de objeto para o StorageGRID.

Exemplo 2: Servidor de gerenciamento de chaves externas (KMS)

Neste exemplo, o StorageGRID atua como cliente.

1. Usando o software servidor de gerenciamento de chaves externo, você configura o StorageGRID como um cliente KMS e obtém um certificado de servidor assinado pela CA, um certificado de cliente público e a chave privada para o certificado de cliente.
2. Usando o Gerenciador de Grade, você configura um servidor KMS e carrega os certificados de servidor e cliente e a chave privada do cliente.
3. Quando um nó StorageGRID precisa de uma chave de criptografia, ele faz uma solicitação ao servidor KMS que inclui dados do certificado e uma assinatura com base na chave privada.
4. O servidor KMS valida a assinatura do certificado e decide que pode confiar no StorageGRID.
5. O servidor KMS responde usando a conexão validada.

Tipos de certificado de servidor suportados

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (algoritmo de assinatura digital de curva elítica).

> O tipo de codificação da diretiva de segurança deve corresponder ao tipo de certificado do servidor. Por exemplo, as cifras RSA exigem certificados RSA e as cifras ECDSA exigem certificados ECDSA. "Gerenciar certificados de segurança"Consulte . Se configurar uma política de segurança personalizada que não seja compatível com o certificado do servidor, pode "reverter temporariamente para a política de segurança padrão".

Para obter mais informações sobre como o StorageGRID protege as conexões do cliente, "Segurança para clientes S3"consulte .

Configurar certificados de interface de gerenciamento

Você pode substituir o certificado de interface de gerenciamento padrão por um único certificado personalizado que permite que os usuários acessem o Gerenciador de Grade e o Gerenciador do locatário sem encontrar avisos de segurança. Você também pode reverter para o certificado de interface de gerenciamento padrão ou gerar um novo.

Sobre esta tarefa

Por padrão, cada nó de administrador é emitido um certificado assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de interface de gerenciamento personalizado comum e uma chave privada correspondente.

Como um único certificado de interface de gerenciamento personalizado é usado para todos os nós de administração, você deve especificar o certificado como um certificado curinga ou multi-domínio se os clientes precisarem verificar o nome do host ao se conetar ao Gerenciador de Grade e ao Gerenciador de locatário.

Defina o certificado personalizado de modo que corresponda a todos os nós de administração na grade.

Você precisa concluir a configuração no servidor e, dependendo da autoridade de certificação raiz (CA) que você está usando, os usuários também podem precisar instalar o certificado de CA de grade no navegador da Web que eles usarão para acessar o Gerenciador de Grade e o Gerenciador de locatário.

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 este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de validade do certificado da interface de gerenciamento na guia Global.

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.
- reverter de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrãoVocê .

Adicione um certificado de interface de gerenciamento personalizado

Para adicionar um certificado de interface de gerenciamento personalizado, você pode fornecer seu próprio certificado ou gerar um usando o Gerenciador de Grade.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor**: O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado**: O arquivo de chave privada de certificado de servidor personalizado (`.key`).

> As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA**: Um único arquivo opcional contendo 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.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

Gerar certificado

Gere os ficheiros de certificado do servidor.

> A prática recomendada para um ambiente de produção é usar um certificado de interface de gerenciamento personalizado assinado por uma autoridade de certificação externa.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.

Campo	Descrição
IP	Um ou mais endereços IP a incluir no certificado.
Assunto (opcional)	X,509 Assunto ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

> Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Depois de adicionar um certificado de interface de gerenciamento personalizado, a página de certificado de interface de gerenciamento exibe informações detalhadas de certificado para os certificados que estão em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

Restaure o certificado padrão da interface de gerenciamento

Você pode reverter para o uso do certificado de interface de gerenciamento padrão para conexões do Gerenciador de Grade e do Gerenciador de Tenant.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **Use default certificate** (usar certificado padrão).

   Quando você restaura o certificado de interface de gerenciamento padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. O certificado de interface de gerenciamento padrão é usado para todas as novas conexões de cliente subsequentes.

4. Atualize a página para garantir que o navegador da Web seja atualizado.

Use um script para gerar um novo certificado de interface de gerenciamento autoassinado

Se for necessária uma validação estrita do nome do host, você pode usar um script para gerar o certificado da interface de gerenciamento.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

A melhor prática para um ambiente de produção é usar um certificado assinado por uma autoridade de certificação externa.

Passos

1. Obtenha o nome de domínio totalmente qualificado (FQDN) de cada nó Admin.
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. Configure o StorageGRID com um novo certificado autoassinado.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Para `--domains`, use curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração. Por exemplo, `*.ui.storagegrid.example.com` usa o caractere curinga * para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
   - Defina `--type` como `management` para configurar o certificado da interface de gerenciamento, que é usado pelo Gerenciador de Grade e pelo Gerenciador de Locatário.
   - Por padrão, os certificados gerados são válidos por um ano (365 dias) e devem ser recriados antes de expirarem. Você pode usar o `--days` argumento para substituir o período de validade padrão.

O período de validade de um certificado começa quando `make-certificate` é executado. Você deve garantir que o cliente de gerenciamento esteja sincronizado com a mesma fonte de tempo que o StorageGRID; caso contrário, o cliente poderá rejeitar o certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

A saída resultante contém o certificado público necessário pelo cliente da API de gerenciamento.

4. Selecione e copie o certificado.

   Inclua as tags DE INÍCIO e FIM em sua seleção.

5. Faça logout do shell de comando. `$ exit`
6. Confirme se o certificado foi configurado:
   a. Acesse o Gerenciador de Grade.
   b. Selecione **CONFIGURATION** > **Security** > **Certificates**
   c. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags DE INÍCIO e FIM.

Transfira ou copie o certificado da interface de gestão

Você pode salvar ou copiar o conteúdo do certificado da interface de gerenciamento para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA `.pem`. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote CA**.

   Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

   Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Configure os certificados API do S3

Você pode substituir ou restaurar o certificado do servidor usado para conexões de cliente S3 para nós de storage ou para pontos de extremidade do balanceador de carga. O certificado de servidor personalizado de substituição é específico para a sua organização.

Os detalhes do Swift foram removidos desta versão do site do doc. "StorageGRID 11,8: Configurar certificados API S3 e Swift"Consulte .

Sobre esta tarefa

Por padrão, cada nó de armazenamento é emitido um certificado de servidor X,509 assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e uma chave privada correspondente.

Um único certificado de servidor personalizado é usado para todos os nós de armazenamento, portanto, você deve especificar o certificado como um certificado curinga ou multi-domínio se os clientes precisarem verificar o nome do host ao se conetar ao endpoint de armazenamento. Defina o certificado personalizado de modo que corresponda a todos os nós de storage na grade.

Depois de concluir a configuração no servidor, talvez você também precise instalar o certificado de CA de

grade no cliente de API S3 que você usará para acessar o sistema, dependendo da autoridade de certificação raiz (CA) que você estiver usando.

> Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of global Server certificate for S3 API** é acionado quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de expiração do certificado API S3 na guia Global.

Você pode fazer upload ou gerar um certificado de API S3 personalizado.

Adicione um certificado de API S3 personalizado

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 API certificate**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor**: O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado**: O arquivo de chave privada de certificado de servidor personalizado (`.key`).

> As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA**: Um único arquivo opcional contendo os certificados de cada autoridade de certificação de emissão intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

c. Selecione os detalhes do certificado para exibir os metadados e o PEM para cada certificado personalizado da API S3 que foi carregado. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**.

  O certificado de servidor personalizado é usado para novas conexões de cliente S3 subsequentes.

Gerar certificado

Gere os ficheiros de certificado do servidor.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a incluir no certificado.

Campo	Descrição
Assunto (opcional)	X,509 Assunto ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para exibir os metadados e o PEM para o certificado personalizado da API S3 que foi gerado.

   - Selecione **Transferir certificado** para guardar o ficheiro de certificado.

     Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

     Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**.

   O certificado de servidor personalizado é usado para novas conexões de cliente S3 subsequentes.

5. Selecione uma guia para exibir metadados para o certificado padrão do servidor StorageGRID, um certificado assinado pela CA que foi carregado ou um certificado personalizado que foi gerado.

   Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Atualize a página para garantir que o navegador da Web seja atualizado.

7. Depois de adicionar um certificado de API S3 personalizado, a página de certificado de API S3 exibe informações detalhadas de certificado para o certificado de API S3 personalizado que está em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

Restaure o certificado padrão da API S3

Você pode reverter para o uso do certificado padrão da API S3 para conexões de cliente S3 para nós de storage. No entanto, você não pode usar o certificado padrão da API S3 para um endpoint do balanceador de carga.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 API certificate**.
3. Selecione **Use default certificate** (usar certificado padrão).

   Quando você restaura a versão padrão do certificado global da API S3, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. O certificado padrão da API S3 será usado para novas conexões de cliente S3 subsequentes aos nós de storage.

4. Selecione **OK** para confirmar o aviso e restaurar o certificado padrão da API S3.

   Se você tiver permissão de acesso root e o certificado de API S3 personalizado tiver sido usado para conexões de endpoint do balanceador de carga, uma lista será exibida de endpoints do balanceador de carga que não estarão mais acessíveis usando o certificado de API S3 padrão. Aceda a "Configurar pontos de extremidade do balanceador de carga" para editar ou remover os endpoints afetados.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

Faça o download ou copie o certificado API S3

Você pode salvar ou copiar o conteúdo do certificado API S3 para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 API certificate**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA `.pem`. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote CA**.

   Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

   Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Informações relacionadas

- "USE A API REST DO S3"
- "Configurar nomes de domínio de endpoint S3"

Copie o certificado da CA de Grade

O StorageGRID usa uma autoridade de certificação interna (CA) para proteger o tráfego interno. Este certificado não muda se você carregar seus próprios certificados.

Antes de começar

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

Sobre esta tarefa

Se um certificado de servidor personalizado tiver sido configurado, os aplicativos cliente devem verificar o servidor usando o certificado de servidor personalizado. Eles não devem copiar o certificado da CA do sistema StorageGRID.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Grid CA**.

2. Na seção **Certificate PEM**, baixe ou copie o certificado.

Transfira o ficheiro de certificado

Transfira o ficheiro de certificado `.pem`.

a. Selecione **Baixar certificado**.

b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado PEM

Copie o texto do certificado para colar em outro lugar.

a. Selecione **Copiar certificado PEM**.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

Para clientes S3 que executam validação estrita de nome de host e não suportam a desativação estrita de validação de nome de host, como clientes ONTAP que usam FabricPool, você pode gerar ou carregar um certificado de servidor ao configurar o ponto de extremidade do balanceador de carga.

Antes de começar

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

Sobre esta tarefa

Ao criar um endpoint de balanceador de carga, você pode gerar um certificado de servidor autoassinado ou carregar um certificado assinado por uma autoridade de certificação (CA) conhecida. Em ambientes de produção, você deve usar um certificado assinado por uma CA conhecida. Os certificados assinados por uma CA podem ser girados sem interrupções. Eles também são mais seguros porque fornecem melhor proteção contra ataques do homem no meio.

As etapas a seguir fornecem diretrizes gerais para clientes S3 que usam FabricPool. Para obter informações e procedimentos mais detalhados, "Configurar o StorageGRID para FabricPool"consulte .

Passos

1. Opcionalmente, configure um grupo de alta disponibilidade (HA) para uso do FabricPool.
2. Crie um ponto de extremidade do balanceador de carga S3 para o FabricPool usar.

   Quando você cria um endpoint do balanceador de carga HTTPS, é solicitado que você carregue o certificado do servidor, a chave privada do certificado e o pacote opcional da CA.

3. Anexar o StorageGRID como uma categoria de nuvem no ONTAP.

   Especifique a porta de endpoint do balanceador de carga e o nome de domínio totalmente qualificado usado no certificado da CA que você carregou. Em seguida, forneça o certificado CA.

   Se uma CA intermediária tiver emitido o certificado StorageGRID, você deverá fornecer o certificado de CA intermediário. Se o certificado StorageGRID tiver sido emitido diretamente pela CA raiz, você deverá fornecer o certificado CA raiz.

Configurar certificados de cliente

Os certificados de cliente permitem que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus, fornecendo uma maneira segura para que ferramentas externas monitorem o StorageGRID.

Se você precisar acessar o StorageGRID usando uma ferramenta de monitoramento externa, você deve carregar ou gerar um certificado de cliente usando o Gerenciador de Grade e copiar as informações do certificado para a ferramenta externa.

"Gerenciar certificados de segurança"Consulte e "Configurar certificados de servidor personalizados".

Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **expiração de certificados de cliente configurados na página certificados** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de validade do certificado do cliente na guia Client.

Se você estiver usando um servidor de gerenciamento de chaves (KMS) para proteger os dados em nós de dispositivo especialmente configurados, consulte as informações específicas sobre "Carregar um certificado de cliente KMS"o .

Antes de começar

- Você tem permissão de acesso root.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Para configurar um certificado de cliente:
  - Você tem o endereço IP ou o nome de domínio do nó Admin.
  - Se tiver configurado o certificado da interface de gerenciamento do StorageGRID, você terá a CA, o certificado do cliente e a chave privada usadas para configurar o certificado da interface de gerenciamento.
  - Para carregar o seu próprio certificado, a chave privada do certificado está disponível no seu computador local.
  - A chave privada deve ter sido salva ou gravada no momento em que foi criada. Se você não tiver a chave privada original, você deve criar uma nova.
- Para editar um certificado de cliente:
  - Você tem o endereço IP ou o nome de domínio do nó Admin.
  - Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se usada) estão disponíveis no computador local.

Adicionar certificados de cliente

Para adicionar o certificado de cliente, use um destes procedimentos:

- Certificado de interface de gerenciamento já configurado
- Certificado de cliente emitido pela CA
- Certificado gerado pelo Grid Manager

Certificado de interface de gerenciamento já configurado

Use este procedimento para adicionar um certificado de cliente se um certificado de interface de gerenciamento já estiver configurado usando uma CA fornecida pelo cliente, um certificado de cliente e uma chave privada.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
5. Selecione **continuar**.
6. Para a etapa **Anexar certificados**, carregue o certificado da interface de gerenciamento.
   a. Selecione **carregar certificado**.
   b. Selecione **Procurar** e selecione o ficheiro de certificado da interface de gestão (`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

      O novo certificado é exibido na guia Cliente.
7. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Certificado de cliente emitido pela CA

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use um certificado de cliente emitido pela CA e uma chave privada.

Passos

1. Execute as etapas para "configurar um certificado de interface de gerenciamento".
2. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
3. Selecione **Adicionar**.
4. Introduza um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione

permitir prometheus.

6. Selecione **continuar**.
7. Para a etapa **Anexar certificados**, carregue o certificado do cliente, a chave privada e os arquivos do pacote CA:
   a. Selecione **carregar certificado**.
   b. Selecione **Procurar** e selecione o certificado do cliente, a chave privada e os ficheiros do pacote CA (`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

      Os novos certificados aparecem na guia Cliente.
8. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Certificado gerado pelo Grid Manager

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use a função gerar certificado no Gerenciador de Grade.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
5. Selecione **continuar**.
6. Para a etapa **Anexar certificados**, selecione **gerar certificado**.
7. Especifique as informações do certificado:
   - **Assunto** (opcional): X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
   - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que é gerado.
   - * Adicionar extensões de uso de chave*: Se selecionado (padrão e recomendado), o uso de chave e extensões de uso de chave estendidas são adicionados ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe essa caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.
8. Selecione **Generate**.
9. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

Não será possível visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou transfira a chave para um local seguro.

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
- Selecione **Download private key** para salvar a chave privada como um arquivo.

  Especifique o nome do arquivo de chave privada e o local de download.

10. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

    O novo certificado é exibido na guia Cliente.

11. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Global**.
12. Selecione **certificado de interface de gestão**.
13. Selecione **usar certificado personalizado**.
14. Carregue os arquivos certificate.pem e private_key.pem da detalhes do certificado do cliente etapa. Não há necessidade de carregar o pacote CA.
    a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
    b. Carregar cada ficheiro de certificado (`.pem`).
    c. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.

       O novo certificado é exibido na página de certificado da Interface de Gerenciamento.

15. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Configure uma ferramenta de monitoramento externa

Passos

1. Configure as seguintes configurações em sua ferramenta de monitoramento externo, como Grafana.
   a. **Nome**: Insira um nome para a conexão.

      O StorageGRID não requer essas informações, mas você deve fornecer um nome para testar a conexão.

   b. **URL**: Insira o nome de domínio ou o endereço IP do nó Admin. Especifique HTTPS e porta 9091.

      Por exemplo: `https://admin-node.example.com:9091`

   c. Ative **TLS Client Auth** e **com CA Cert**.
   d. Em Detalhes de autenticação TLS/SSL, copie e cole

- A interface de gerenciamento certificado CA para **CA Cert**
- O certificado de cliente para **Cert de cliente**
- A chave privada para **chave do cliente**

e. **ServerName**: Insira o nome de domínio do nó Admin.

   Servername deve corresponder ao nome de domínio como aparece no certificado da interface de gerenciamento.

2. Salve e teste o certificado e a chave privada que você copiou do StorageGRID ou de um arquivo local.

   Agora você pode acessar as métricas Prometheus do StorageGRID com sua ferramenta de monitoramento externo.

   Para obter informações sobre as métricas, consulte o "Instruções para monitorar o StorageGRID".

Editar certificados de cliente

Você pode editar um certificado de cliente administrador para alterar seu nome, ativar ou desativar o acesso Prometheus ou carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.

   As datas de expiração do certificado e as permissões de acesso Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta será acionado.

2. Selecione o certificado que pretende editar.
3. Selecione **Editar** e, em seguida, selecione **Editar nome e permissão**
4. Introduza um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
6. Selecione **continuar** para salvar o certificado no Gerenciador de Grade.

   O certificado atualizado é exibido na guia Cliente.

Anexar novo certificado de cliente

Você pode carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.

   As datas de expiração do certificado e as permissões de acesso Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta será acionado.

2. Selecione o certificado que pretende editar.
3. Selecione **Editar** e, em seguida, selecione uma opção de edição.

Carregar certificado

Copie o texto do certificado para colar em outro lugar.

a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.

b. Carregue o nome do certificado do cliente (`.pem`).

   Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   - Selecione **Transferir certificado** para guardar o ficheiro de certificado.

     Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

   O certificado atualizado é exibido na guia Cliente.

Gerar certificado

Gere o texto do certificado para colar em outro lugar.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

   - **Assunto** (opcional): X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
   - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que é gerado.
   - * Adicionar extensões de uso de chave*: Se selecionado (padrão e recomendado), o uso de chave e extensões de uso de chave estendidas são adicionados ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe essa caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   Não será possível visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou transfira a chave para um local seguro.

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
- Selecione **Download private key** para salvar a chave privada como um arquivo.

  Especifique o nome do arquivo de chave privada e o local de download.

e. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

Baixe ou copie certificados de cliente

Você pode baixar ou copiar um certificado de cliente para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende copiar ou transferir.
3. Baixe ou copie o certificado.

Transfira o ficheiro de certificado

Transfira o ficheiro de certificado `.pem`.

a. Selecione **Baixar certificado**.
b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado

Copie o texto do certificado para colar em outro lugar.

a. Selecione **Copiar certificado PEM**.
b. Cole o certificado copiado em um editor de texto.
c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Remover certificados de cliente

Se você não precisar mais de um certificado de cliente administrador, poderá removê-lo.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende remover.
3. Selecione **Delete** e confirme.

> Para remover até 10 certificados, selecione cada certificado a ser removido na guia Cliente e selecione **ações** > **Excluir**.

Depois que um certificado é removido, os clientes que usaram o certificado devem especificar um novo certificado de cliente para acessar o banco de dados do StorageGRID Prometheus.

Configure as definições de segurança

Gerencie a política TLS e SSH

A política TLS e SSH determina quais protocolos e cifras são usados para estabelecer conexões TLS seguras com aplicativos cliente e conexões SSH seguras com serviços StorageGRID internos.

A política de segurança controla como TLS e SSH criptografam dados em movimento. Em geral, use a política de compatibilidade moderna (padrão), a menos que seu sistema precise ser compatível com critérios comuns ou que você precise usar outras cifras.

> Alguns serviços do StorageGRID não foram atualizados para usar as cifras nessas políticas.

Antes de começar

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

Selecione uma política de segurança

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.

   A guia **TLS e políticas SSH** mostra as políticas disponíveis. A política atualmente ativa é anotada por uma marca de seleção verde no bloco de política.

2. Revise os blocos para saber mais sobre as políticas disponíveis.

Política	Descrição
Compatibilidade moderna (padrão)	Use a política padrão se você precisar de criptografia forte e a menos que você tenha requisitos especiais. Esta política é compatível com a maioria dos clientes TLS e SSH.
Compatibilidade legada	Use esta política se precisar de opções de compatibilidade adicionais para clientes mais antigos. As opções adicionais desta política podem torná-la menos segura do que a política de compatibilidade moderna.
Critérios comuns	Use esta política se você precisar da certificação Common Criteria.
FIPS rigoroso	Use esta política se você precisar de certificação Common Criteria e precisar usar o módulo de segurança criptográfica NetApp 3.0.8 para conexões de clientes externos para terminais de balanceador de carga, Gerenciador de locatário e Gerenciador de Grade. O uso desta política pode reduzir o desempenho. **Nota**: Depois de selecionar esta política, todos os nós devem "reinicializado de uma forma rolling"ativar o módulo de segurança criptográfica do NetApp. Utilize **Maintenance** > **Rolling Reboot** para iniciar e monitorizar reinicializações.
Personalizado	Crie uma política personalizada se você precisar aplicar seus próprios cifras.

3. Para ver detalhes sobre as cifras, protocolos e algoritmos de cada política, selecione **Exibir detalhes**.
4. Para alterar a política atual, selecione **Use policy**.

   Uma marca de seleção verde aparece ao lado de **política atual** no bloco de política.

Crie uma política de segurança personalizada

Você pode criar uma política personalizada se precisar aplicar suas próprias cifras.

Passos

1. No bloco da política que é o mais semelhante à política personalizada que você deseja criar, selecione **Exibir detalhes**.
2. Selecione **Copiar para a área de transferência** e, em seguida, selecione **Cancelar**.

3. No bloco **Política personalizada**, selecione **Configurar e usar**.
4. Cole o JSON que você copiou e faça as alterações necessárias.
5. Selecione **Use policy**.

   Uma marca de seleção verde aparece ao lado de **Current policy** no mosaico Custom policy (Política personalizada).

6. Opcionalmente, selecione **Editar configuração** para fazer mais alterações na nova política personalizada.

Reverter temporariamente para a política de segurança padrão

Se você tiver configurado uma política de segurança personalizada, talvez não consiga entrar no Gerenciador de Grade se a diretiva TLS configurada for incompatível com o "certificado de servidor configurado".

Você pode reverter temporariamente para a política de segurança padrão.

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.
   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 comando:

   ```
   restore-default-cipher-configurations
   ```

3. Em um navegador da Web, acesse o Gerenciador de Grade no mesmo nó Admin.
4. Siga as etapas em Selecione uma política de segurança para configurar a política novamente.

Configurar a segurança de rede e de objetos

Você pode configurar a segurança de rede e de objetos para criptografar objetos armazenados, para impedir determinadas solicitações S3 ou para permitir que conexões de cliente aos nós de armazenamento usem HTTP em vez de HTTPS.

Criptografia de objeto armazenado

A criptografia de objeto armazenado permite a criptografia de todos os dados de objeto à medida que são ingeridos através do S3. Por padrão, os objetos armazenados não são criptografados, mas você pode optar por criptografar objetos usando o algoritmo de criptografia AES-128 ou AES-256. Quando você ativa a configuração, todos os objetos recém-ingeridos são criptografados, mas nenhuma alteração é feita aos objetos armazenados existentes. Se desativar a encriptação, os objetos atualmente encriptados permanecem encriptados, mas os objetos recentemente ingeridos não são encriptados.

A configuração de criptografia de objeto armazenado se aplica somente a objetos S3 que não tenham sido criptografados por criptografia no nível do bucket ou no nível do objeto.

Para obter mais detalhes sobre os métodos de criptografia StorageGRID, "Reveja os métodos de encriptação StorageGRID"consulte .

Impedir a modificação do cliente

Impedir a modificação do cliente é uma configuração de todo o sistema. Quando a opção **Prevent client modification** é selecionada, as seguintes solicitações são negadas.

S3 API REST

- DeleteBucket Requests
- Quaisquer solicitações para modificar os dados de um objeto existente, metadados definidos pelo usuário ou marcação de objeto S3

Ative HTTP para conexões de nó de armazenamento

Por padrão, os aplicativos clientes usam o protocolo de rede HTTPS para quaisquer conexões diretas aos nós de storage. Opcionalmente, você pode ativar o HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

Use HTTP para conexões de nó de armazenamento somente se os clientes S3 precisarem fazer conexões HTTP diretamente aos nós de armazenamento. Não é necessário usar essa opção para clientes que usam somente conexões HTTPS ou para clientes que se conetam ao serviço Load Balancer (porque você pode "configure cada ponto de extremidade do balanceador de carga"usar HTTP ou HTTPS).

"Resumo: Endereços IP e portas para conexões de clientes"Consulte para saber quais portas os clientes S3 usam ao se conetar a nós de armazenamento usando HTTP ou HTTPS.

Selecione as opções

Antes de começar

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

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.
2. Selecione a guia **rede e objetos**.
3. Para criptografia de objetos armazenados, use a configuração **nenhum** (padrão) se você não quiser que objetos armazenados sejam criptografados ou selecione **AES-128** ou **AES-256** para criptografar objetos armazenados.
4. Opcionalmente, selecione **impedir modificação do cliente** se você quiser impedir que clientes S3 façam solicitações específicas.

   Se alterar esta definição, demora cerca de um minuto para a nova definição ser aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

5. Opcionalmente, selecione **Ativar HTTP para conexões de nó de armazenamento** se os clientes se conetarem diretamente aos nós de armazenamento e você quiser usar conexões HTTP.

   Tenha cuidado ao ativar o HTTP para uma grade de produção porque as solicitações serão enviadas sem criptografia.

6. Selecione **Guardar**.

Alterar as definições de segurança da interface

As configurações de segurança da interface permitem que você controle se os usuários estão desconetados se estiverem inativos por mais do que o tempo especificado e se um rastreamento de pilha está incluído nas respostas de erro da API.

Antes de começar

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

Sobre esta tarefa

A página **Configurações de segurança** inclui as configurações **tempo limite de inatividade do navegador** e **rastreamento de pilha da API de gerenciamento**.

Tempo limite de inatividade do navegador

Indica por quanto tempo o navegador de um usuário pode estar inativo antes de o usuário ser desconetado. O padrão é 15 minutos.

O tempo limite de inatividade do navegador também é controlado pelo seguinte:

- Um temporizador StorageGRID separado, não configurável, incluído para a segurança do sistema. O token de autenticação de cada usuário expira 16 horas após o login do usuário. Quando a autenticação de um usuário expira, esse usuário é desconetado automaticamente, mesmo que o tempo limite de inatividade do navegador esteja desativado ou o valor do tempo limite do navegador não tenha sido atingido. Para renovar o token, o usuário deve entrar novamente.
- Configurações de tempo limite para o provedor de identidade, supondo que o logon único (SSO) esteja ativado para o StorageGRID.

  Se o SSO estiver ativado e o navegador de um usuário expirar, o usuário deverá inserir novamente suas credenciais SSO para acessar o StorageGRID novamente. "Configurar o logon único"Consulte .

Rastreamento de pilha de API de gerenciamento

Controla se um rastreamento de pilha é retornado nas respostas de erro do Grid Manager e do Tenant Manager API.

Essa opção está desativada por padrão, mas talvez você queira habilitar essa funcionalidade para um ambiente de teste. Em geral, você deve deixar o rastreamento de pilha desativado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.
2. Selecione a guia **Interface**.
3. Para alterar a configuração de tempo limite de inatividade do navegador:
   a. Expanda o acordeão.
   b. Para alterar o período de tempo limite, especifique um valor entre 60 segundos e 7 dias. O tempo limite padrão é de 15 minutos.
   c. Para desativar este recurso, desmarque a caixa de seleção.
   d. Selecione **Guardar**.

      A nova configuração não afeta os usuários que estão conetados no momento. Os usuários devem entrar novamente ou atualizar seus navegadores para que a nova configuração de tempo limite entre em vigor.
4. Para alterar a configuração de rastreamento de pilha da API de gerenciamento:
   a. Expanda o acordeão.
   b. Marque a caixa de seleção para retornar um rastreamento de pilha nas respostas de erro do Grid Manager e do Tenant Manager API.

      Deixe o rastreamento de pilha desativado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

   c. Selecione **Guardar**.

Configurar servidores de gerenciamento de chaves

O que é um servidor de gerenciamento de chaves (KMS)?

Um servidor de gerenciamento de chaves (KMS) é um sistema externo de terceiros que fornece chaves de criptografia para nós de dispositivos StorageGRID no site associado do StorageGRID usando o Protocolo de interoperabilidade de Gerenciamento de chaves (KMIP).

O StorageGRID suporta apenas determinados servidores de gerenciamento de chaves. Para obter uma lista de produtos e versões compatíveis, use o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para qualquer nó de dispositivo StorageGRID que tenha a configuração **criptografia de nó** ativada durante a instalação. O uso de servidores de gerenciamento de chaves com esses nós de dispositivo permite que você proteja seus dados mesmo que um dispositivo seja removido do data center. Depois que os volumes do dispositivo são criptografados, você não pode acessar nenhum dado no dispositivo, a menos que o nó

possa se comunicar com o KMS.

> O StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar os nós do dispositivo. Se você pretende usar um servidor de gerenciamento de chaves externo para proteger dados do StorageGRID, você deve entender como configurar esse servidor e entender como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo dessas instruções. Se precisar de ajuda, consulte a documentação do servidor de gerenciamento de chaves ou entre em Contato com o suporte técnico.

KMS e configuração do dispositivo

Antes de usar um servidor de gerenciamento de chaves (KMS) para proteger dados do StorageGRID nos nós do dispositivo, você deve concluir duas tarefas de configuração: Configurar um ou mais servidores KMS e habilitar a criptografia de nós para os nós do dispositivo. Quando essas duas tarefas de configuração são concluídas, o processo de gerenciamento de chaves ocorre automaticamente.

O fluxograma mostra as etapas de alto nível para usar um KMS para proteger os dados do StorageGRID em nós do dispositivo.

O fluxograma mostra a configuração do KMS e a configuração do appliance ocorrendo em paralelo; no entanto, você pode configurar os servidores de gerenciamento de chaves antes ou depois de habilitar a criptografia de nó para novos nós de dispositivo, com base em seus requisitos.

Configurar o servidor de gerenciamento de chaves (KMS)

A configuração de um servidor de gerenciamento de chaves inclui as seguintes etapas de alto nível.

Passo	Consulte
Acesse o software KMS e adicione um cliente para StorageGRID a cada cluster KMS ou KMS.	"Configure o StorageGRID como um cliente no KMS"
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configure o StorageGRID como um cliente no KMS"
Adicione o KMS ao Gerenciador de Grade, atribua-o a um único site ou a um grupo padrão de sites, carregue os certificados necessários e salve a configuração do KMS.	"Adicionar um servidor de gerenciamento de chaves (KMS)"

Configure o aparelho

A configuração de um nó de dispositivo para uso do KMS inclui os seguintes passos de alto nível.

1. Durante o estágio de configuração de hardware da instalação do dispositivo, use o Instalador de dispositivos StorageGRID para ativar a configuração **criptografia de nó** para o dispositivo.

Não é possível ativar a configuração **criptografia de nó** depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não têm criptografia de nó ativada.

2. Execute o Instalador de dispositivos StorageGRID. Durante a instalação, uma chave de criptografia de dados aleatórios (DEK) é atribuída a cada volume de dispositivo, da seguinte forma:
   - Os DEKs são usados para criptografar os dados em cada volume. Essas chaves são geradas usando a criptografia de disco LUKS (Unified Key Setup) do Linux no sistema operacional do dispositivo e não podem ser alteradas.
   - Cada DEK individual é criptografado por uma chave mestra de criptografia (KEK). O KEK inicial é uma chave temporária que criptografa os DEKs até que o dispositivo possa se conetar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

```
https://docs.netapp.com/us-en/storagegrid-
appliances/installconfig/optional-enabling-node-
encryption.html["Habilite a criptografia do nó"^]Consulte para obter
detalhes.
```

Processo de criptografia de gerenciamento de chaves (ocorre automaticamente)

A criptografia de gerenciamento de chaves inclui as seguintes etapas de alto nível que são executadas automaticamente.

1. Quando você instala um dispositivo que tem criptografia de nó ativada na grade, o StorageGRID determina se existe uma configuração de KMS para o site que contém o novo nó.
   - Se um KMS já tiver sido configurado para o site, o appliance receberá a configuração do KMS.
   - Se um KMS ainda não tiver sido configurado para o site, os dados no appliance continuarão a ser criptografados pelo KEK temporário até que você configure um KMS para o site e o appliance receba a configuração do KMS.
2. O dispositivo usa a configuração KMS para se conetar ao KMS e solicitar uma chave de criptografia.
3. O KMS envia uma chave de criptografia para o dispositivo. A nova chave do KMS substitui o KEK temporário e agora é usada para criptografar e descriptografar os DEKs para os volumes do dispositivo.

Todos os dados existentes antes do nó de dispositivo criptografado se conetarem ao KMS configurado são criptografados com uma chave temporária. No entanto, os volumes do dispositivo não devem ser considerados protegidos contra a remoção do data center até que a chave temporária seja substituída pela chave de criptografia KMS.

4. Se o aparelho estiver ligado ou reinicializado, ele se reconeta ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não pode sobreviver a uma perda de energia ou a uma reinicialização.

Considerações e requisitos para usar um servidor de gerenciamento de chaves

Antes de configurar um servidor de gerenciamento de chaves externo (KMS), você deve entender as considerações e os requisitos.

Qual versão do KMIP é suportada?

O StorageGRID é compatível com KMIP versão 1,4.

"Especificação do protocolo de interoperabilidade de gerenciamento de chaves versão 1,4"

Quais são as considerações de rede?

As configurações do firewall de rede devem permitir que cada nó do dispositivo se comunique através da porta usada para comunicações KMIP (Key Management Interoperability Protocol). A porta KMIP padrão é 5696.

Você deve garantir que cada nó de dispositivo que usa criptografia de nó tenha acesso de rede ao cluster KMS ou KMS configurado para o site.

Quais versões do TLS são suportadas?

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID pode dar suporte ao protocolo TLS 1,2 ou TLS 1,3 quando faz conexões KMIP a um cluster KMS ou KMS, com base no suporte do KMS e no qual "Política TLS e SSH" você está usando.

O StorageGRID negocia o protocolo e a cifra (TLS 1,2) ou conjunto de cifra (TLS 1,3) com o KMS quando faz a conexão. Para ver quais versões de protocolo e conjuntos de cifras/cifras estão disponíveis, consulte `tlsOutbound` a seção da política TLS e SSH ativa da grade (**CONFIGURATION** > **Security Security Security Security settings**).

Quais aparelhos são suportados?

Você pode usar um servidor de gerenciamento de chaves (KMS) para gerenciar chaves de criptografia para qualquer dispositivo StorageGRID em sua grade que tenha a configuração **criptografia de nó** ativada. Esta definição só pode ser ativada durante a fase de configuração de hardware da instalação do dispositivo utilizando o Instalador de dispositivos StorageGRID.

> Não é possível ativar a criptografia de nó depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não têm a criptografia de nó ativada.

Você pode usar o KMS configurado para dispositivos StorageGRID e nós de dispositivo.

Não é possível usar o KMS configurado para nós baseados em software (não-appliance), incluindo o seguinte:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados nos mecanismos de contêiner em hosts Linux

Os nós implantados nessas outras plataformas podem usar criptografia fora do StorageGRID no armazenamento de dados ou no nível de disco.

Quando devo configurar servidores de gerenciamento de chaves?

Para uma nova instalação, você normalmente deve configurar um ou mais servidores de gerenciamento de chaves no Gerenciador de Grade antes de criar locatários. Essa ordem garante que os nós sejam protegidos antes que quaisquer dados de objeto sejam armazenados neles.

Você pode configurar os servidores de gerenciamento de chaves no Gerenciador de Grade antes ou depois

de instalar os nós do dispositivo.

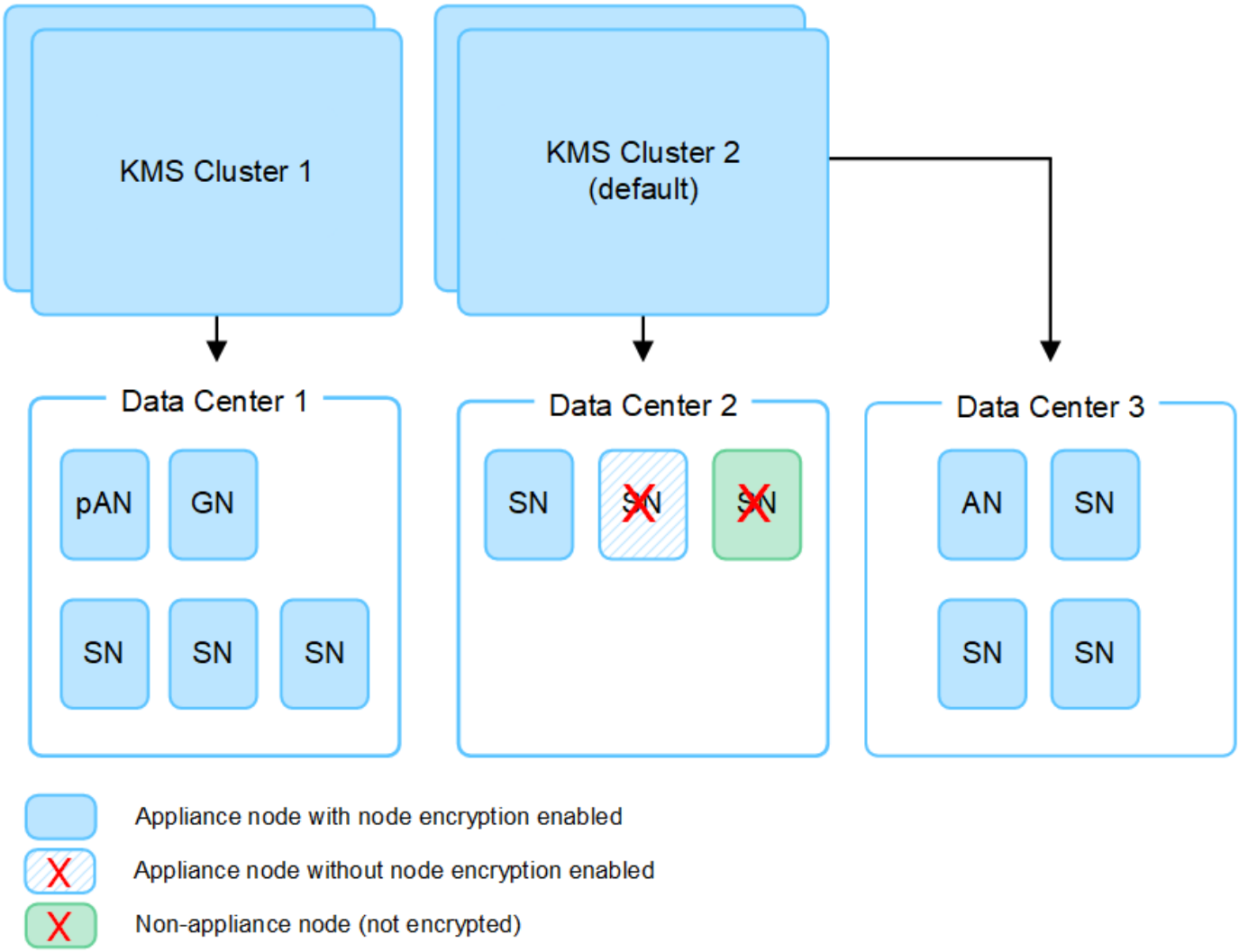
Quantos servidores de gerenciamento de chaves eu preciso?

Você pode configurar um ou mais servidores de gerenciamento de chaves externos para fornecer chaves de criptografia aos nós do dispositivo em seu sistema StorageGRID. Cada KMS fornece uma única chave de criptografia para os nós do dispositivo StorageGRID em um único local ou em um grupo de sites.

O StorageGRID é compatível com o uso de clusters KMS. Cada cluster KMS contém vários servidores de gerenciamento de chaves replicados que compartilham configurações e chaves de criptografia. O uso de clusters KMS para gerenciamento de chaves é recomendado porque melhora os recursos de failover de uma configuração de alta disponibilidade.

Por exemplo, suponha que seu sistema StorageGRID tenha três locais de data center. Você pode configurar um cluster KMS para fornecer uma chave para todos os nós do dispositivo no Data Center 1 e um segundo cluster KMS para fornecer uma chave para todos os nós do dispositivo em todos os outros locais. Ao adicionar o segundo cluster KMS, você pode configurar um KMS padrão para o Data Center 2 e o Data Center 3.

Observe que não é possível usar um KMS para nós que não sejam do dispositivo ou para nenhum nó de dispositivo que não tenha a configuração **criptografia do nó** ativada durante a instalação.



O que acontece quando uma chave é girada?

Como uma prática recomendada de segurança, você deve ser usado periodicamente "rode a chave de encriptação"por cada KMS configurado.

Quando a nova versão da chave estiver disponível:

- Ele é distribuído automaticamente para os nós de dispositivos criptografados no site ou sites associados ao KMS. A distribuição deve ocorrer dentro de uma hora de quando a chave é girada.
- Se o nó do dispositivo criptografado estiver offline quando a nova versão da chave for distribuída, o nó receberá a nova chave assim que for reinicializada.
- Se a nova versão de chave não puder ser usada para criptografar volumes de appliance por qualquer motivo, o alerta **rotação da chave de criptografia KMS falhou** é acionado para o nó do appliance. Talvez seja necessário entrar em Contato com o suporte técnico para obter ajuda na resolução desse alerta.

Posso reutilizar um nó de appliance depois que ele foi criptografado?

Se você precisar instalar um dispositivo criptografado em outro sistema StorageGRID, primeiro será necessário desativar o nó da grade para mover dados de objeto para outro nó. Em seguida, você pode usar o Instalador de dispositivos StorageGRID para "Limpe a configuração do KMS". A limpeza da configuração KMS desativa a configuração **criptografia de nó** e remove a associação entre o nó do dispositivo e a configuração KMS para o site StorageGRID.

> Sem acesso à chave de criptografia KMS, todos os dados que permanecem no dispositivo não podem mais ser acessados e ficam permanentemente bloqueados.

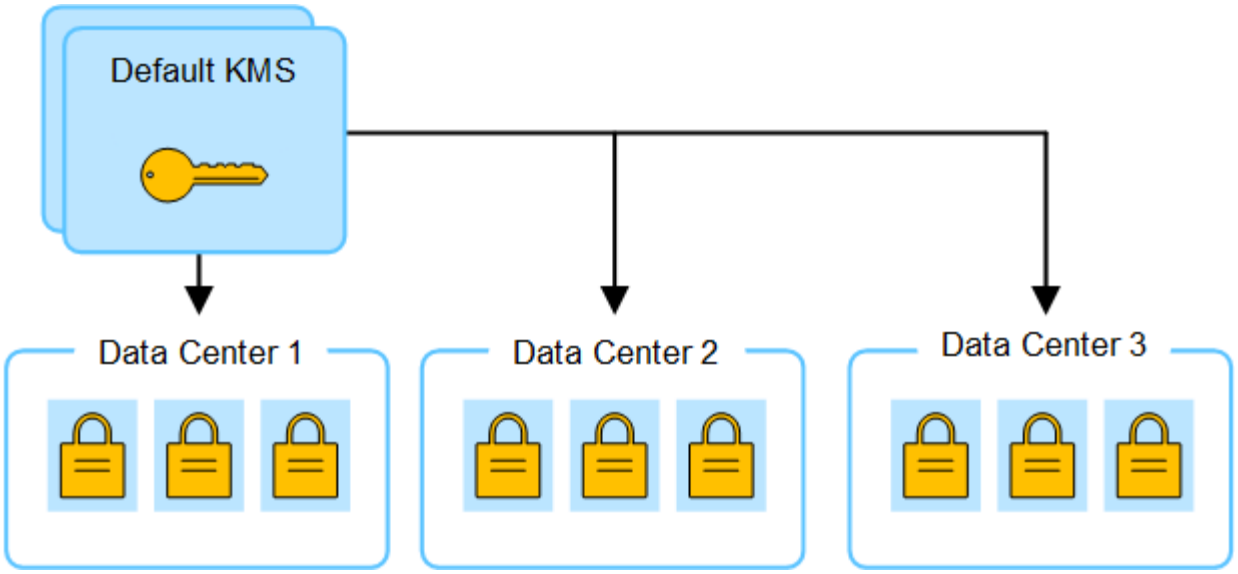
Considerações para alterar o KMS para um site

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do dispositivo em um único local ou em um grupo de sites. Se você precisar alterar qual KMS é usado para um site, talvez seja necessário copiar a chave de criptografia de um KMS para outro.

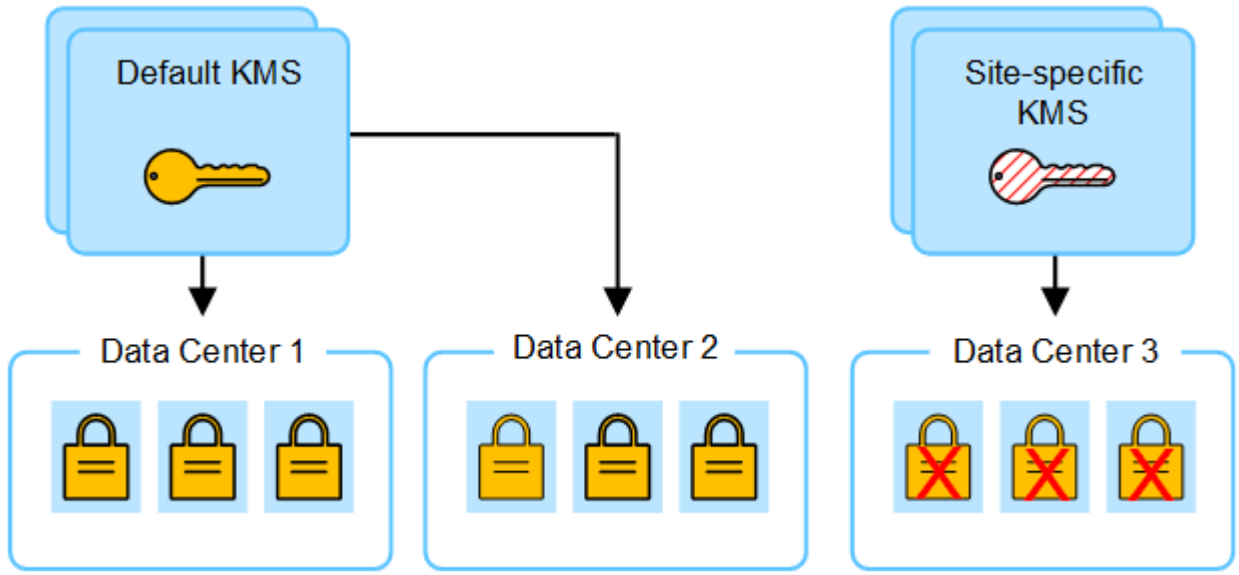
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS. Você deve garantir que o KMS tenha a chave correta para descriptografar os nós de dispositivo criptografado no local.

Por exemplo:

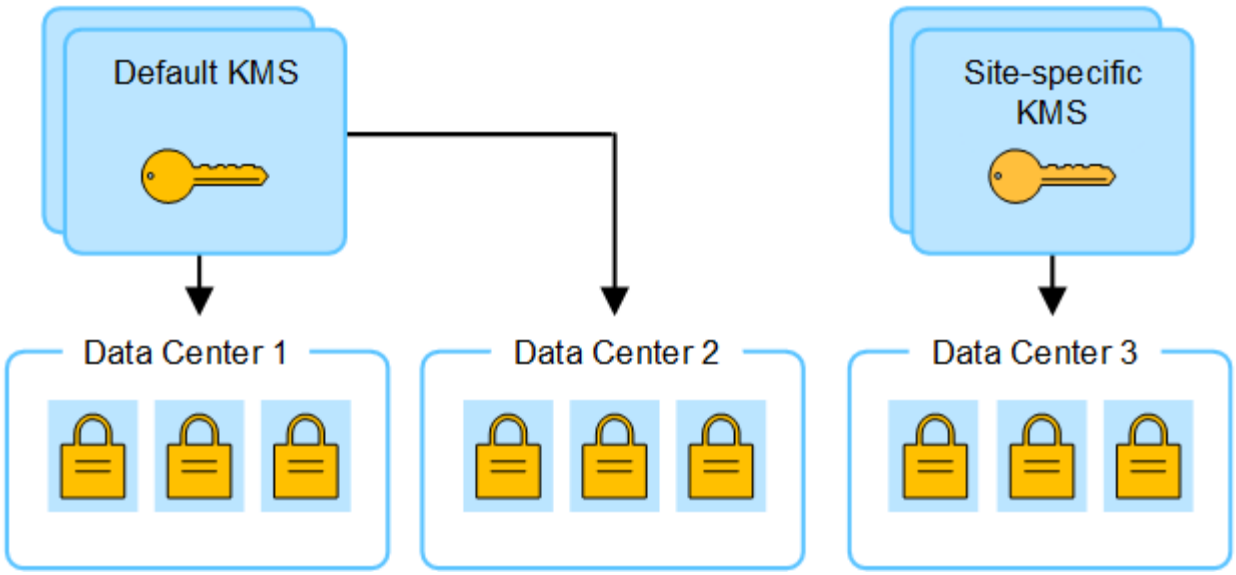
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar os nós do dispositivo em todos os locais. Esta mesma chave também deve ser usada para descriptografar esses aparelhos.



3. Você decide adicionar um KMS específico para um site (Data Center 3 na figura). No entanto, como os nós do appliance já estão criptografados, um erro de validação ocorre quando você tenta salvar a configuração para o KMS específico do site. O erro ocorre porque o KMS específico do site não tem a chave correta para descriptografar os nós nesse site.



4. Para resolver o problema, copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. (Tecnicamente, você copia a chave original para uma nova chave com o mesmo alias. A chave original torna-se uma versão anterior da nova chave.) O KMS específico do local agora tem a chave correta para descriptografar os nós do appliance no Data Center 3, para que ele possa ser salvo no StorageGRID.



Casos de uso para alterar qual KMS é usado para um site

A tabela resume as etapas necessárias para os casos mais comuns para alterar o KMS de um site.

Caso de uso para alterar o KMS de um site	Passos necessários
Você tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como KMS padrão.	Edite o KMS específico do site. No campo **gerencia chaves para**, selecione **Sites não gerenciados por outro KMS (KMS padrão)**. O KMS específico do site agora será usado como o KMS padrão. Ele se aplicará a quaisquer sites que não tenham um KMS dedicado. "Editar um servidor de gerenciamento de chaves (KMS)"
Você tem um KMS padrão e adiciona um novo site em uma expansão. Você não quer usar o KMS padrão para o novo site.	1. Se os nós de appliance no novo site já tiverem sido criptografados pelo KMS padrão, use o software KMS para copiar a versão atual da chave de criptografia do KMS padrão para um novo KMS. 2. Usando o Gerenciador de Grade, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você quer que o KMS para um site use um servidor diferente.	1. Se os nós do dispositivo no local já tiverem sido criptografados pelo KMS existente, use o software KMS para copiar a versão atual da chave de criptografia do KMS existente para o novo KMS. 2. Usando o Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome de host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configure o StorageGRID como um cliente no KMS

Você deve configurar o StorageGRID como um cliente para cada servidor de gerenciamento de chaves externo ou cluster KMS antes de poder adicionar o KMS ao

StorageGRID.

> Estas instruções se aplicam ao Thales CipherTrust Manager e Hashicorp Vault. Para obter uma lista de produtos e versões compatíveis, use o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

Passos

1. A partir do software KMS, crie um cliente StorageGRID para cada cluster KMS ou KMS que você pretende usar.

   Cada KMS gerencia uma única chave de criptografia para os nós do StorageGRID Appliances em um único local ou em um grupo de sites.

2. Crie uma chave usando um dos seguintes dois métodos:
   - Use a página de gerenciamento de chaves do seu produto KMS. Crie uma chave de criptografia AES para cada cluster KMS ou KMS.

     A chave de criptografia deve ter 2.048 bits ou mais e deve ser exportável.

   - Peça ao StorageGRID que crie a chave. Você será solicitado quando testar e salvar após "carregar certificados de cliente".
3. Registre as seguintes informações para cada cluster KMS ou KMS.

   Você precisa dessas informações quando adicionar o KMS ao StorageGRID:

   - Nome do host ou endereço IP para cada servidor.
   - Porta KMIP usada pelo KMS.
   - Alias de chave para a chave de criptografia no KMS.
4. Para cada cluster KMS ou KMS, obtenha um certificado de servidor assinado por uma autoridade de certificação (CA) ou um pacote de certificados que contém cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

   O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

   - O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM).
   - O campo Nome alternativo do assunto (SAN) em cada certificado de servidor deve incluir o nome de domínio totalmente qualificado (FQDN) ou o endereço IP ao qual o StorageGRID se conetará.

     > Ao configurar o KMS no StorageGRID, você deve inserir os mesmos FQDNs ou endereços IP no campo **Nome do host**.

   - O certificado do servidor deve corresponder ao certificado usado pela interface KMIP do KMS, que normalmente usa a porta 5696.
5. Obtenha o certificado de cliente público emitido para o StorageGRID pelo KMS externo e a chave privada para o certificado de cliente.

   O certificado de cliente permite que o StorageGRID se autentique no KMS.

Você usa o assistente do servidor de gerenciamento de chaves do StorageGRID para adicionar cada cluster KMS ou KMS.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você tem "Configurado o StorageGRID como um cliente no KMS", e você tem as informações necessárias para cada cluster KMS ou KMS.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Sobre esta tarefa

Se possível, configure qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. Se você criar o KMS padrão primeiro, todos os dispositivos criptografados por nó na grade serão criptografados pelo KMS padrão. Se você quiser criar um KMS específico do site mais tarde, primeiro copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. "Considerações para alterar o KMS para um site"Consulte para obter detalhes.

Passo 1: KMS detalhes

Na Etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves, você fornece detalhes sobre o cluster KMS ou KMS.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página servidor de gerenciamento de chaves é exibida com a guia Detalhes da configuração selecionada.

2. Selecione **criar**.

   A etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

3. Insira as seguintes informações para o KMS e o cliente StorageGRID que você configurou nesse KMS.

Campo	Descrição
KMS nome	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres. **Nota**: Se você não criou uma chave usando seu produto KMS, será solicitado que o StorageGRID crie a chave.

Campo	Descrição
Gere as chaves para	O site StorageGRID que será associado a este KMS. Se possível, você deve configurar qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplica a todos os sites não gerenciados por outro KMS. • Selecione um site se este KMS gerenciará chaves de criptografia para os nós do dispositivo em um local específico. • Selecione **Sites não gerenciados por outro KMS (KMS padrão)** para configurar um KMS padrão que se aplicará a quaisquer sites que não tenham um KMS dedicado e a quaisquer sites que você adicionar em expansões subsequentes. **Nota:** Um erro de validação ocorrerá quando você salvar a configuração do KMS se você selecionar um site que foi criptografado anteriormente pelo KMS padrão, mas você não forneceu a versão atual da chave de criptografia original para o novo KMS.
Porta	A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP.
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Nota:** o campo Nome alternativo (SAN) do assunto do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **continuar**.

Passo 2: Faça upload do certificado do servidor

Na Etapa 2 (carregar certificado do servidor) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado do servidor (ou pacote de certificados) para o KMS. O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

Passos

1. A partir de **passo 2 (carregar certificado do servidor)**, navegue até a localização do certificado ou pacote de certificados do servidor guardado.
2. Carregue o ficheiro de certificado.

   Os metadados do certificado do servidor são exibidos.

Se você carregou um pacote de certificados, os metadados de cada certificado serão exibidos em sua própria guia.

3. Selecione **continuar**.

passo 3: Carregue certificados de cliente

Na Etapa 3 (carregar certificados de cliente) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado de cliente e a chave privada do certificado de cliente. O certificado de cliente permite que o StorageGRID se autentique no KMS.

Passos

1. A partir de **passo 3 (carregar certificados de cliente)**, navegue até a localização do certificado de cliente.
2. Carregue o ficheiro de certificado do cliente.

   Os metadados do certificado do cliente são exibidos.

3. Navegue até a localização da chave privada para o certificado do cliente.
4. Carregue o ficheiro de chave privada.
5. Selecione **testar e salvar**.

   Se uma chave não existir, você será solicitado a que o StorageGRID crie uma.

   As conexões entre o servidor de gerenciamento de chaves e os nós do dispositivo são testadas. Se todas as conexões forem válidas e a chave correta for encontrada no KMS, o novo servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.

   Imediatamente após adicionar um KMS, o status do certificado na página Key Management Server (servidor de gerenciamento de chaves) aparece como desconhecido. Pode demorar StorageGRID até 30 minutos para obter o status real de cada certificado. Você deve atualizar o navegador da Web para ver o status atual.

6. Se uma mensagem de erro for exibida quando você selecionar **Test and save**, revise os detalhes da mensagem e selecione **OK**.

   Por exemplo, você pode receber um erro de entidade 422: Não processável se um teste de conexão falhar.

7. Se você precisar salvar a configuração atual sem testar a conexão externa, selecione **Force save**.

   Selecionar **Force save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.

   A configuração do KMS é salva, mas a conexão com o KMS não é testada.

O gerenciamento de um servidor de gerenciamento de chaves (KMS) envolve a visualização ou edição de detalhes, o gerenciamento de certificados, a visualização de nós criptografados e a remoção de um KMS quando não for mais necessário.

Antes de começar

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

Ver detalhes do KMS

Você pode exibir informações sobre cada servidor de gerenciamento de chaves (KMS) em seu sistema StorageGRID, incluindo detalhes das chaves e o status atual dos certificados de servidor e cliente.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página servidor de gerenciamento de chaves é exibida e mostra as seguintes informações:

   - A guia Detalhes da configuração lista todos os servidores de gerenciamento de chaves configurados.
   - A guia nós criptografados lista todos os nós que têm criptografia de nó ativada.

2. Para exibir os detalhes de um KMS específico e executar operações nesse KMS, selecione o nome do KMS. A página de detalhes do KMS lista as seguintes informações:

Campo	Descrição
Gere as chaves para	O site StorageGRID associado ao KMS. Este campo exibe o nome de um site StorageGRID específico ou **sites não gerenciados por outro KMS (KMS padrão).**
Nome do anfitrião	O nome de domínio totalmente qualificado ou endereço IP do KMS. Se houver um cluster de dois servidores de gerenciamento de chaves, o nome de domínio totalmente qualificado ou o endereço IP de ambos os servidores serão listados. Se houver mais de dois servidores de gerenciamento de chaves em um cluster, o nome de domínio totalmente qualificado ou o endereço IP do primeiro KMS são listados juntamente com o número de servidores de gerenciamento de chaves adicionais no cluster. Por exemplo: `10.10.10.10 and 10.10.10.11` Ou `10.10.10.10 and 2 others`. Para visualizar todos os nomes de host em um cluster, selecione um KMS e selecione **Editar** ou **ações** > **Editar**.

3. Selecione uma guia na página de detalhes do KMS para exibir as seguintes informações:

Separador	Campo	Descrição
Principais detalhes	Nome da chave	O alias de chave para o cliente StorageGRID no KMS.
UID da chave	O identificador exclusivo da versão mais recente da chave.	Modificado pela última vez
A data e a hora da versão mais recente da chave.	Certificado do servidor	Metadados
Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.	Certificado PEM	O conteúdo do arquivo PEM (Privacy Enhanced mail) para o certificado.
Certificado de cliente	Metadados	Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.

4. sempre que exigido pelas práticas de segurança da sua organização, selecione **Rotate key** ou use o software KMS para criar uma nova versão da chave.

   Quando a rotação da chave é bem-sucedida, os campos UID da chave e Last modified são atualizados.

> Se você girar a chave de criptografia usando o software KMS, gire-a da última versão usada da chave para uma nova versão da mesma chave. Não rode para uma chave totalmente diferente.
>
> Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS. O StorageGRID requer que todas as versões de chave usadas anteriormente (bem como quaisquer versões futuras) sejam acessíveis a partir do KMS com o mesmo alias de chave. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados.

Gerenciar certificados

Resolver imediatamente quaisquer problemas de certificado de servidor ou cliente. Se possível, substitua os certificados antes de expirarem.

> Você deve resolver quaisquer problemas de certificado o mais rápido possível para manter o acesso aos dados.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.
2. Na tabela, observe o valor de expiração do certificado para cada KMS.

3. Se a expiração do certificado para qualquer KMS for desconhecida, aguarde até 30 minutos e, em seguida, atualize seu navegador da Web.
4. Se a coluna expiração do certificado indicar que um certificado expirou ou está prestes a expirar, selecione o KMS para ir para a página de detalhes do KMS.
   a. Selecione **certificado do servidor** e verifique o valor do campo "expira em".
   b. Para substituir o certificado, selecione **Editar certificado** para carregar um novo certificado.
   c. Repita essas subetapas e selecione **certificado do cliente** em vez de certificado do servidor.
5. Quando os alertas **expiração do certificado KMS CA**, **expiração do certificado do cliente KMS** e **expiração do certificado do servidor KMS** forem acionados, anote a descrição de cada alerta e execute as ações recomendadas.

   Pode demorar StorageGRID até 30 minutos para obter atualizações para a expiração do certificado. Atualize seu navegador da Web para ver os valores atuais.

> Se você receber um status de **o status do certificado do servidor é desconhecido**, verifique se o KMS permite obter um certificado do servidor sem exigir um certificado do cliente.

Exibir nós criptografados

Você pode exibir informações sobre os nós do dispositivo no seu sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Na parte superior da página, selecione a guia **nós criptografados**.

   A guia nós criptografados lista os nós do dispositivo no sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

3. Revise as informações na tabela para cada nó de dispositivo.

Coluna	Descrição
Nome do nó	O nome do nó do dispositivo.
Tipo de nó	O tipo de nó: Storage, Admin ou Gateway.
Local	O nome do site do StorageGRID onde o nó está instalado.
KMS nome	O nome descritivo do KMS usado para o nó. Se nenhum KMS estiver listado, selecione a guia Detalhes da configuração para adicionar um KMS. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Coluna	Descrição
UID da chave	O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do dispositivo. Para ver um UID de chave inteiro, selecione o texto. Um traço (--) indica que a chave UID é desconhecida, possivelmente por causa de um problema de conexão entre o nó do aparelho e o KMS.
Estado	O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conetado, o carimbo de data/hora será atualizado a cada 30 minutos. Pode levar vários minutos para que o status da conexão seja atualizado após as alterações de configuração do KMS. **Observação:** Atualize seu navegador para ver os novos valores.

4. Se a coluna Status indicar um problema KMS, solucione o problema imediatamente.

   Durante as operações normais de KMS, o status será **conectado ao KMS**. Se um nó for desconetado da grade, o estado de conexão do nó é mostrado (administrativamente para baixo ou desconhecido).

   Outras mensagens de status correspondem a alertas StorageGRID com os mesmos nomes:

   - Falha ao carregar a configuração DE KMS
   - Erro de conetividade DE KMS
   - Nome da chave de encriptação KMS não encontrado
   - Falha na rotação da chave de CRIPTOGRAFIA KMS
   - A chave KMS falhou ao desencriptar um volume de aparelho
   - KMS não está configurado

   Execute as ações recomendadas para esses alertas.

> Você deve resolver quaisquer problemas imediatamente para garantir que seus dados estejam totalmente protegidos.

Edite um KMS

Talvez seja necessário editar a configuração de um servidor de gerenciamento de chaves, por exemplo, se um certificado estiver prestes a expirar.

Antes de começar

- Se pretende atualizar o site selecionado para um KMS, analisou o "Considerações para alterar o KMS para um site".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

A página servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja editar e selecione **ações** > **Editar**.

   Você também pode editar um KMS selecionando o nome do KMS na tabela e selecionando **Editar** na página de detalhes do KMS.

3. Opcionalmente, atualize os detalhes em **Etapa 1 (detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

Campo	Descrição
KMS nome	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres. Você só precisa editar o nome da chave em casos raros. Por exemplo, você deve editar o nome da chave se o alias for renomeado no KMS ou se todas as versões da chave anterior tiverem sido copiadas para o histórico de versões do novo alias.
Gere as chaves para	Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, opcionalmente selecione **Sites não gerenciados por outro KMS (KMS padrão)**. Esta seleção converte um KMS específico do site para o KMS padrão, que se aplicará a todos os sites que não têm um KMS dedicado e a quaisquer sites adicionados em uma expansão. **Observação:** se você estiver editando um KMS específico do site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não será possível selecionar um site específico.
Porta	A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP.
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Nota:** o campo Nome alternativo (SAN) do assunto do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **continuar**.

   A etapa 2 (carregar certificado do servidor) do assistente Editar um servidor de gerenciamento de chaves é exibida.

6. Se precisar substituir o certificado do servidor, selecione **Procurar** e carregue o novo arquivo.

7. Selecione **continuar**.

   A etapa 3 (carregar certificados de cliente) do assistente Editar um servidor de gerenciamento de chaves é exibida.

8. Se precisar substituir o certificado de cliente e a chave privada do certificado de cliente, selecione **Procurar** e carregue os novos arquivos.
9. Selecione **testar e salvar**.

   As conexões entre o servidor de gerenciamento de chaves e todos os nós de dispositivos criptografados por nós nos locais afetados são testadas. Se todas as conexões de nó forem válidas e a chave correta for encontrada no KMS, o servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.

10. Se for apresentada uma mensagem de erro, reveja os detalhes da mensagem e selecione **OK**.

    Por exemplo, você pode receber um erro de entidade 422: Não processável se o site selecionado para este KMS já for gerenciado por outro KMS, ou se um teste de conexão falhou.

11. Se você precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Force save**.

    > Selecionar **Force save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

    A configuração do KMS é salva.

12. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.

    A configuração do KMS é salva, mas a conexão com o KMS não é testada.

Remover um servidor de gerenciamento de chaves (KMS)

Em alguns casos, você pode querer remover um servidor de gerenciamento de chaves. Por exemplo, você pode querer remover um KMS específico do site se você tiver desativado o site.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Sobre esta tarefa

Você pode remover um KMS nestes casos:

- Você pode remover um KMS específico do site se o site tiver sido desativado ou se o site não incluir nós de dispositivo com criptografia de nó ativada.
- Você pode remover o KMS padrão se um KMS específico do site já existir para cada site que tenha nós de dispositivo com criptografia de nó ativada.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja remover e selecione **ações** > **Remover**.

   Você também pode remover um KMS selecionando o nome do KMS na tabela e selecionando **Remover** na página de detalhes do KMS.

3. Confirme se o seguinte é verdadeiro:
   - Você está removendo um KMS específico do site para um site que não tem nó de dispositivo com criptografia de nó ativada.
   - Você está removendo o KMS padrão, mas um KMS específico do site já existe para cada site com criptografia de nó.
4. Selecione **Sim**.

   A configuração do KMS é removida.

Gerenciar configurações de proxy

Configurar proxy de armazenamento

Se você estiver usando serviços de plataforma ou pools de storage em nuvem, poderá configurar um proxy não transparente entre nós de storage e os pontos de extremidade externos do S3. Por exemplo, você pode precisar de um proxy não transparente para permitir que mensagens de serviços de plataforma sejam enviadas para endpoints externos, como um endpoint na Internet.

> As configurações de proxy de armazenamento configuradas não se aplicam aos endpoints de serviços da plataforma Kafka.

Antes de começar

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

Sobre esta tarefa

Você pode configurar as configurações para um único proxy de armazenamento.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Proxy settings**.
2. Na guia **armazenamento**, marque a caixa de seleção **Ativar proxy de armazenamento**.
3. Selecione o protocolo para o proxy de armazenamento.
4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para se conetar ao servidor proxy.

   Deixe este campo em branco para usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para

SOCKS5.

6. Selecione **Guardar**.

   Depois que o proxy de armazenamento é salvo, novos endpoints para serviços de plataforma ou pools de armazenamento em nuvem podem ser configurados e testados.

   As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

7. Verifique as configurações do servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma do StorageGRID não sejam bloqueadas.
8. Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção e selecione **Salvar**.

Configure as configurações de proxy de administrador

Se você enviar pacotes AutoSupport usando HTTP ou HTTPS, poderá configurar um servidor proxy não transparente entre nós de administração e suporte técnico (AutoSupport).

Para obter mais informações sobre o AutoSupport, "Configurar o AutoSupport"consulte .

Antes de começar

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

Sobre esta tarefa

Você pode configurar as configurações para um único proxy de administrador.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Proxy settings**.

   A página Configurações de proxy é exibida. Por padrão, o armazenamento é selecionado no menu de guias.

2. Selecione a guia **Admin**.
3. Marque a caixa de seleção **Enable Admin Proxy** (Ativar proxy de administrador).
4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Introduza a porta utilizada para ligar ao servidor proxy.
6. Opcionalmente, insira um nome de usuário e senha para o servidor proxy.

   Deixe esses campos em branco se o servidor proxy não exigir um nome de usuário ou uma senha.

7. Selecione uma das seguintes opções:

   - Se você quiser proteger a conexão com o proxy de administrador, selecione **Verify proxy certificate**. Carregue um pacote CA para verificar a autenticidade dos certificados SSL apresentados pelo servidor proxy admin.

O AutoSupport On Demand, o e-Series AutoSupport através do StorageGRID e a determinação do caminho de atualização na página de atualização do StorageGRID não funcionarão se um certificado proxy for verificado.

Depois de carregar o pacote CA, os metadados são exibidos.

- Se você não quiser validar certificados ao se comunicar com o servidor proxy de administrador, selecione **não verificar o certificado de proxy**.

8. Selecione **Guardar**.

   Depois que o proxy de administração é salvo, o servidor proxy entre nós de administração e o suporte técnico é configurado.

   As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

9. Se você precisar desativar o proxy de administrador, desmarque a caixa de seleção **Ativar proxy de administrador** e selecione **Salvar**.

Controle firewalls

Controle o acesso no firewall externo

Você pode abrir ou fechar portas específicas no firewall externo.

Você pode controlar o acesso às interfaces de usuário e APIs nos nós de administração do StorageGRID abrindo ou fechando portas específicas no firewall externo. Por exemplo, você pode evitar que os locatários sejam capazes de se conetar ao Gerenciador de Grade no firewall, além de usar outros métodos para controlar o acesso ao sistema.

Se quiser configurar o firewall interno do StorageGRID, "Configurar firewall interno"consulte .

Porta	Descrição	Se a porta estiver aberta…
443	Porta HTTPS padrão para nós de administração	Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade, a API de gerenciamento de grade, o Gerenciador de locatário e a API de gerenciamento do locatário. **Nota:** a porta 443 também é usada para algum tráfego interno.

Porta	Descrição	Se a porta estiver aberta…
8443	Porta restrita do Gerenciador de Grade em nós de administração	• Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade e a API de Gerenciamento de Grade usando HTTPS. • Os navegadores da Web e os clientes de API de gerenciamento não podem acessar o Gerenciador do locatário ou a API de gerenciamento do locatário. • As solicitações de conteúdo interno serão rejeitadas.
9443	Porta restrita do Gerenciador de inquilinos em nós de administração	• Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador do locatário e a API de gerenciamento do locatário usando HTTPS. • Navegadores da Web e clientes de API de gerenciamento não podem acessar o Gerenciador de Grade ou a API de Gerenciamento de Grade. • As solicitações de conteúdo interno serão rejeitadas.

O logon único (SSO) não está disponível nas portas do Gerenciador de Grade restrito ou do Gerenciador de locatário. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Informações relacionadas

- "Faça login no Gerenciador de Grade"
- "Crie uma conta de locatário"
- "Comunicações externas"

Gerenciar controles internos de firewall

O StorageGRID inclui um firewall interno em cada nó que aumenta a segurança da sua grade, permitindo que você controle o acesso da rede ao nó. Use o firewall para impedir o acesso à rede em todas as portas, exceto as necessárias para a implantação da grade específica. As alterações de configuração feitas na página de controle do Firewall são implantadas em cada nó.

Use as três guias na página de controle do Firewall para personalizar o acesso de que você precisa para sua grade.

- **Lista de endereços privilegiados**: Use esta guia para permitir o acesso selecionado a portas fechadas. Você pode adicionar endereços IP ou sub-redes na notação CIDR que podem acessar portas fechadas usando a guia Gerenciar acesso externo.
- **Gerenciar acesso externo**: Use esta guia para fechar portas abertas por padrão ou reabrir portas

previamente fechadas.

- **Rede cliente não confiável**: Use esta guia para especificar se um nó confia no tráfego de entrada da rede cliente.

  As configurações nesta guia substituem as configurações na guia Gerenciar acesso externo.

  - Um nó com uma rede cliente não confiável aceitará somente conexões em portas de endpoint do balanceador de carga configuradas nesse nó (pontos de extremidade globais, de interface de nó e de tipo de nó).
  - As portas de endpoint do balanceador de carga *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Gerenciar redes externas.
  - Quando confiável, todas as portas abertas na guia Gerenciar acesso externo são acessíveis, bem como quaisquer pontos de extremidade do balanceador de carga abertos na rede do cliente.

> As configurações feitas em uma guia podem afetar as alterações de acesso feitas em outra guia. Certifique-se de verificar as configurações em todas as guias para garantir que sua rede se comporta da maneira que você espera.

Para configurar controles internos de firewall, "Configurar controles de firewall"consulte .

Para obter mais informações sobre firewalls externos e segurança de rede, "Controle o acesso no firewall externo"consulte .

Lista de endereços privilegiados e Gerenciar guias de acesso externo

A guia lista de endereços privilegiados permite que você Registre um ou mais endereços IP que recebem acesso a portas de grade fechadas. A guia Gerenciar acesso externo permite fechar o acesso externo a portas externas selecionadas ou a todas as portas externas abertas (as portas externas são portas que são acessíveis por nós que não são de grade por padrão). Essas duas guias geralmente podem ser usadas em conjunto para personalizar o acesso exato à rede que você precisa para permitir a sua grade.

> Os endereços IP privilegiados não têm acesso interno à porta de grade por padrão.

Exemplo 1: Use um host de salto para tarefas de manutenção

Suponha que você queira usar um host de salto (um host de segurança endurecido) para administração de rede. Você pode usar estas etapas gerais:

1. Use a guia lista de endereços privilegiados para adicionar o endereço IP do host de salto.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.

> Adicione o endereço IP privilegiado antes de bloquear as portas 443 e 8443. Todos os usuários conetados atualmente em uma porta bloqueada, incluindo você, perderão acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Depois de salvar sua configuração, todas as portas externas no Admin Node em sua grade serão bloqueadas para todos os hosts, exceto o host jump. Em seguida, você pode usar o host jump para executar tarefas de manutenção em sua grade de forma mais segura.

Exemplo 2: Bloquear portas sensíveis

Suponha que você queira bloquear portas sensíveis e o serviço nessa porta (por exemplo, SSH na porta 22). Você pode usar as seguintes etapas gerais:

1. Use a guia lista de endereços privilegiados para conceder acesso somente aos hosts que precisam acessar o serviço.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.

> Adicione o endereço IP privilegiado antes de bloquear o acesso a quaisquer portas atribuídas ao Access Grid Manager e ao Gerenciador de inquilinos (as portas predefinidas são 443 e 8443). Todos os usuários conetados atualmente em uma porta bloqueada, incluindo você, perderão acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Depois de salvar sua configuração, a porta 22 e o serviço SSH estarão disponíveis para os hosts na lista de endereços privilegiados. Todos os outros hosts terão acesso negado ao serviço, independentemente da interface da solicitação.

Exemplo 3: Desativar o acesso a serviços não utilizados

Em um nível de rede, você pode desativar alguns serviços que você não pretende usar. Por exemplo, para bloquear o tráfego do cliente HTTP S3, você usaria a opção na guia Gerenciar acesso externo para bloquear a porta 18084.

Separador redes Cliente não fidedignas

Se você estiver usando uma rede cliente, você pode ajudar a proteger o StorageGRID contra ataques hostis aceitando tráfego de clientes de entrada apenas em endpoints configurados explicitamente.

Por padrão, a rede do cliente em cada nó de grade é *confiável*. Ou seja, por padrão, o StorageGRID confia em conexões de entrada para cada nó de grade em todos "portas externas disponíveis".

Você pode reduzir a ameaça de ataques hostis em seu sistema StorageGRID especificando que a rede de clientes em cada nó seja *não confiável*. Se a rede de cliente de um nó não for confiável, o nó só aceita conexões de entrada em portas explicitamente configuradas como pontos de extremidade do balanceador de carga. "Configurar pontos de extremidade do balanceador de carga"Consulte e "Configurar controles de firewall".

Exemplo 1: O Gateway Node aceita apenas solicitações HTTPS S3

Suponha que você queira que um nó de gateway recuse todo o tráfego de entrada na rede do cliente, exceto para solicitações HTTPS S3. Você executaria estes passos gerais:

1. Na "Pontos de extremidade do balanceador de carga" página, configure um ponto de extremidade do balanceador de carga para S3 em HTTPS na porta 443.
2. Na página de controle do Firewall, selecione não confiável para especificar que a rede do cliente no nó de gateway não é confiável.

Depois de salvar sua configuração, todo o tráfego de entrada na rede de clientes do nó de Gateway será descartado, exceto para solicitações HTTPS S3 na porta 443 e ICMP echo (ping).

Exemplo 2: O nó de storage envia S3 solicitações de serviços de plataforma

Suponha que você queira ativar o tráfego de serviços de plataforma S3 de saída de um nó de armazenamento, mas você deseja impedir quaisquer conexões de entrada para esse nó de armazenamento na rede do cliente. Você executaria este passo geral:

- Na guia redes de clientes não confiáveis da página de controle do Firewall, indique que a rede de cliente no nó de armazenamento não é confiável.

Depois de salvar sua configuração, o nó de armazenamento não aceita mais nenhum tráfego de entrada na rede do cliente, mas continua a permitir solicitações de saída para destinos de serviços de plataforma configurados.

Exemplo 3: Limitando o acesso ao Gerenciador de Grade a uma sub-rede

Suponha que você queira permitir o acesso do Gerenciador de Grade somente em uma sub-rede específica. Você executaria os seguintes passos:

1. Anexe a rede cliente dos seus nós de administrador à sub-rede.
2. Use a guia rede de cliente não confiável para configurar a rede de cliente como não confiável.
3. Quando você cria um ponto de extremidade do balanceador de carga da interface de gerenciamento, insira a porta e selecione a interface de gerenciamento que a porta acessará.
4. Selecione **Sim** para rede cliente não confiável.
5. Use a guia Gerenciar acesso externo para bloquear todas as portas externas (com ou sem endereços IP privilegiados definidos para hosts fora dessa sub-rede).

Depois de salvar sua configuração, somente os hosts na sub-rede especificada podem acessar o Gerenciador de Grade. Todos os outros hosts estão bloqueados.

Configurar firewall interno

Você pode configurar o firewall do StorageGRID para controlar o acesso à rede a portas específicas nos nós do StorageGRID.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você revisou as informações em "Gerenciar controles de firewall" e "Diretrizes de rede".
- Se você quiser que um nó de administrador ou nó de gateway aceite o tráfego de entrada somente em endpoints configurados explicitamente, você definiu os endpoints do balanceador de carga.

> Ao alterar a configuração da rede do cliente, as conexões de cliente existentes podem falhar se os endpoints do balanceador de carga não tiverem sido configurados.

Sobre esta tarefa

O StorageGRID inclui um firewall interno em cada nó que permite abrir ou fechar algumas das portas nos nós da grade. Você pode usar as guias de controle do Firewall para abrir ou fechar portas abertas por padrão na rede de Grade, na rede Admin e na rede do Cliente. Você também pode criar uma lista de endereços IP privilegiados que podem acessar portas de grade fechadas. Se você estiver usando uma rede de cliente, poderá especificar se um nó confia no tráfego de entrada da rede de cliente e configurar o acesso de portas

específicas na rede de cliente.

Limitar o número de portas abertas para endereços IP fora da sua grade a apenas aquelas que são absolutamente necessárias aumenta a segurança da sua grade. Você usa as configurações em cada uma das três guias de controle do Firewall para garantir que somente as portas necessárias estejam abertas.

Para obter mais informações sobre como usar controles de firewall, incluindo exemplos, "Gerenciar controles de firewall"consulte .

Para obter mais informações sobre firewalls externos e segurança de rede, "Controle o acesso no firewall externo"consulte .

Aceder aos controlos da firewall

Passos

1. Selecione **CONFIGURATION** > **Security** > **Firewall control**.

   As três guias desta página são descritas em "Gerenciar controles de firewall".

2. Selecione qualquer separador para configurar os controlos da firewall.

   Você pode usar essas guias em qualquer ordem. As configurações definidas em uma guia não limitam o que você pode fazer nas outras guias; no entanto, as alterações de configuração feitas em uma guia podem alterar o comportamento das portas configuradas em outras guias.

Lista de endereços privilegiados

Use a guia lista de endereços privilegiados para conceder aos hosts acesso a portas fechadas por padrão ou fechadas por configurações na guia Gerenciar acesso externo.

Endereços IP privilegiados e sub-redes não têm acesso interno à grade por padrão. Além disso, os pontos de extremidade do balanceador de carga e as portas adicionais abertas na guia Lista de endereços privilegiados são acessíveis mesmo que estejam bloqueados na guia Gerenciar acesso externo.

> As configurações na guia lista de endereços privilegiados não podem substituir as configurações na guia rede cliente não confiável.

Passos

1. Na guia lista de endereços privilegiados, insira o endereço ou a sub-rede IP que deseja conceder acesso a portas fechadas.
2. Opcionalmente, selecione **Adicionar outro endereço IP ou sub-rede na notação CIDR** para adicionar clientes privilegiados adicionais.

   > Adicione o mínimo possível de endereços à lista privilegiada.

3. Opcionalmente, selecione **permitir endereços IP privilegiados para acessar portas internas do StorageGRID**. "Portas internas do StorageGRID"Consulte .

   > Esta opção remove algumas proteções para serviços internos. Deixe-o desativado, se possível.

4. Selecione **Guardar**.

Gerenciar o acesso externo

Quando uma porta é fechada na guia Gerenciar acesso externo, a porta não pode ser acessada por nenhum endereço IP que não seja da grade, a menos que você adicione o endereço IP à lista de endereços privilegiados. Você só pode fechar portas abertas por padrão e só pode abrir portas fechadas.

> As configurações na guia Gerenciar acesso externo não podem substituir as configurações na guia rede cliente não confiável. Por exemplo, se um nó não for confiável, a porta SSH/22 será bloqueada na rede do cliente, mesmo que esteja aberta na guia Gerenciar acesso externo. As configurações na guia rede do cliente não confiável substituem as portas fechadas (como 443, 8443, 9443) na rede do cliente.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós que não são da grade por padrão) para os nós da grade.
2. Configure as portas que deseja abrir e fechar usando as seguintes opções:
   - Utilize a alternância ao lado de cada porta para abrir ou fechar a porta selecionada.
   - Selecione **abrir todas as portas exibidas** para abrir todas as portas listadas na tabela.
   - Selecione **Fechar todas as portas exibidas** para fechar todas as portas listadas na tabela.

   > Se você fechar as portas 443 ou 8443 do Gerenciador de Grade, qualquer usuário conetado atualmente em uma porta bloqueada, incluindo você, perderá o acesso ao Gerenciador de Grade, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

   > Use a barra de rolagem no lado direito da tabela para ter certeza de que visualizou todas as portas disponíveis. Utilize o campo de pesquisa para encontrar as definições de qualquer porta externa introduzindo um número de porta. Pode introduzir um número de porta parcial. Por exemplo, se você inserir um **2**, todas as portas que têm a string "2" como parte de seu nome serão exibidas.

3. Selecione **Guardar**

Rede cliente não confiável

Se a rede do cliente para um nó não for confiável, o nó só aceita o tráfego de entrada em portas configuradas como endpoints do balanceador de carga e, opcionalmente, portas adicionais selecionadas nesta guia. Você também pode usar essa guia para especificar a configuração padrão para novos nós adicionados em uma expansão.

> As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

As alterações de configuração feitas na guia **rede cliente não confiável** substituem as configurações na guia **Gerenciar acesso externo**.

Passos

1. Selecione **rede Cliente não fidedigna**.
2. Na seção Definir novo nó padrão, especifique qual deve ser a configuração padrão quando novos nós são

adicionados à grade em um procedimento de expansão.

- **Trusted** (padrão): Quando um nó é adicionado em uma expansão, sua rede de clientes é confiável.
- **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede cliente não é confiável.

  Conforme necessário, você pode retornar a essa guia para alterar a configuração de um novo nó específico.

  Esta configuração não afeta os nós existentes no seu sistema StorageGRID.

3. Use as opções a seguir para selecionar os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga configurados explicitamente ou em portas selecionadas adicionais:

   - Selecione **não confiar nos nós exibidos** para adicionar todos os nós exibidos na tabela à lista rede cliente não confiável.
   - Selecione **confiar em nós exibidos** para remover todos os nós exibidos na tabela da lista rede de clientes não confiável.
   - Use a alternância ao lado de cada nó para definir a rede do cliente como confiável ou não confiável para o nó selecionado.

     Por exemplo, você pode selecionar **não confiar nos nós exibidos** para adicionar todos os nós à lista rede de clientes não confiável e, em seguida, usar a alternância além de um nó individual para adicionar esse nó único à lista rede de clientes confiáveis.

     Use a barra de rolagem no lado direito da tabela para ter certeza de que você visualizou todos os nós disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer nó inserindo o nome do nó. Pode introduzir um nome parcial. Por exemplo, se você inserir um **GW**, todos os nós que têm a string "GW" como parte de seu nome serão exibidos.

4. Selecione **Guardar**.

   As novas configurações de firewall são imediatamente aplicadas e aplicadas. As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Gerenciar locatários

O que são contas de inquilino?

Uma conta de locatário permite que você use a API REST do Simple Storage Service (S3) para armazenar e recuperar objetos em um sistema StorageGRID.

Os detalhes do Swift foram removidos desta versão do site do doc. "StorageGRID 11,8: Gerenciar locatários"Consulte .

Como administrador de grade, você cria e gerencia as contas de locatário que os clientes S3 usam para armazenar e recuperar objetos.

Cada conta de locatário tem grupos federados ou locais, usuários, buckets do S3 e objetos.

As contas de inquilino podem ser usadas para segregar objetos armazenados por diferentes entidades. Por exemplo, várias contas de inquilino podem ser usadas para qualquer um desses casos de uso:

- * Caso de uso corporativo:* se você estiver administrando um sistema StorageGRID em um aplicativo corporativo, talvez queira separar o armazenamento de objetos da grade pelos diferentes departamentos da sua organização. Nesse caso, você pode criar contas de inquilino para o departamento de marketing, o departamento de suporte ao cliente, o departamento de recursos humanos e assim por diante.

> Se você usar o protocolo cliente S3, poderá usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa usar contas de locatário. Consulte as instruções de implementação "Buckets e políticas de buckets do S3" para obter mais informações.

- * Caso de uso do provedor de serviços:* se você estiver administrando um sistema StorageGRID como provedor de serviços, você pode segregar o armazenamento de objetos da grade pelas diferentes entidades que alugarão o armazenamento em sua grade. Neste caso, você criaria contas de inquilino para a empresa A, empresa B, empresa C e assim por diante.

Para obter mais informações, "Use uma conta de locatário"consulte .

Como faço para criar uma conta de locatário?

Use o Gerenciador de Grade para criar uma conta de locatário. Ao criar uma conta de locatário, você especifica as seguintes informações:

- Informações básicas, incluindo o nome do locatário, o tipo de cliente (S3) e a cota de armazenamento opcional.
- Permissões para a conta de locatário, como se a conta de locatário pode usar os serviços da plataforma S3, configurar sua própria origem de identidade, usar S3 Select ou usar uma conexão de federação de grade.
- O acesso raiz inicial para o locatário, com base se o sistema StorageGRID usa grupos e usuários locais, federação de identidade ou logon único (SSO).

Além disso, você pode ativar a configuração bloqueio de objeto S3 para o sistema StorageGRID se as contas de locatário do S3 precisarem cumprir os requisitos regulamentares. Quando o bloqueio de objeto S3 está ativado, todas as contas de locatário do S3 podem criar e gerenciar buckets compatíveis.

Para que é utilizado o Tenant Manager?

Depois de criar a conta de locatário, os usuários do locatário podem entrar no Gerenciador do locatário para executar tarefas como as seguintes:

- Configurar federação de identidade (a menos que a origem de identidade seja compartilhada com a grade)
- Gerenciar grupos e usuários
- Use a federação de grade para clone de conta e replicação entre grade
- Gerenciar S3 chaves de acesso
- Crie e gerencie buckets do S3
- Use os serviços da plataforma S3
- Utilize S3 Select (Selecionar)
- Monitorar o uso do storage

Embora os usuários de locatários do S3 possam criar e gerenciar chaves de acesso do S3 e buckets com o Gerenciador de locatários, eles precisam usar um aplicativo cliente do S3 para obter e gerenciar objetos. "USE A API REST DO S3"Consulte para obter detalhes.

Crie uma conta de locatário

Você deve criar pelo menos uma conta de locatário para controlar o acesso ao storage no sistema StorageGRID.

As etapas para criar uma conta de locatário variam de acordo com "federação de identidade"a configuração e "logon único"se a conta do Gerenciador de Grade que você usa para criar a conta de locatário pertence a um grupo de administração com a permissão de acesso root.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Acesso root ou permissão de contas do locatário".
- Se a conta de locatário usar a origem de identidade configurada para o Gerenciador de Grade e você quiser conceder permissão de acesso raiz para a conta de locatário a um grupo federado, você importou esse grupo federado para o Gerenciador de Grade. Você não precisa atribuir nenhuma permissão do Gerenciador de Grade a esse grupo de administradores. "Gerenciar grupos de administradores"Consulte .
- Se você quiser permitir que um locatário do S3 clone dados de conta e replique objetos de bucket para outra grade usando uma conexão de federação de grade:
  - Você "configurada a conexão de federação de grade"tem .
  - O estado da ligação é **ligado**.
  - Você tem permissão de acesso root.
  - Você revisou as considerações para "gerenciamento dos locatários permitidos para a federação da grade".
  - Se a conta de locatário usar a origem de identidade configurada para o Gerenciador de Grade, você importou o mesmo grupo federado para o Gerenciador de Grade em ambas as grades.

    Ao criar o locatário, você selecionará esse grupo para ter a permissão de acesso raiz inicial para as contas de locatário de origem e destino.

  Se esse grupo de administração não existir em ambas as grades antes de criar o locatário, o locatário não será replicado para o destino.

Acesse o assistente

Passos

1. Selecione **TENANTS**.
2. Selecione **criar**.

Introduza os detalhes

Passos

1. Insira os detalhes para o locatário.

Campo	Descrição
Nome	Um nome para a conta de locatário. Os nomes de inquilinos não precisam ser únicos. Quando a conta de locatário é criada, ela recebe um ID de conta exclusivo de 20 dígitos.
Descrição (opcional)	Uma descrição para ajudar a identificar o inquilino. Se você estiver criando um locatário que usará uma conexão de federação de grade, opcionalmente, use este campo para ajudar a identificar qual é o locatário de origem e qual é o locatário de destino. Por exemplo, essa descrição para um locatário criado na Grade 1 também aparecerá para o locatário replicado para a Grade 2: "Este locatário foi criado na Grade 1."
Tipo de cliente	O tipo de protocolo de cliente que este locatário usará, seja **S3** ou **Swift**. **Nota**: O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.
Cota de armazenamento (opcional)	Se você quiser que esse locatário tenha uma cota de armazenamento, um valor numérico para a cota e as unidades.

2. Selecione **continuar**.

Selecione permissões

Passos

1. Opcionalmente, selecione as permissões básicas que você deseja que esse locatário tenha.

> Algumas dessas permissões têm requisitos adicionais. Para obter detalhes, selecione o ícone de ajuda para cada permissão.

Permissão	Se selecionado…
Permitir serviços de plataforma	O locatário pode usar serviços de plataforma S3, como o CloudMirror. "Gerencie os serviços de plataforma para contas de inquilino S3"Consulte .
Use a própria fonte de identidade	O locatário pode configurar e gerenciar sua própria fonte de identidade para grupos federados e usuários. Esta opção é desativada se tiver "SSO configurado" para o seu sistema StorageGRID.
Permitir S3 Selecione	O locatário pode emitir S3 solicitações de API SelectObjectContent para filtrar e recuperar dados de objeto. "Gerenciar S3 Selecione para contas de inquilino"Consulte . **Importante**: As solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Ative esse recurso somente quando necessário e somente para locatários confiáveis.

2. Opcionalmente, selecione as permissões avançadas que você deseja que esse locatário tenha.

Permissão	Se selecionado…
Conexão de federação de grade	O locatário pode usar uma conexão de federação de grade, que: • Faz com que esse locatário e todos os grupos de locatários e usuários adicionados à conta sejam clonados dessa grade (a *grade de origem*) para a outra grade na conexão selecionada (a *grade de destino*). • Permite que esse locatário configure a replicação entre grade entre intervalos correspondentes em cada grade. "Gerenciar os locatários permitidos para a federação de grade"Consulte .
S3 bloqueio de objetos	Permita que o locatário use recursos específicos do bloqueio de objetos S3: • **Definir período máximo de retenção** define quanto tempo novos objetos adicionados a este balde devem ser retidos, a partir do momento em que são ingeridos. • **Permitir o modo de conformidade** impede que os usuários substituam ou excluam versões de objetos protegidos durante o período de retenção.

3. Selecione **continuar**.

Defina o acesso root e crie o locatário

Passos

1. Defina o acesso root para a conta de locatário, com base se o seu sistema StorageGRID usa federação de identidade, logon único (SSO) ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver ativada	Especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade estiver ativada	a. Selecione um grupo federado existente para ter permissão de acesso root para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso root para o locatário. Nenhum usuário local pode entrar.

2. Selecione **criar inquilino**.

   Uma mensagem de sucesso é exibida e o novo locatário é listado na página de locatários. Para saber como exibir detalhes do locatário e monitorar a atividade do locatário, "Monitorar a atividade do locatário"consulte .

A aplicação de configurações de locatário na grade pode levar 15 minutos ou mais com base na conetividade de rede, no status do nó e nas operações do Cassandra.

3. Se você selecionou a permissão **usar conexão de federação de grade** para o locatário:
   a. Confirme se um locatário idêntico foi replicado para a outra grade na conexão. Os locatários em ambas as grades terão o mesmo ID de conta, nome, descrição, cota e permissões de 20 dígitos.

      Se você vir a mensagem de erro "Tenant created without a clone", consulte as instruções em "Solucionar erros de federação de grade".

   b. Se você forneceu uma senha de usuário raiz local ao definir o acesso root, "altere a senha do usuário raiz local" para o locatário replicado.

      Um usuário raiz local não pode entrar no Gerenciador do locatário na grade de destino até que a senha seja alterada.

Iniciar sessão no locatário (opcional)

Conforme necessário, você pode fazer login no novo locatário agora para concluir a configuração ou entrar no locatário mais tarde. As etapas de login dependem se você está conetado ao Gerenciador de Grade usando a porta padrão (443) ou uma porta restrita. "Controle o acesso no firewall externo"Consulte .

Inicie sessão agora

Se você estiver usando…	Faça isso…
Porta 443 e você define uma senha para o usuário raiz local	1. Selecione **entrar como root**. Quando você faz login, os links são exibidos para configurar buckets, federação de identidade, grupos e usuários. 2. Selecione os links para configurar a conta de locatário. Cada link abre a página correspondente no Gerenciador do Locatário. Para concluir a página, consulte "instruções para o uso de contas de inquilino".
Porta 443 e você não definiu uma senha para o usuário raiz local	Selecione **entrar** e insira as credenciais de um usuário no grupo federado de acesso raiz.

Se você estiver usando…	Faça isso…
Uma porta restrita	1. Selecione **Finish** 2. Selecione **Restricted** na tabela Tenant para saber mais sobre como acessar essa conta de locatário. O URL do Gerenciador do Locatário tem este formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador ◦ *port* é a porta somente locatário ◦ *20-digit-account-id* É o ID exclusivo da conta do locatário

Inicie sessão mais tarde

Se você estiver usando…	Faça um destes…
Porta 443	• No Gerenciador de Grade, selecione **TENANTS** e **Sign in** à direita do nome do locatário. • Insira o URL do locatário em um navegador da Web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador ◦ *20-digit-account-id* É o ID exclusivo da conta do locatário
Uma porta restrita	• No Gerenciador de Grade, selecione **TENANTS** e **restricted**. • Insira o URL do locatário em um navegador da Web: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador ◦ *port* é a porta restrita somente para locatário ◦ *20-digit-account-id* É o ID exclusivo da conta do locatário

Configure o locatário

Siga as instruções em "Use uma conta de locatário" para gerenciar grupos de locatários e usuários, chaves de

acesso do S3, buckets, serviços de plataforma e replicação entre grades e clone de contas.

Editar conta de locatário

Você pode editar uma conta de locatário para alterar o nome de exibição, a cota de armazenamento ou as permissões de locatário.

Se um locatário tiver a permissão **usar conexão de federação de grade**, você poderá editar os detalhes do locatário de qualquer grade na conexão. No entanto, quaisquer alterações feitas em uma grade na conexão não serão copiadas para a outra grade. Se você quiser manter os detalhes do locatário exatamente em sincronia entre grades, faça as mesmas edições em ambas as grades. "Gerenciar os locatários permitidos para conexão de federação de grade"Consulte .

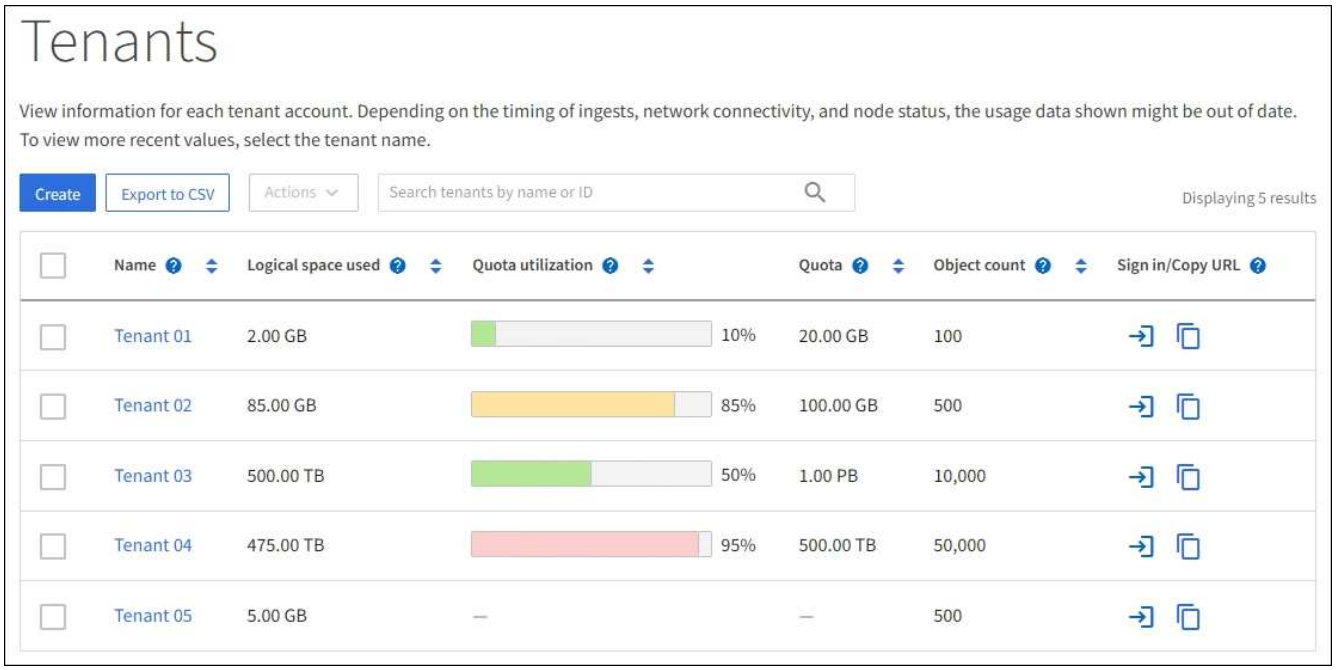
Antes de começar

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

A aplicação de configurações de locatário na grade pode levar 15 minutos ou mais com base na conetividade de rede, no status do nó e nas operações do Cassandra.

Passos

1. Selecione **TENANTS**.



2. Localize a conta de locatário que você deseja editar.

   Use a caixa de pesquisa para procurar um locatário por nome ou ID de locatário.

3. Selecione o locatário. Você pode fazer um dos seguintes procedimentos:
   - Marque a caixa de seleção para o locatário e selecione **ações** > **Editar**.
   - Selecione o nome do locatário para exibir a página de detalhes e selecione **Editar**.

4. Opcionalmente, altere os valores para estes campos:
   - **Nome**
   - **Descrição**
   - **Cota de armazenamento**
5. Selecione **continuar**.
6. Selecione ou desmarque as permissões para a conta de locatário.
   - Se você desabilitar **Serviços de plataforma** para um locatário que já os esteja usando, os serviços que eles configuraram para seus buckets do S3 deixarão de funcionar. Nenhuma mensagem de erro é enviada ao locatário. Por exemplo, se o locatário tiver configurado a replicação do CloudMirror para um bucket do S3, ele ainda poderá armazenar objetos no bucket, mas as cópias desses objetos não serão mais feitas no bucket externo do S3 configurado como um endpoint. "Gerencie os serviços de plataforma para contas de inquilino S3"Consulte .
   - Altere a configuração de **Use own Identity source** para determinar se a conta do locatário usará sua própria origem de identidade ou a fonte de identidade que foi configurada para o Grid Manager.

     Se **usar a própria fonte de identidade** for:

     - Desativado e selecionado, o locatário já habilitou sua própria fonte de identidade. Um locatário deve desativar sua origem de identidade antes de poder usar a fonte de identidade que foi configurada para o Gerenciador de Grade.
     - Desativado e não selecionado, SSO está ativado para o sistema StorageGRID. O locatário deve usar a fonte de identidade que foi configurada para o Gerenciador de Grade.
   - Selecione ou desmarque a permissão **Allow S3 Select** conforme necessário. "Gerenciar S3 Selecione para contas de inquilino"Consulte .
   - Para remover a permissão **Use Grid Federation Connection**:
     i. Selecione a guia **Grid Federation**.
     ii. Selecione **Remover permissão**.
   - Para adicionar a permissão **Use Grid Federation Connection**:
     i. Selecione a guia **Grid Federation**.
     ii. Marque a caixa de seleção **usar conexão de federação de grade**.
     iii. Opcionalmente, selecione **Clonar usuários locais existentes e grupos** para cloná-los para a grade remota. Se desejar, você pode parar a clonagem em andamento ou tentar novamente a clonagem se alguns usuários ou grupos locais não tiverem sido clonados após a última operação de clone ter sido concluída.
   - Para definir um período de retenção máximo ou permitir o modo de conformidade:

     > S3 o bloqueio de objetos tem de estar ativado na grelha antes de poder utilizar estas definições.

     i. Selecione a guia **S3 Object Lock**.
     ii. Para **Definir período de retenção máximo**, insira um valor e selecione o período de tempo na lista suspensa.
     iii. Para **permitir o modo de conformidade**, selecione a caixa de verificação.

Altere a senha para o usuário raiz local do locatário

Talvez seja necessário alterar a senha do usuário raiz local de um locatário se o usuário raiz estiver bloqueado para fora da conta.

Antes de começar

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

Sobre esta tarefa

Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, o usuário raiz local não poderá entrar na conta de locatário. Para executar tarefas de usuário raiz, os usuários devem pertencer a um grupo federado que tenha a permissão de acesso raiz para o locatário.

Passos

1. Selecione **TENANTS**.

2. Selecione a conta de locatário. Você pode fazer um dos seguintes procedimentos:
   - Marque a caixa de seleção para o locatário e selecione **ações** > **alterar senha de root**.
   - Selecione o nome do locatário para exibir a página de detalhes e selecione **ações** > **alterar senha de root**.
3. Introduza a nova palavra-passe para a conta de locatário.
4. Selecione **Guardar**.

Eliminar conta de inquilino

Você pode excluir uma conta de locatário se quiser remover permanentemente o acesso do locatário ao sistema.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você removeu todos os buckets e objetos do S3 associados à conta de locatário.
- Se o locatário tiver permissão para usar uma conexão de federação de grade, você revisou as considerações para "Excluindo um locatário com a permissão usar conexão de federação de grade".

Passos

1. Selecione **TENANTS**.
2. Localize a conta de locatário ou contas que você deseja excluir.

   Use a caixa de pesquisa para procurar um locatário por nome ou ID de locatário.

3. Para excluir vários locatários, marque as caixas de seleção e selecione **ações** > **Excluir**.
4. Para excluir um único locatário, faça um dos seguintes procedimentos:
   - Marque a caixa de seleção e selecione **ações** > **Excluir**.
   - Selecione o nome do locatário para exibir a página de detalhes e selecione **ações** > **Excluir**.
5. Selecione **Sim**.

Gerenciar serviços de plataforma

O que são serviços de plataforma?

Os serviços de plataforma incluem replicação do CloudMirror, notificações de eventos e o serviço de integração de pesquisa.

Se você ativar os serviços de plataforma para contas de locatário do S3, configure sua grade para que os locatários possam acessar os recursos externos necessários para usar esses serviços.

Replicação do CloudMirror

O serviço de replicação do StorageGRID CloudMirror é usado para espelhar objetos específicos de um bucket do StorageGRID para um destino externo especificado.

Por exemplo, você pode usar a replicação do CloudMirror para espelhar Registros específicos de clientes no Amazon S3 e aproveitar os serviços da AWS para realizar análises nos seus dados.

> A replicação do CloudMirror tem algumas semelhanças e diferenças importantes com o recurso de replicação entre grades. Para saber mais, "Compare a replicação entre redes e a replicação do CloudMirror"consulte .

> A replicação do CloudMirror não é suportada se o bucket de origem tiver o S3 Object Lock ativado.

Notificações

As notificações de eventos por bucket são usadas para enviar notificações sobre ações específicas executadas em objetos para um cluster Kafka externo especificado ou Amazon Simple Notification Service.

Por exemplo, você pode configurar alertas para serem enviados aos administradores sobre cada objeto

adicionado a um bucket, onde os objetos representam arquivos de log associados a um evento crítico do sistema.

> Embora a notificação de evento possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

Serviço de integração de pesquisa

O serviço de integração de pesquisa é usado para enviar metadados de objeto S3 para um índice Elasticsearch especificado, onde os metadados podem ser pesquisados ou analisados usando o serviço externo.

Por exemplo, você pode configurar seus buckets para enviar metadados de objeto S3 para um serviço Elasticsearch remoto. Você pode usar o Elasticsearch para realizar pesquisas entre buckets e realizar análises sofisticadas de padrões presentes nos metadados do objeto.

> Embora a integração do Elasticsearch possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

Com os serviços de plataforma, os locatários têm a capacidade de usar recursos de storage externos, serviços de notificação e serviços de pesquisa ou análise com seus dados. Como o local de destino para serviços de plataforma geralmente é externo à implantação do StorageGRID, você deve decidir se deseja permitir que os locatários usem esses serviços. Se o fizer, você deverá habilitar o uso de serviços de plataforma quando criar ou editar contas de locatário. Você também deve configurar sua rede de modo que as mensagens de serviços de plataforma que os locatários geram possam chegar aos destinos deles.

Recomendações para o uso de serviços de plataforma

Antes de usar os serviços da plataforma, esteja ciente das seguintes recomendações:

- Se um bucket do S3 no sistema StorageGRID tiver o controle de versão e a replicação do CloudMirror habilitado, você também deverá habilitar o controle de versão do bucket do S3 para o endpoint de destino. Isso permite que a replicação do CloudMirror gere versões de objetos semelhantes no endpoint.
- Você não deve usar mais de 100 locatários ativos com solicitações do S3 que exigem replicação, notificações e integração de pesquisa do CloudMirror. Ter mais de 100 inquilinos ativos ativos pode resultar em desempenho mais lento do cliente S3.
- As solicitações para um endpoint que não pode ser concluído serão enfileiradas para um máximo de 500.000 solicitações. Esse limite é compartilhado igualmente entre locatários ativos. Novos inquilinos podem exceder temporariamente este limite de 500.000 para que os inquilinos recém-criados não sejam injustamente penalizados.

Informações relacionadas

- "Gerenciar serviços de plataforma"
- "Configure as configurações de proxy de armazenamento"
- "Monitore o StorageGRID"

Rede e portas para serviços de plataforma

Se você permitir que um locatário do S3 use serviços de plataforma, você deve

configurar a rede para a grade para garantir que as mensagens de serviços de plataforma possam ser entregues aos seus destinos.

Você pode ativar os serviços de plataforma para uma conta de locatário do S3 ao criar ou atualizar a conta de locatário. Se os serviços de plataforma estiverem ativados, o locatário poderá criar endpoints que servem como destino para replicação do CloudMirror, notificações de eventos ou mensagens de integração de pesquisa a partir de seus buckets do S3. Essas mensagens de serviços de plataforma são enviadas de nós de storage que executam o serviço ADC para os endpoints de destino.

Por exemplo, os locatários podem configurar os seguintes tipos de endpoints de destino:

- Um cluster Elasticsearch hospedado localmente
- Um aplicativo local compatível com o recebimento de mensagens do Amazon Simple Notification Service
- Um cluster Kafka hospedado localmente
- Um bucket do S3 hospedado localmente na mesma ou em outra instância do StorageGRID
- Um endpoint externo, como um endpoint no Amazon Web Services.

Para garantir que as mensagens dos serviços da plataforma possam ser entregues, você deve configurar a rede ou as redes que contêm os nós de armazenamento ADC. Você deve garantir que as portas a seguir possam ser usadas para enviar mensagens de serviços de plataforma para os endpoints de destino.

Por padrão, as mensagens dos serviços da plataforma são enviadas nas seguintes portas:

- **80**: Para URIs de endpoint que começam com http (a maioria dos endpoints)
- **443**: Para URIs de endpoint que começam com https (a maioria dos endpoints)
- **9092**: Para URIs de endpoint que começam com http ou https (somente endpoints Kafka)

Os locatários podem especificar uma porta diferente quando criam ou editam um endpoint.

> Se uma implantação do StorageGRID for usada como destino para a replicação do CloudMirror, as mensagens de replicação podem ser recebidas em uma porta diferente de 80 ou 443. Verifique se a porta que está sendo usada para S3 pela implantação do StorageGRID de destino está especificada no endpoint.

Se você usar um servidor proxy não transparente, também deverá "configure as configurações de proxy de armazenamento"permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet.

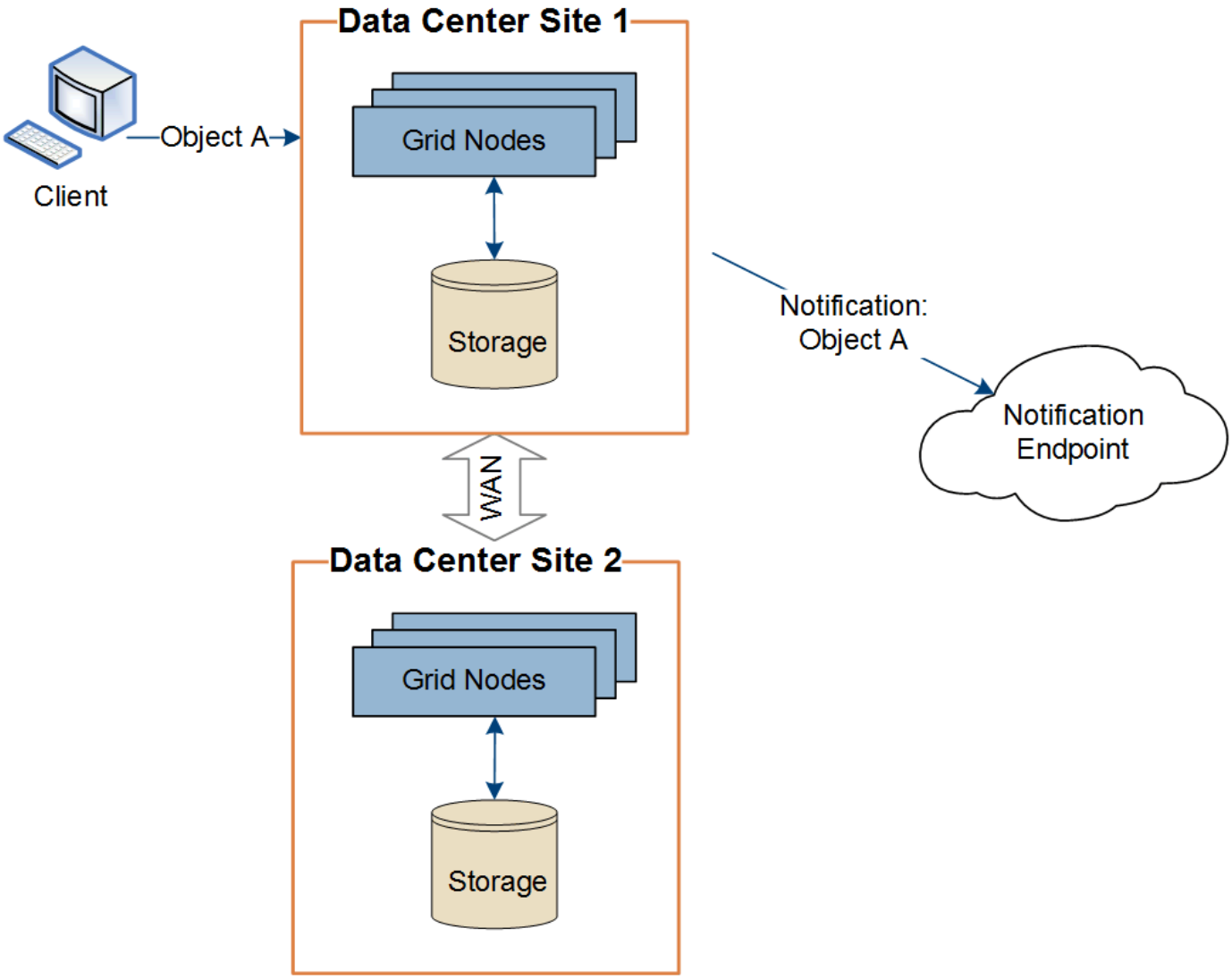
Informações relacionadas

"Use uma conta de locatário"

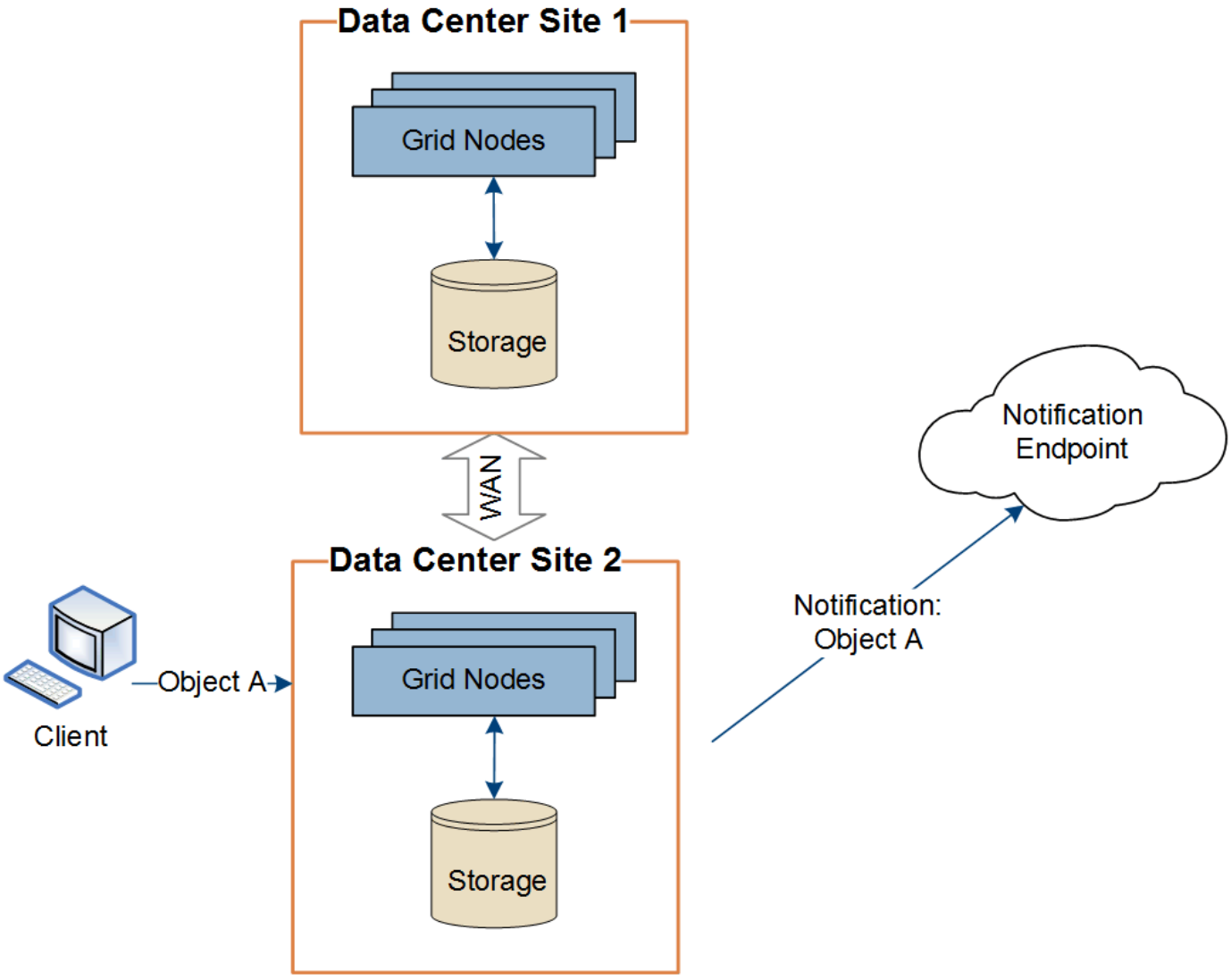
Entrega por local de mensagens de serviços de plataforma

Todas as operações de serviços de plataforma são realizadas por local.

Ou seja, se um locatário usar um cliente para executar uma operação de criação de API S3 em um objeto conetando-se a um nó de gateway no Data Center Site 1, a notificação sobre essa ação será acionada e enviada a partir do Data Center Site 1.



Se o cliente executar posteriormente uma operação de exclusão de API S3 nesse mesmo objeto do Data Center Site 2, a notificação sobre a ação de exclusão será acionada e enviada do Data Center Site 2.



Certifique-se de que a rede em cada local está configurada de forma a que as mensagens dos serviços da plataforma possam ser entregues aos seus destinos.

Solucionar problemas de serviços de plataforma

Os endpoints usados nos serviços de plataforma são criados e mantidos por usuários de inquilinos no Gerenciador de inquilinos; no entanto, se um locatário tiver problemas para configurar ou usar serviços de plataforma, talvez você possa usar o Gerenciador de Grade para ajudar a resolver o problema.

Problemas com novos endpoints

Antes que um locatário possa usar os serviços da plataforma, ele deve criar um ou mais pontos de extremidade usando o Gerenciador do locatário. Cada endpoint representa um destino externo para um serviço de plataforma, como um bucket do StorageGRID S3, um bucket do Amazon Web Services, um tópico do Amazon Simple Notification Service, um tópico do Kafka ou um cluster do Elasticsearch hospedado localmente ou na AWS. Cada endpoint inclui a localização do recurso externo e as credenciais necessárias para acessar esse recurso.

Quando um locatário cria um endpoint, o sistema StorageGRID valida que o endpoint existe e que ele pode ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó

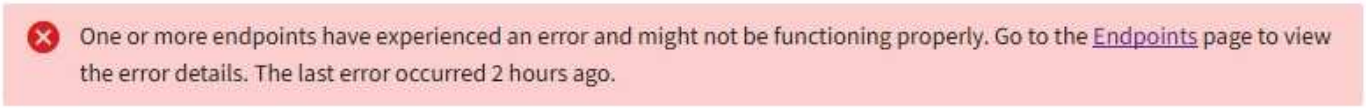
em cada local.

Se a validação do endpoint falhar, uma mensagem de erro explica por que a validação do endpoint falhou. O usuário do locatário deve resolver o problema e tentar criar o endpoint novamente.

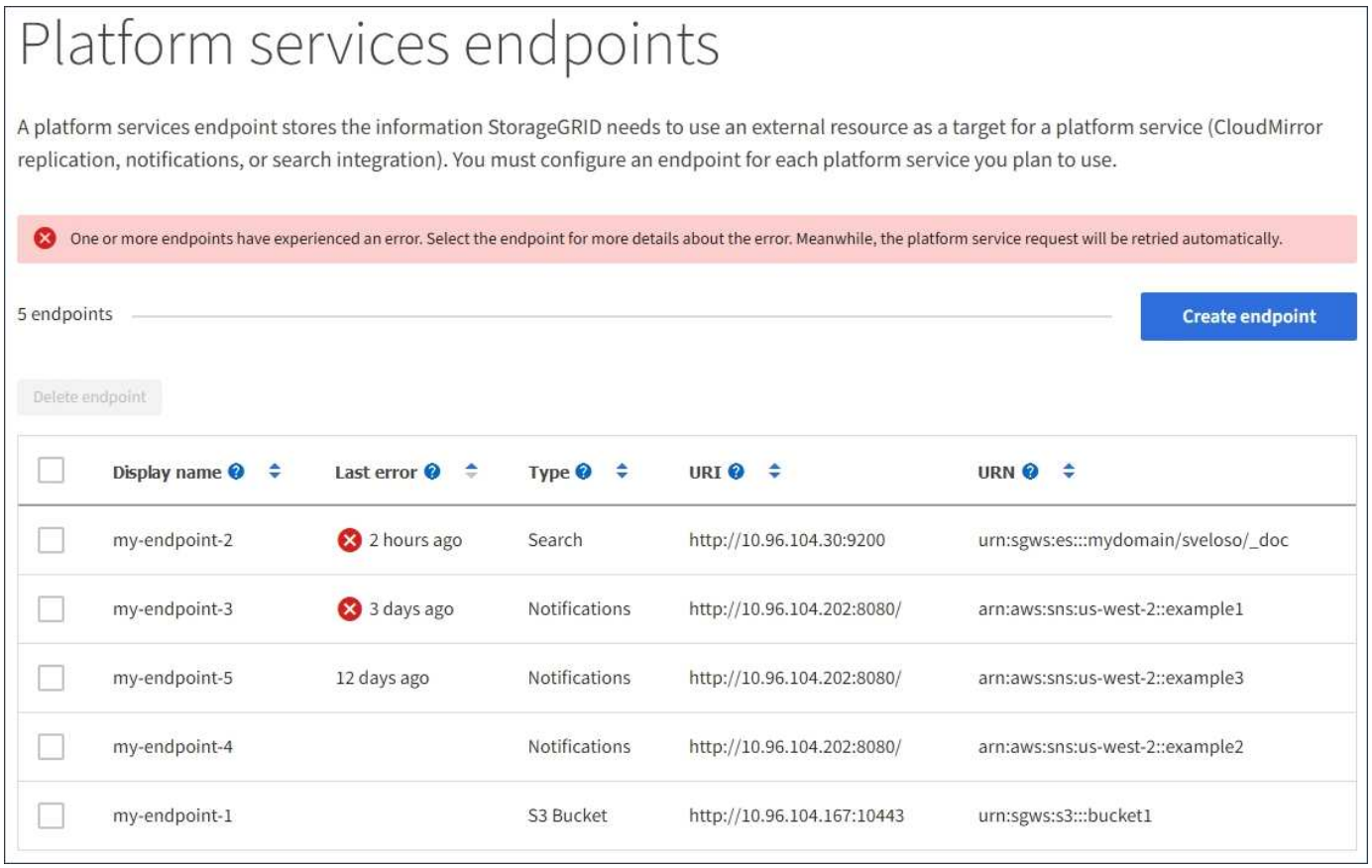
A criação do endpoint falhará se os serviços da plataforma não estiverem habilitados para a conta do locatário.

Problemas com endpoints existentes

Se ocorrer um erro quando o StorageGRID tenta alcançar um endpoint existente, uma mensagem é exibida no painel no Gerenciador de inquilinos.



Os usuários do locatário podem ir para a página Endpoints para revisar a mensagem de erro mais recente para cada endpoint e determinar quanto tempo atrás o erro ocorreu. A coluna **último erro** exibe a mensagem de erro mais recente para cada endpoint e indica quanto tempo atrás o erro ocorreu. Erros que incluem o ícone ocorreram nos últimos 7 dias.



Algumas mensagens de erro na coluna **último erro** podem incluir um LOGID entre parênteses. Um administrador de grade ou suporte técnico pode usar esse ID para localizar informações mais detalhadas sobre o erro no bycast.log.

Problemas relacionados aos servidores proxy

Se você tiver configurado um "proxy de storage" entre nós de storage e endpoints de serviço da plataforma, poderão ocorrer erros se o serviço proxy não permitir mensagens do StorageGRID. Para resolver esses problemas, verifique as configurações do servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma não sejam bloqueadas.

Determine se ocorreu um erro

Se algum erro de endpoint tiver ocorrido nos últimos 7 dias, o painel no Gerenciador de inquilinos exibirá uma mensagem de alerta. Pode aceder à página Endpoints para ver mais detalhes sobre o erro.

Falha nas operações do cliente

Alguns problemas de serviços de plataforma podem causar falha nas operações do cliente no bucket do S3. Por exemplo, as operações do cliente S3 falharão se o serviço interno da Máquina de Estado replicado (RSM) parar ou se houver muitas mensagens de serviços de plataforma enfileiradas para entrega.

Para verificar o status dos serviços:

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***site*** > ***Storage Node*** > **SSM** > **Serviços**.

Erros de endpoint recuperáveis e irrecuperáveis

Após a criação de endpoints, os erros de solicitação de serviço da plataforma podem ocorrer por vários motivos. Alguns erros são recuperáveis com a intervenção do usuário. Por exemplo, erros recuperáveis podem ocorrer pelos seguintes motivos:

- As credenciais do usuário foram excluídas ou expiraram.
- O intervalo de destino não existe.
- A notificação não pode ser entregue.

Se o StorageGRID encontrar um erro recuperável, a solicitação de serviço da plataforma será tentada novamente até que seja bem-sucedida.

Outros erros são irrecuperáveis. Por exemplo, um erro irrecuperável ocorre se o endpoint for excluído.

Se o StorageGRID encontrar um erro de endpoint irrecuperável:

- No Gerenciador de Grade, vá para **suporte** > **Ferramentas** > **métricas** > **Grafana** > **Visão geral dos Serviços de Plataforma** para ver os detalhes do erro.
- No Gerenciador do Locatário, vá para **STORAGE (S3)** > **Platform Services Endpoints** para ver os detalhes do erro.
- Verifique se existem erros relacionados no `/var/local/log/bycast-err.log`. Os nós de storage que têm o serviço ADC contêm esse arquivo de log.

As mensagens dos serviços da plataforma não podem ser entregues

Se o destino encontrar um problema que o impeça de aceitar mensagens de serviços da plataforma, a operação do cliente no bucket será bem-sucedida, mas a mensagem de serviços da plataforma não será entregue. Por exemplo, esse erro pode acontecer se as credenciais forem atualizadas no destino, de modo que o StorageGRID não possa mais se autenticar no serviço de destino.

Verifique se existem alertas relacionados.

Desempenho mais lento para solicitações de serviço de plataforma

O software StorageGRID pode controlar as solicitações recebidas do S3 para um bucket se a taxa na qual as solicitações estão sendo enviadas exceder a taxa na qual o endpoint de destino pode receber as solicitações. O estrangulamento só ocorre quando há um backlog de solicitações aguardando para serem enviadas para o endpoint de destino.

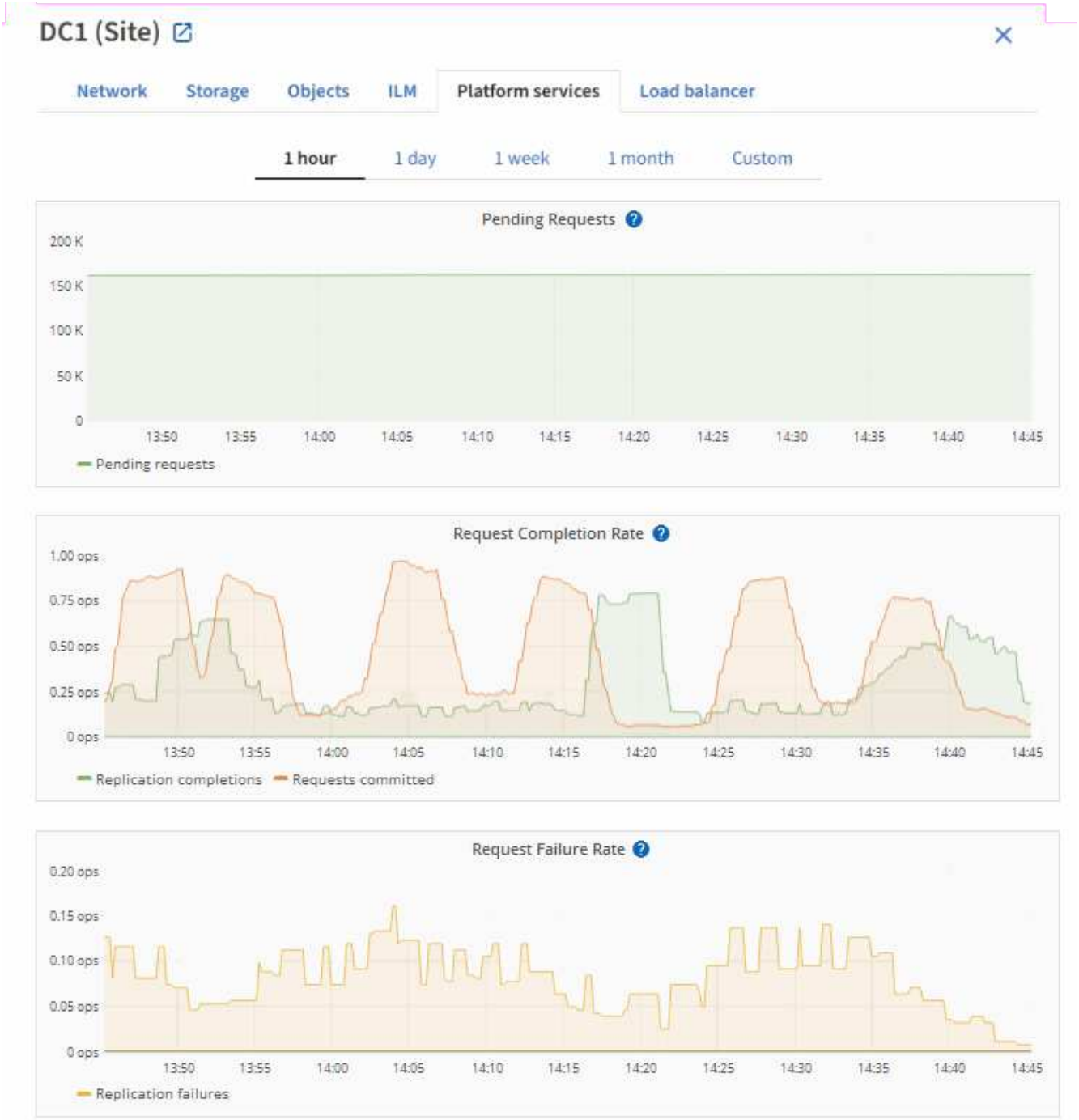
O único efeito visível é que as solicitações S3 recebidas demorarão mais tempo para serem executadas. Se você começar a detetar desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o backlog de solicitações continuar a crescer, as operações do cliente S3 (como SOLICITAÇÕES PUT) acabarão falhando.

As solicitações do CloudMirror são mais propensas a serem afetadas pelo desempenho do endpoint de destino, pois essas solicitações geralmente envolvem mais transferência de dados do que solicitações de integração de pesquisa ou notificação de eventos.

As solicitações de serviço da plataforma falham

Para visualizar a taxa de falha da solicitação para serviços de plataforma:

1. Selecione **NODES**.
2. Selecione ***site*** > **Serviços de Plataforma**.
3. Veja o gráfico de taxa de erro de solicitação.



Alerta de serviços de plataforma indisponíveis

O alerta **Platform services unavailable** indica que nenhuma operação de serviço de plataforma pode ser executada em um local porque poucos nós de storage com o serviço RSM estão em execução ou disponíveis.

O serviço RSM garante que as solicitações de serviço da plataforma sejam enviadas para seus respetivos endpoints.

Para resolver esse alerta, determine quais nós de storage no local incluem o serviço RSM. (O serviço RSM está presente nos nós de storage que também incluem o serviço ADC.) Em seguida, certifique-se de que uma maioria simples desses nós de storage esteja em execução e disponível.

Se mais de um nó de storage que contém o serviço RSM falhar em um local, você perderá quaisquer solicitações de serviço de plataforma pendentes para esse site.

Orientação adicional para solução de problemas para endpoints de serviços de plataforma

Para obter informações adicionais, **Usar uma conta de locatário › solucionar problemas de endpoints de serviços de plataforma**consulte .

Informações relacionadas

"Solucionar problemas do sistema StorageGRID"

Gerenciar S3 Selecione para contas de inquilino

Você pode permitir que certos locatários do S3 usem o S3 Select para emitir solicitações SelectObjectContent em objetos individuais.

S3 Select fornece uma maneira eficiente de pesquisar grandes quantidades de dados sem ter que implantar um banco de dados e recursos associados para habilitar pesquisas. Ele também reduz o custo e a latência da recuperação de dados.

O que é o S3 Select?

S3 Select permite que os clientes S3 usem as solicitações SelectObjectContent para filtrar e recuperar apenas os dados necessários de um objeto. A implementação do StorageGRID do S3 Select inclui um subconjunto de comandos e recursos do S3 Select.

Considerações e requisitos para usar o S3 Select

Requisitos de administração da grade

O administrador da grade deve conceder aos locatários S3 Select Ability. Selecione **permitir S3 Selecionar** quando "criando um locatário" ou "editando um locatário".

Requisitos de formato de objeto

O objeto que você deseja consultar deve estar em um dos seguintes formatos:

- **CSV**. Pode ser usado como está ou comprimido em arquivos GZIP ou bzip2.
- **Parquet**. Requisitos adicionais para objetos em Parquet:
  - S3 Select suporta apenas compactação colunar usando GZIP ou Snappy. S3 Select não suporta compactação de objetos inteiros para objetos Parquet.
  - S3 a seleção não suporta saída em Parquet. Você deve especificar o formato de saída como CSV ou JSON.
  - O tamanho máximo do grupo de linhas não comprimidas é de 512 MB.
  - Você deve usar os tipos de dados especificados no esquema do objeto.
  - Você não pode usar os tipos lógicos INTERVALO, JSON, LISTA, HORA ou UUID.

Requisitos de endpoint

A solicitação SelectObjectContent deve ser enviada para um "Ponto de extremidade do balanceador de carga

StorageGRID".

Os nós Admin e Gateway usados pelo endpoint devem ser um dos seguintes:

- Nó de um dispositivo de serviços
- Um nó de software baseado em VMware
- Um nó bare metal executando um kernel com cgroup v2 habilitado

Considerações gerais

As consultas não podem ser enviadas diretamente para nós de storage.

> As solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Ative esse recurso somente quando necessário e somente para locatários confiáveis.

Consulte "Instruções para utilizar o S3 Select".

Para visualizar "Gráficos de Grafana" as operações S3 Select ao longo do tempo, selecione **SUPPORT** > **Tools** > **Metrics** no Grid Manager.

Configurar conexões de cliente

Configurar conexões de cliente S3

Como administrador de grade, você gerencia as opções de configuração que controlam como os aplicativos clientes S3 se conetam ao sistema StorageGRID para armazenar e recuperar dados.

> Os detalhes do Swift foram removidos desta versão do site do doc. "StorageGRID 11,8: Configurar conexões de cliente S3 e Swift"Consulte .

Tarefas de configuração

1. Execute tarefas de pré-requisito no StorageGRID, com base na forma como o aplicativo cliente se conetará ao StorageGRID.

Tarefas necessárias

Você deve obter:

- Endereços IP
- Nomes de domínio
- Certificado SSL

Tarefas opcionais

Opcionalmente, configure:

- Federação de identidade
- SSO

1. Use StorageGRID para obter os valores que o aplicativo precisa para se conetar à grade. Você pode usar o assistente de configuração do S3 ou configurar cada entidade do StorageGRID manualmente. E

Utilize o assistente de configuração S3

Siga as etapas no assistente de configuração S3.

Configure manualmente

1. Crie um grupo de alta disponibilidade
2. Crie o ponto final do balanceador de carga
3. Crie uma conta de locatário
4. Crie bucket e chaves de acesso
5. Configurar regra e política ILM

1. Use o aplicativo S3 para concluir a conexão com o StorageGRID. Crie entradas DNS para associar endereços IP a qualquer nome de domínio que você pretende usar.

   Conforme necessário, execute a configuração adicional da aplicação.

2. Executar tarefas contínuas na aplicação e no StorageGRID para gerenciar e monitorar o storage de objetos ao longo do tempo.

Informações necessárias para anexar o StorageGRID a um aplicativo cliente

Antes de poder anexar o StorageGRID a um aplicativo cliente S3, você deve executar as etapas de configuração no StorageGRID e obter determinado valor.

Quais valores eu preciso?

A tabela a seguir mostra os valores que você deve configurar no StorageGRID e onde esses valores são usados pelo aplicativo S3 e pelo servidor DNS.

Valor	Onde o valor está configurado	Onde o valor é usado
Endereços IP virtuais (VIP)	StorageGRID > grupo HA	Entrada DNS
Porta	StorageGRID > ponto final do balanceador de carga	Aplicação cliente
Certificado SSL	StorageGRID > ponto final do balanceador de carga	Aplicação cliente
Nome do servidor (FQDN)	StorageGRID > ponto final do balanceador de carga	• Aplicação cliente • Entrada DNS
S3 ID da chave de acesso e chave de acesso secreta	StorageGRID > locatário e balde	Aplicação cliente
Nome do balde/recipiente	StorageGRID > locatário e balde	Aplicação cliente

Como obtenho esses valores?

Dependendo de seus requisitos, você pode fazer um dos seguintes procedimentos para obter as informações de que precisa:

- **Use o "Assistente de configuração S3"**. O assistente de configuração do S3 ajuda a configurar rapidamente os valores necessários no StorageGRID e gera um ou dois arquivos que você pode usar ao configurar o aplicativo S3. O assistente orienta você pelas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID.

  > ⓘ Se você estiver configurando um aplicativo S3, é recomendável usar o assistente de configuração S3, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá uma personalização significativa.

- **Use o "Assistente de configuração do FabricPool"**. Semelhante ao assistente de configuração do S3, o assistente de configuração do FabricPool ajuda você a configurar rapidamente os valores necessários e gera um arquivo que você pode usar ao configurar um nível de nuvem do FabricPool no ONTAP.

  > ⓘ Se você planeja usar o StorageGRID como o sistema de storage de objetos em uma categoria de nuvem do FabricPool, é recomendável usar o assistente de configuração do FabricPool, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá personalização significativa.

- **Configurar itens manualmente**. Se estiver a ligar a uma aplicação S3 e preferir não utilizar o assistente de configuração S3, pode obter os valores necessários executando a configuração manualmente. Siga estes passos:

  a. Configure o grupo de alta disponibilidade (HA) que você deseja usar para o aplicativo S3. "Configurar grupos de alta disponibilidade"Consulte .

  b. Crie o ponto de extremidade do balanceador de carga que o aplicativo S3 usará. "Configurar pontos de extremidade do balanceador de carga"Consulte .

c. Crie a conta de locatário que o aplicativo S3 usará. "Crie uma conta de locatário"Consulte .

d. Para um locatário do S3, faça login na conta do locatário e gere uma ID de chave de acesso e chave de acesso secreta para cada usuário que acessará o aplicativo. "Crie suas próprias chaves de acesso"Consulte .

e. Crie um ou mais buckets do S3 na conta do locatário. Para S3, "Crie um balde S3D."consulte .

f. Para adicionar instruções de posicionamento específicas para os objetos pertencentes ao novo locatário ou bucket/container, crie uma nova regra ILM e ative uma nova política ILM para usar essa regra. "Criar regra ILM"Consulte e "Criar política ILM".

Segurança para clientes S3

As contas de locatário do StorageGRID usam aplicativos clientes S3 para salvar dados de objeto no StorageGRID. Você deve rever as medidas de segurança implementadas para aplicativos clientes.

Resumo

A lista a seguir resume como a segurança é implementada para a API REST do S3:

Segurança da ligação
TLS

Autenticação do servidor
Certificado de servidor X,509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador

Autenticação de cliente
S3 ID da chave de acesso à conta e chave de acesso secreta

Autorização do cliente
Propriedade do bucket e todas as políticas de controle de acesso aplicáveis

Como o StorageGRID fornece segurança para aplicativos clientes

Os aplicativos clientes S3 podem se conectar ao serviço Load Balancer em nós de Gateway ou nós de administração ou diretamente aos nós de storage.

- Os clientes que se conetam ao serviço Load Balancer podem usar HTTPS ou HTTP, com base em como "configure o ponto final do balanceador de carga"você .

  O HTTPS fornece comunicação segura e criptografada por TLS e é recomendado. Você deve anexar um certificado de segurança ao endpoint.

  O HTTP fornece uma comunicação menos segura e não criptografada e só deve ser usado para grades de teste ou não-produção.

- Os clientes que se conetam a nós de storage também podem usar HTTPS ou HTTP.

  HTTPS é o padrão e é recomendado.

  O HTTP fornece uma comunicação menos segura e não criptografada, mas pode ser opcionalmente "ativado" para grades de teste ou não-produção.

- As comunicações entre o StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço Load Balancer e os nós de armazenamento dentro da grade são criptografadas se o ponto de extremidade do balanceador de carga está configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer "Cabeçalhos de autenticação HTTP" ao StorageGRID para executar operações de API REST.

Certificados de segurança e aplicativos de cliente

Em todos os casos, os aplicativos clientes podem fazer conexões TLS usando um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado gerado pelo sistema StorageGRID:

- Quando os aplicativos cliente se conetam ao serviço do Load Balancer, eles usam o certificado que foi configurado para o endpoint do balanceador de carga. Cada ponto de extremidade do balanceador de carga tem o seu próprio certificado& n.o 8212;um certificado de servidor personalizado carregado pelo administrador da grelha ou um certificado que o administrador da grelha gerou no StorageGRID ao configurar o ponto de extremidade.

  "Considerações para balanceamento de carga"Consulte .

- Quando os aplicativos cliente se conetam diretamente a um nó de armazenamento, eles usam os certificados de servidor gerados pelo sistema que foram gerados para nós de armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade de certificação do sistema) ou um único certificado de servidor personalizado fornecido para a grade por um administrador de grade. "Adicione um certificado de API S3 personalizado"Consulte .

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que usam para estabelecer conexões TLS.

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto de conjuntos de codificação que os aplicativos clientes podem usar ao estabelecer uma sessão TLS. Para configurar cifras, vá para **CONFIGURATION** > **Security** > **Security settings** e selecione **TLS e SSH policies**.

Versões suportadas do TLS

O StorageGRID é compatível com TLS 1,2 e TLS 1,3.

SSLv3 e TLS 1,1 (ou versões anteriores) não são mais compatíveis.

Utilize o assistente de configuração S3

Use o assistente de configuração S3: Considerações e requisitos

Você pode usar o assistente de configuração S3 para configurar o StorageGRID como o sistema de armazenamento de objetos para um aplicativo S3.

Quando utilizar o assistente de configuração S3

O assistente de configuração S3 orienta você em cada etapa da configuração do StorageGRID para uso com um aplicativo S3. Como parte da conclusão do assistente, você baixa arquivos que você pode usar para inserir valores no aplicativo S3. Use o assistente para configurar o sistema mais rapidamente e para garantir

que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID.

Se tiver o "Permissão de acesso à raiz", pode concluir o assistente de configuração do S3 quando começar a utilizar o Gestor de grelha do StorageGRID ou pode aceder e concluir o assistente posteriormente. Dependendo de seus requisitos, você também pode configurar alguns ou todos os itens necessários manualmente e, em seguida, usar o assistente para montar os valores que um aplicativo S3 precisa.

Antes de utilizar o assistente

Antes de utilizar o assistente, confirme que concluiu estes pré-requisitos.

Obtenha endereços IP e configure interfaces VLAN

Se você configurar um grupo de alta disponibilidade (HA), você sabe a quais nós o aplicativo S3 se conetará e a qual rede StorageGRID será usada. Você também sabe quais valores inserir para o CIDR de sub-rede, endereço IP de gateway e endereços IP virtual (VIP).

Se você planeja usar uma LAN virtual para segregar o tráfego do aplicativo S3, já configurou a interface VLAN. "Configurar interfaces VLAN"Consulte .

Configure a federação de identidade e o SSO

Se você planeja usar federação de identidade ou logon único (SSO) para seu sistema StorageGRID, ativou esses recursos. Você também sabe qual grupo federado deve ter acesso root para a conta de locatário que o aplicativo S3 usará. "Use a federação de identidade"Consulte e "Configurar o logon único".

Obter e configurar nomes de domínio

Você sabe qual nome de domínio totalmente qualificado (FQDN) usar para o StorageGRID. As entradas do servidor de nomes de domínio (DNS) mapearão esse FQDN para os endereços IP virtuais (VIP) do grupo HA criado usando o assistente.

Se você planeja usar S3 solicitações virtuais de estilo hospedado, você deve ter "Configurados S3 nomes de domínio de endpoint"o . Recomenda-se o uso de solicitações virtuais de estilo hospedado.

Revise os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga do StorageGRID, analisou as considerações gerais sobre o balanceamento de carga. Você tem os certificados que você vai carregar ou os valores que você precisa para gerar um certificado.

Se você planeja usar um endpoint de balanceador de carga externo (de terceiros), terá o nome de domínio totalmente qualificado (FQDN), a porta e o certificado para esse balanceador de carga.

Configure todas as conexões de federação de grade

Se você quiser permitir que o locatário do S3 clone dados de conta e replique objetos de bucket para outra grade usando uma conexão de federação de grade, confirme o seguinte antes de iniciar o assistente:

- Você "configurada a conexão de federação de grade"tem .
- O estado da ligação é **ligado**.
- Você tem permissão de acesso root.

Acesse e conclua o assistente de configuração do S3

Você pode usar o assistente de configuração S3 para configurar o StorageGRID para uso com um aplicativo S3. O assistente de configuração fornece os valores que o aplicativo precisa para acessar um bucket do StorageGRID e salvar objetos.

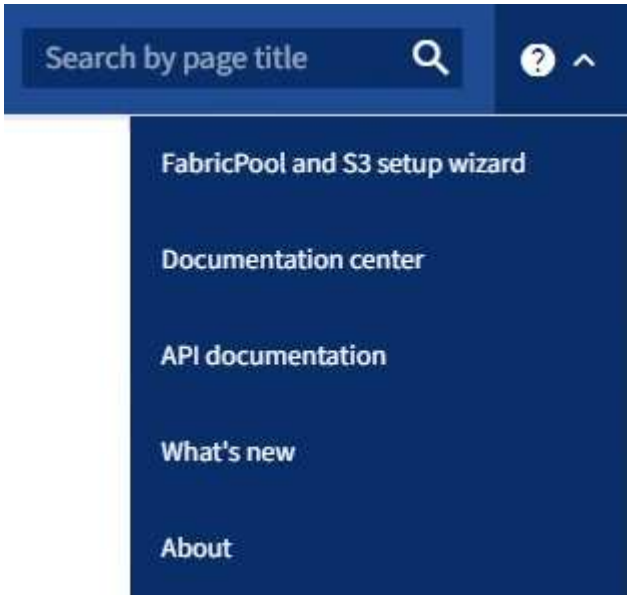
Antes de começar

- Você tem o "Permissão de acesso à raiz".
- Analisou "considerações e requisitos"o para utilizar o assistente.

Acesse o assistente

Passos

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Se o banner **FabricPool and S3 setup wizard** for exibido no painel, selecione o link no banner. Se o banner não for mais exibido, selecione o ícone de ajuda na barra de cabeçalho no Gerenciador de Grade e selecione **Assistente de configuração FabricPool e S3**.



3. Na seção S3 da aplicação da página do assistente de configuração FabricPool e S3, selecione **Configurar agora**.

Etapa 1 de 6: Configurar o grupo HA

Um grupo de HA é uma coleção de nós que contêm cada um o serviço StorageGRID Load Balancer. Um grupo de HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo de HA para ajudar a manter as conexões de dados do S3 disponíveis. Se a interface ativa no grupo de HA falhar, uma interface de backup poderá gerenciar a carga de trabalho com pouco impacto nas operações do S3.

Para obter detalhes sobre esta tarefa, "Gerenciar grupos de alta disponibilidade"consulte .

Passos

1. Se você pretende usar um balanceador de carga externo, não precisa criar um grupo de HA. Selecione **Ignorar este passo** e vá para Etapa 2 de 6: Configurar o ponto final do balanceador de carga.
2. Para usar o balanceador de carga do StorageGRID, você pode criar um novo grupo de HA ou usar um grupo de HA existente.

Criar grupo HA

a. Para criar um novo grupo HA, selecione **criar grupo HA**.

b. Para a etapa **Digite detalhes**, preencha os campos a seguir.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

c. Para a etapa **Adicionar interfaces**, selecione as interfaces de nó que deseja usar neste grupo HA.

Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

d. Para a etapa **priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para esse grupo de HA.

Arraste linhas para alterar os valores na coluna **Priority Order**.

A primeira interface na lista é a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.

Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços IP virtual (VIP) serão movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup, e assim por diante. Quando as falhas são resolvidas, os endereços VIP voltam para a interface de maior prioridade disponível.

e. Para a etapa **Inserir endereços IP**, preencha os campos a seguir.

Campo	Descrição
CIDR de sub-rede	O endereço da sub-rede VIP na notação CIDR & n.o 8212; um endereço IPv4 seguido de uma barra e o comprimento da sub-rede (0-32). O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.
Endereço IP do gateway (opcional)	Se os S3 endereços IP usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do StorageGRID VIP. O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Introduza pelo menos um e não mais de dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

f. Selecione **Create HA group** e, em seguida, selecione **Finish** para retornar ao assistente de configuração S3.

g. Selecione **continuar** para ir para a etapa do balanceador de carga.

Use o grupo HA existente

a. Para usar um grupo HA existente, selecione o nome do grupo HA no **Selecione um grupo HA**.

b. Selecione **continuar** para ir para a etapa do balanceador de carga.

Etapa 2 de 6: Configurar o ponto final do balanceador de carga

O StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos clientes. O balanceamento de carga maximiza a velocidade e a capacidade de conexão em vários nós de storage.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós de gateway e administrador, ou pode se conetar a um balanceador de carga externo (de terceiros). Recomenda-se a utilização do balanceador de carga StorageGRID.

Para obter detalhes sobre esta tarefa, "Considerações para balanceamento de carga"consulte .

Para usar o serviço de balanceador de carga do StorageGRID, selecione a guia **balanceador de carga do StorageGRID** e, em seguida, crie ou selecione o ponto de extremidade do balanceador de carga que deseja usar. Para usar um balanceador de carga externo, selecione a guia **balanceador de carga externo** e forneça detalhes sobre o sistema que você já configurou.

Criar endpoint

Passos

1. Para criar um ponto de extremidade do balanceador de carga, selecione **Create endpoint**.
2. Para a etapa **Digite os detalhes do endpoint**, preencha os campos a seguir.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo é padrão para 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada. Se você inserir 80 ou 443, o endpoint será configurado apenas em nós de Gateway, porque essas portas serão reservadas em nós de administração. **Observação:** as portas usadas por outros serviços de grade não são permitidas. Consulte "Referência da porta de rede".
Tipo de cliente	Deve ser **S3**.
Protocolo de rede	Selecione **HTTPS**. **Nota**: A comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

3. Para a etapa **Select Binding mode** (Selecionar modo de encadernação), especifique o modo de encadernação. O modo de vinculação controla como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP específicos e interfaces de rede.

Modo	Descrição
Global (predefinição)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global** (padrão), a menos que você precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos de HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo de HA para acessar esse endpoint. Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nós	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar esse endpoint.

Modo	Descrição
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway para acessar esse ponto final.

4. Para a etapa de Acesso ao locatário, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de inquilino podem usar esse endpoint para acessar seus buckets.
Permitir inquilinos selecionados	Somente as contas de locatário selecionadas podem usar esse endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar esse endpoint para acessar seus buckets. Todos os outros inquilinos podem usar este endpoint.

5. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use essa opção para carregar um certificado de servidor assinado pela CA, uma chave privada de certificado e um pacote de CA opcional.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Consulte "Configurar pontos de extremidade do balanceador de carga" para obter detalhes sobre o que introduzir.
Use o certificado StorageGRID S3	Utilize esta opção apenas se já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID. "Configure os certificados API do S3"Consulte para obter detalhes.

6. Selecione **Finish** (concluir) para voltar ao assistente de configuração do S3.
7. Selecione **Continue** para ir para a etapa de locatário e bucket.

> As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Use o ponto de extremidade do balanceador de carga existente

Passos

1. Para usar um endpoint existente, selecione seu nome no **Selecione um endpoint do balanceador de carga**.

2. Selecione **Continue** para ir para a etapa de locatário e bucket.

Use balanceador de carga externo

Passos

1. Para usar um balanceador de carga externo, preencha os campos a seguir.

Campo	Descrição
FQDN	O nome de domínio totalmente qualificado (FQDN) do balanceador de carga externo.
Porta	O número da porta que o aplicativo S3 usará para se conetar ao balanceador de carga externo.
Certificado	Copie o certificado do servidor para o balanceador de carga externo e cole-o neste campo.

2. Selecione **Continue** para ir para a etapa de locatário e bucket.

Passo 3 de 6: Crie locatário e bucket

Um locatário é uma entidade que pode usar aplicativos S3 para armazenar e recuperar objetos no StorageGRID. Cada locatário tem seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos.

Um bucket é um contentor usado para armazenar os objetos e metadados de objetos de um locatário. Embora os locatários possam ter muitos buckets, o assistente ajuda você a criar um locatário e um bucket da maneira mais rápida e fácil. Se você precisar adicionar buckets ou definir opções mais tarde, você pode usar o Gerenciador do locatário.

Para obter detalhes sobre esta tarefa, "Crie uma conta de locatário" consulte e "Crie um balde S3D.".

Passos

1. Insira um nome para a conta de locatário.

   Os nomes de inquilinos não precisam ser únicos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.

2. Defina o acesso root para a conta de locatário, com base se o sistema StorageGRID usa "federação de identidade", "Logon único (SSO)"ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver ativada	Especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade estiver ativada	a. Selecione um grupo federado existente a ter "Permissão de acesso à raiz" para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.

Opção	Faça isso
Se a federação de identidade e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente a ter "Permissão de acesso à raiz" para o locatário. Nenhum usuário local pode entrar.

3. Se você quiser que o assistente crie o ID da chave de acesso e a chave de acesso secreta para o usuário raiz, selecione **Create root user S3 access key automatically**.

   Selecione esta opção se o único usuário para o locatário for o usuário raiz. Se outros usuários usarem esse locatário, "Use o Gerenciador do Locatário" para configurar chaves e permissões.

4. Se você quiser criar um bucket para este locatário agora, selecione **Create bucket for this tenant**.

   Se o bloqueio de objeto S3 estiver ativado para a grade, o intervalo criado nesta etapa não terá o bloqueio de objeto S3 ativado. Se você precisar usar um bucket do S3 Object Lock para este aplicativo S3, não selecione criar um bucket agora. Em vez disso, use o Gerenciador do Locatário para "crie o balde" mais tarde.

   a. Introduza o nome do intervalo que a aplicação S3 irá utilizar. Por exemplo, `s3-bucket`.

      Não é possível alterar o nome do bucket depois de criar o bucket.

   b. Selecione a **região** para este intervalo.

      Use a região (`us-east-1`padrão) a menos que você espere usar o ILM no futuro para filtrar objetos com base na região do bucket.

5. Selecione **criar e continuar**.

passo 4 de 6: Transferir dados

Na etapa de download de dados, você pode baixar um ou dois arquivos para salvar os detalhes do que você acabou de configurar.

Passos

1. Se você selecionou **Create root user S3 access key automatically**, siga um ou ambos os procedimentos a seguir:
   - Selecione **Transferir chaves de acesso** para transferir um `.csv` ficheiro que contenha o nome da conta do locatário, o ID da chave de acesso e a chave de acesso secreta.
   - Selecione o ícone de cópia ( ) para copiar o ID da chave de acesso e a chave de acesso secreta para a área de transferência.
2. Selecione **Transferir valores de configuração** para transferir um `.txt` ficheiro que contenha as definições para o terminal do balanceador de carga, locatário, bucket e utilizador raiz.
3. Salve essas informações em um local seguro.

   Não feche esta página até ter copiado ambas as chaves de acesso. As chaves não estarão disponíveis depois de fechar esta página. Certifique-se de salvar essas informações em um local seguro, pois elas podem ser usadas para obter dados do seu sistema StorageGRID.

4. Se solicitado, marque a caixa de seleção para confirmar que você baixou ou copiou as chaves.
5. Selecione **Continue** para ir para a regra ILM e a etapa de política.

Passo 5 de 6: Revise a regra ILM e a política ILM para S3

As regras de gerenciamento do ciclo de vida das informações (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos em seu sistema StorageGRID. A política de ILM incluída no StorageGRID faz duas cópias replicadas de todos os objetos. Esta política está em vigor até que você ative pelo menos uma nova política.

Passos

1. Reveja as informações fornecidas na página.
2. Se você quiser adicionar instruções específicas para os objetos pertencentes ao novo locatário ou bucket, crie uma nova regra e uma nova política. "Criar regra ILM"Consulte e "Use políticas ILM".
3. Selecione **Reviewei estes passos e compreendi o que preciso fazer**.
4. Marque a caixa de seleção para indicar que você entende o que fazer a seguir.
5. Selecione **continuar** para ir para **Resumo**.

Passo 6 de 6: Rever resumo

Passos

1. Reveja o resumo.
2. Anote os detalhes nas próximas etapas, que descrevem a configuração adicional que pode ser necessária antes de se conetar ao cliente S3. Por exemplo, selecionar **entrar como root** leva-o ao Gerenciador de inquilinos, onde você pode adicionar usuários de inquilinos, criar buckets adicionais e atualizar configurações de bucket.
3. Selecione **Finish**.
4. Configure o aplicativo usando o arquivo baixado do StorageGRID ou os valores obtidos manualmente.

Gerenciar grupos de HA

O que são grupos de alta disponibilidade (HA)?

Os grupos de alta disponibilidade (HA) fornecem conexões de dados altamente disponíveis para clientes S3 e conexões altamente disponíveis para o Gerenciador de Grade e o Gerente do locatário.

Você pode agrupar as interfaces de rede de vários nós de administrador e gateway em um grupo de alta disponibilidade (HA). Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho.

Cada grupo de HA fornece acesso aos serviços compartilhados nos nós selecionados.

- Os GRUPOS HA que incluem nós de gateway, nós de administração ou ambos fornecem conexões de dados altamente disponíveis para clientes S3.
- Os GRUPOS DE HA que incluem apenas os nós de Admin fornecem conexões altamente disponíveis ao Gerenciador de Grade e ao Gerente do locatário.
- Um grupo de HA que inclui apenas dispositivos de serviços e nós de software baseados em VMware pode fornecer conexões altamente disponíveis para "S3 inquilinos que usam S3 Select"o . Os GRUPOS HA são

recomendados ao usar S3 Select, mas não são necessários.

Como criar um grupo HA?

1. Você seleciona uma interface de rede para um ou mais nós de administrador ou nós de gateway. Você pode usar uma interface Grid Network (eth0), uma interface Client Network (eth2), uma interface VLAN ou uma interface de acesso que você adicionou ao nó.

   > Não é possível adicionar uma interface a um grupo HA se ele tiver um endereço IP atribuído pelo DHCP.

2. Você especifica uma interface para ser a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.
3. Você determina a ordem de prioridade para quaisquer interfaces de backup.
4. Você atribui um a 10 endereços IP virtuais (VIP) ao grupo. Os aplicativos clientes podem usar qualquer um desses endereços VIP para se conetar ao StorageGRID.

Para obter instruções, "Configurar grupos de alta disponibilidade"consulte .

O que é a interface ativa?

Durante a operação normal, todos os endereços VIP do grupo HA são adicionados à interface principal, que é a primeira interface na ordem de prioridade. Enquanto a interface principal permanecer disponível, ela é usada quando os clientes se conetam a qualquer endereço VIP do grupo. Ou seja, durante a operação normal, a interface principal é a interface "ativa" para o grupo.

Da mesma forma, durante a operação normal, quaisquer interfaces de prioridade inferior para o grupo HA funcionam como interfaces de "backup". Essas interfaces de backup não são usadas a menos que a interface principal (atualmente ativa) fique indisponível.

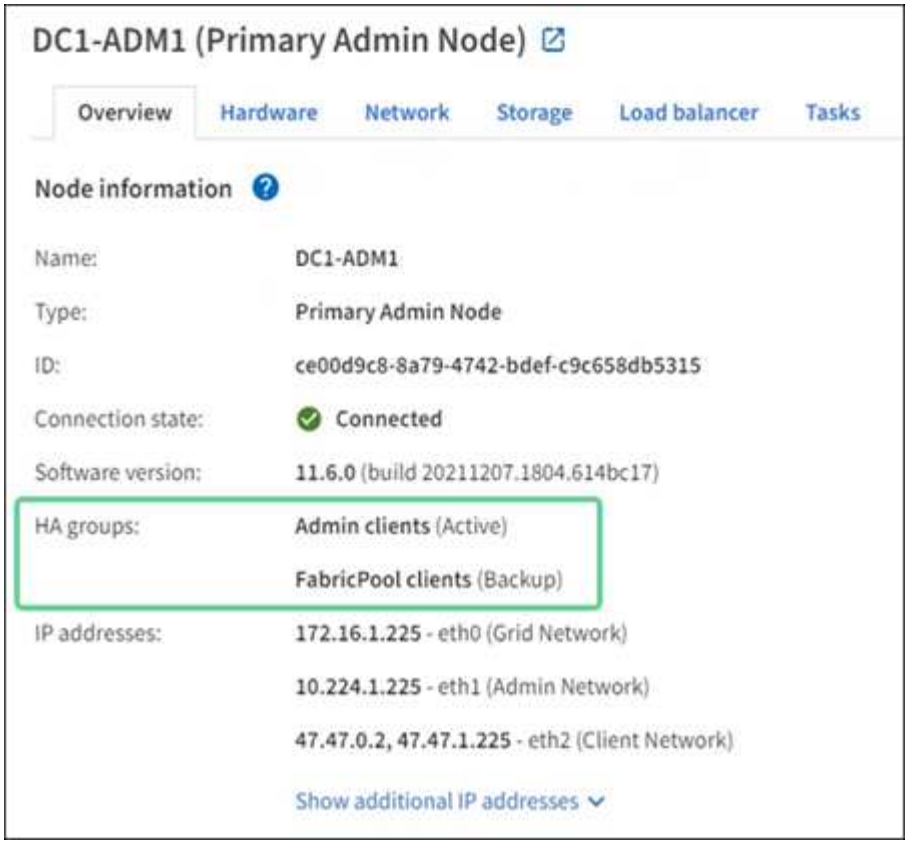
Exibir o status atual do grupo de HA de um nó

Para ver se um nó está atribuído a um grupo de HA e determinar seu status atual, selecione **NÓS** > ***node***.

Se a guia **Visão geral** incluir uma entrada para **grupos de HA**, o nó será atribuído aos grupos de HA listados. O valor após o nome do grupo é o status atual do nó no grupo HA:

- **Ativo**: O grupo HA está sendo hospedado neste nó.
- **Backup**: O grupo HA não está usando esse nó no momento; essa é uma interface de backup.
- **Stopped**: O grupo HA não pode ser hospedado neste nó porque o serviço de alta disponibilidade (keepalived) foi interrompido manualmente.
- **Falha**: O grupo HA não pode ser hospedado neste nó por causa de um ou mais dos seguintes:
  - O serviço do Load Balancer (nginx-gw) não está sendo executado no nó.
  - A interface eth0 ou VIP do nó está inativa.
  - O nó está inativo.

Neste exemplo, o nó de administração principal foi adicionado a dois grupos de HA. Este nó é atualmente a interface ativa para o grupo de clientes administradores e uma interface de backup para o grupo de clientes FabricPool.



O que acontece quando a interface ativa falha?

A interface que atualmente hospeda os endereços VIP é a interface ativa. Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços VIP serão movidos para a primeira interface de backup disponível na ordem de prioridade. Se essa interface falhar, os endereços VIP passam para a próxima interface de backup disponível, e assim por diante.

O failover pode ser acionado por qualquer um destes motivos:

- O nó no qual a interface está configurada é desativado.
- O nó no qual a interface está configurada perde a conetividade com todos os outros nós por pelo menos 2 minutos.
- A interface ativa desce.
- O serviço Load Balancer pára.
- O serviço de alta disponibilidade pára.

> O failover pode não ser acionado por falhas de rede externas ao nó que hospeda a interface ativa. Da mesma forma, o failover não é acionado pelos serviços do Gerenciador de Grade ou do Gerenciador de Locatário.

O processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos clientes tenham pouco impactos e possam confiar em comportamentos normais de repetição para continuar a operação.

Quando a falha é resolvida e uma interface de prioridade mais alta torna-se disponível novamente, os endereços VIP são movidos automaticamente para a interface de prioridade mais alta que está disponível.

Como os grupos HA são usados?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões altamente disponíveis ao StorageGRID para dados de objetos e para uso administrativo.

- Um grupo de HA pode fornecer conexões administrativas altamente disponíveis ao Gerenciador de Grade ou ao Gerente do Locatário.
- Um grupo HA pode fornecer conexões de dados altamente disponíveis para clientes S3.
- Um grupo de HA que contém apenas uma interface permite fornecer muitos endereços VIP e definir explicitamente endereços IPv6.

Um grupo de HA poderá fornecer alta disponibilidade somente se todos os nós incluídos no grupo oferecerem os mesmos serviços. Ao criar um grupo de HA, adicione interfaces dos tipos de nós que fornecem os serviços de que você precisa.

- **Admin Nodes**: Inclua o serviço Load Balancer e habilite o acesso ao Grid Manager ou ao Tenant Manager.
- **Gateway Nodes**: Inclua o serviço Load Balancer.

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso ao Grid Manager	• Nó de administração principal (**primário**) • Nós de administração não primários **Nota:** o nó de administração principal deve ser a interface principal. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.
Acesso apenas ao Gestor do Locatário	• Nós de administração primários ou não primários
Acesso ao cliente S3 — Serviço de Load Balancer	• Nós de administração • Nós de gateway
Acesso de cliente S3 para "S3 Selecione"	• Aparelhos de serviços • Nós de software baseados em VMware **Nota**: Os GRUPOS HA são recomendados ao usar o S3 Select, mas não são necessários.

Limitações do uso de grupos de HA com Grid Manager ou Tenant Manager

Se um serviço do Grid Manager ou do Tenant Manager falhar, o failover do grupo HA não será acionado.

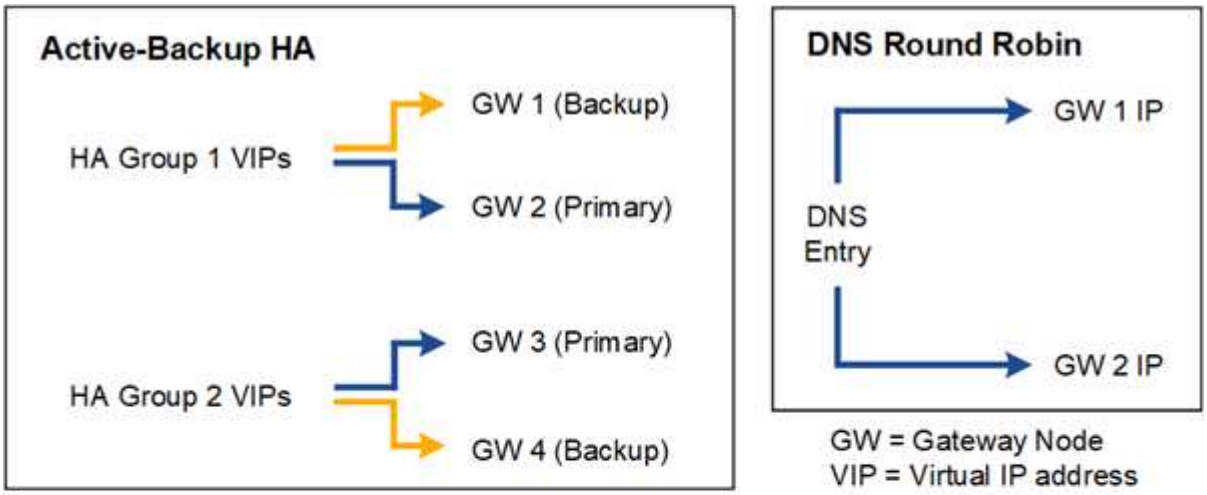
Se você estiver conetado ao Gerenciador de Grade ou ao Gerenciador de Locatário quando ocorrer failover, você será desconetado e deverá fazer login novamente para retomar sua tarefa.

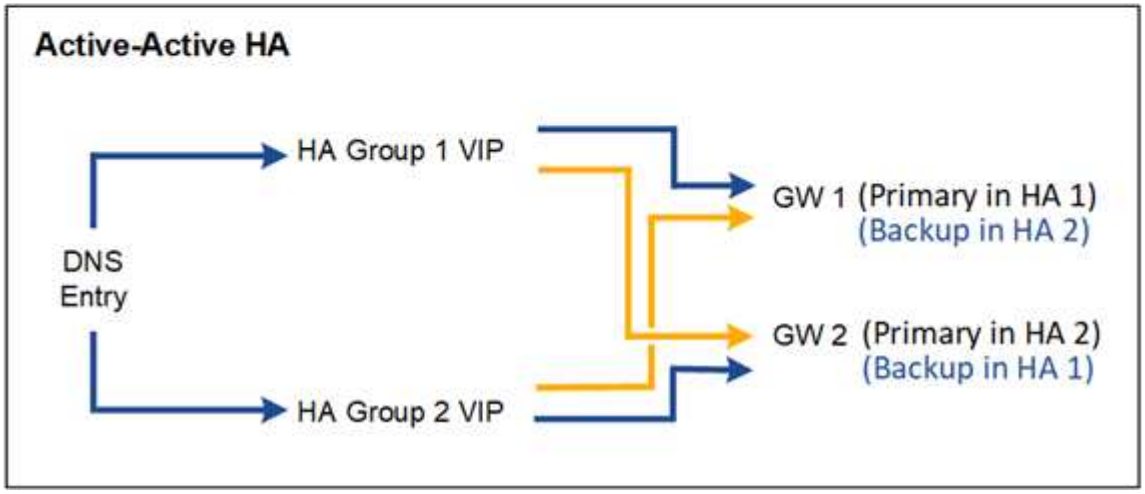
Alguns procedimentos de manutenção não podem ser executados quando o nó Admin principal não está disponível. Durante o failover, você pode usar o Gerenciador de Grade para monitorar seu sistema StorageGRID.

Opções de configuração para grupos de HA

Os diagramas a seguir fornecem exemplos de diferentes maneiras de configurar grupos de HA. Cada opção tem vantagens e desvantagens.

Nos diagramas, azul indica a interface principal no grupo HA e amarelo indica a interface de backup no grupo HA.





A tabela resume os benefícios de cada configuração de HA mostrada no diagrama.

Configuração	Vantagens	Desvantagens
Active-Backup HA	• Gerenciado pelo StorageGRID sem dependências externas. • Failover rápido.	• Apenas um nó em um grupo de HA está ativo. Pelo menos um nó por grupo de HA ficará inativo.

Configuração	Vantagens	Desvantagens
DNS Round Robin	• Maior taxa de transferência agregada. • Sem hosts ociosos.	• Failover lento, que pode depender do comportamento do cliente. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.
Ha ativo-ativo	• O tráfego é distribuído em vários grupos de HA. • Alta taxa de transferência agregada que é dimensionada com o número de grupos de HA. • Failover rápido.	• Mais complexo de configurar. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.

Configurar grupos de alta disponibilidade

Você pode configurar grupos de alta disponibilidade (HA) para fornecer acesso altamente disponível aos serviços em nós de administração ou nós de gateway.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Se você planeja usar uma interface VLAN em um grupo HA, criou a interface VLAN. "Configurar interfaces VLAN"Consulte .
- Se você planeja usar uma interface de acesso para um nó em um grupo de HA, criou a interface:
  - **Red Hat Enterprise Linux (antes de instalar o nó)**: "Criar arquivos de configuração de nó"
  - * Ubuntu ou Debian (antes de instalar o nó)*: "Criar arquivos de configuração de nó"
  - * Linux (após a instalação do nó)*: "Linux: Adicione interfaces de tronco ou acesso a um nó"
  - **VMware (após a instalação do nó)**: "VMware: Adicione interfaces de tronco ou acesso a um nó"

Crie um grupo de alta disponibilidade

Ao criar um grupo de alta disponibilidade, você seleciona uma ou mais interfaces e as organiza por ordem de prioridade. Em seguida, atribua um ou mais endereços VIP ao grupo.

Uma interface deve ser incluída em um grupo de HA para um nó de gateway ou um nó de administrador. Um grupo de HA só pode usar uma interface para qualquer nó; no entanto, outras interfaces para o mesmo nó podem ser usadas em outros grupos de HA.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selecione **criar**.

Introduza os detalhes do grupo HA

Passos

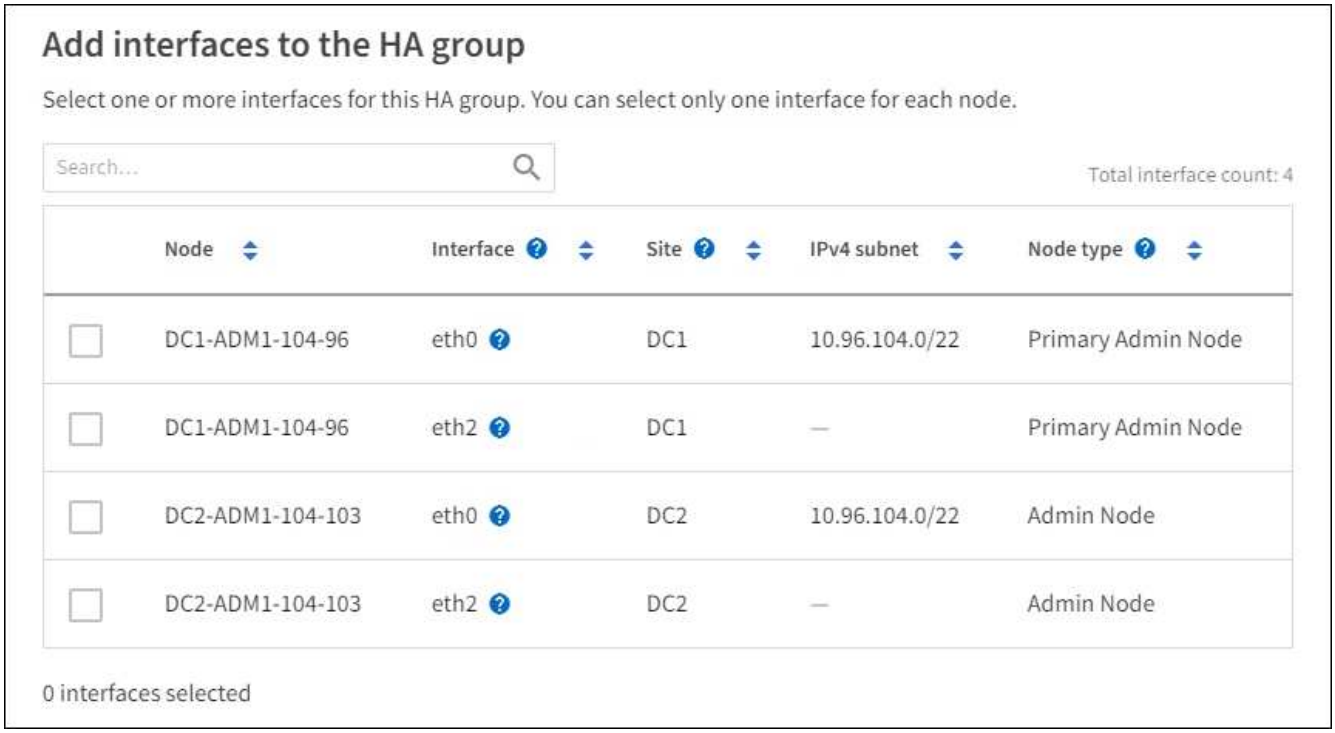
1. Forneça um nome exclusivo para o grupo HA.
2. Opcionalmente, insira uma descrição para o grupo HA.
3. Selecione **continuar**.

Adicionar interfaces ao grupo HA

Passos

1. Selecione uma ou mais interfaces para adicionar a esse grupo de HA.

   Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.



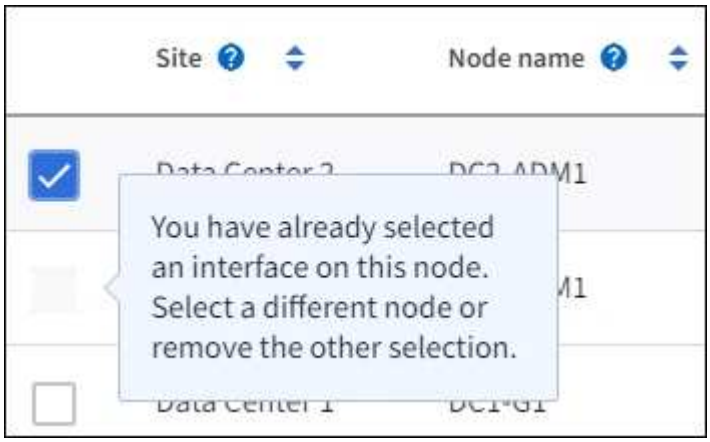
   Depois de criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

Diretrizes para a seleção de interfaces

- Você deve selecionar pelo menos uma interface.
- Você pode selecionar apenas uma interface para um nó.
- Se o grupo de HA for para proteção de HA dos serviços Admin Node, que incluem o Grid Manager e o Tenant Manager, selecione interfaces apenas em nós de administração.
- Se o grupo de HA for para proteção HA do tráfego de clientes S3, selecione interfaces em nós de administração, nós de gateway ou ambos.
- Se você selecionar interfaces em diferentes tipos de nós, uma nota informativa será exibida. Lembre-se de que, se ocorrer um failover, os serviços fornecidos pelo nó ativo anteriormente podem não estar disponíveis no nó recém-ativo. Por exemplo, um nó de gateway de backup não pode fornecer proteção de HA dos serviços Admin Node. Da mesma forma, um nó Admin de backup não pode executar todos

os procedimentos de manutenção que o nó Admin principal pode fornecer.

- Se você não puder selecionar uma interface, sua caixa de seleção será desativada. A dica da ferramenta fornece mais informações.



- Não é possível selecionar uma interface se o seu valor de sub-rede ou gateway entrar em conflito com outra interface selecionada.
- Não é possível selecionar uma interface configurada se ela não tiver um endereço IP estático.

2. Selecione **continuar**.

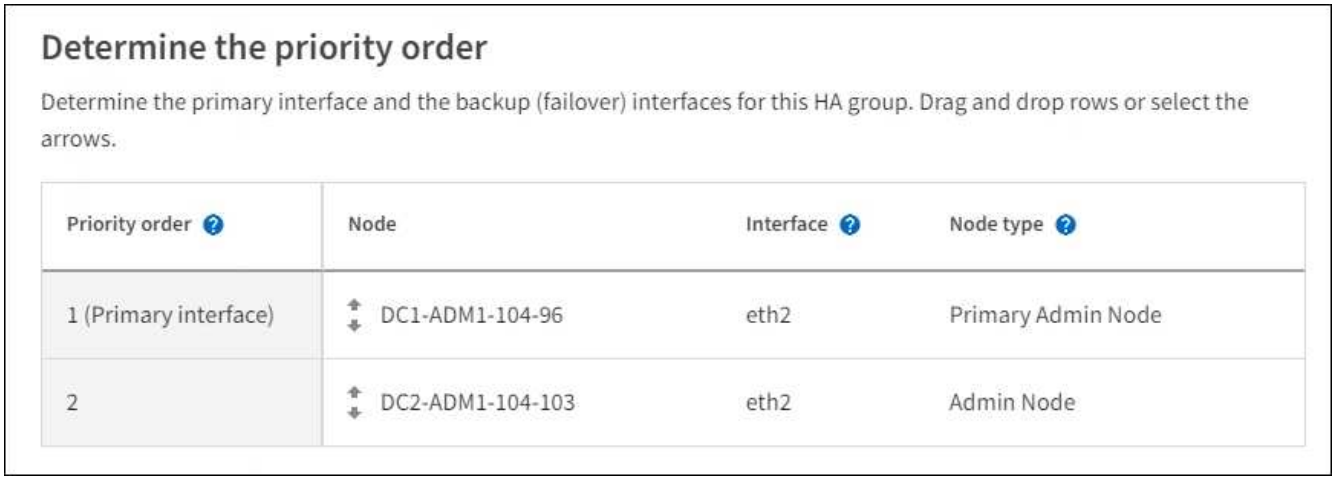
Determine a ordem de prioridade

Se o grupo de HA incluir mais de uma interface, você poderá determinar qual é a interface principal e quais são as interfaces de backup (failover). Se a interface principal falhar, os endereços VIP serão movidos para a interface de maior prioridade disponível. Se essa interface falhar, os endereços VIP passam para a próxima interface de maior prioridade disponível, e assim por diante.

Passos

1. Arraste linhas na coluna **Priority Order** para determinar a interface principal e quaisquer interfaces de backup.

   A primeira interface na lista é a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.



Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deverá selecionar uma interface no nó Admin primário para ser a interface principal. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

2. Selecione **continuar**.

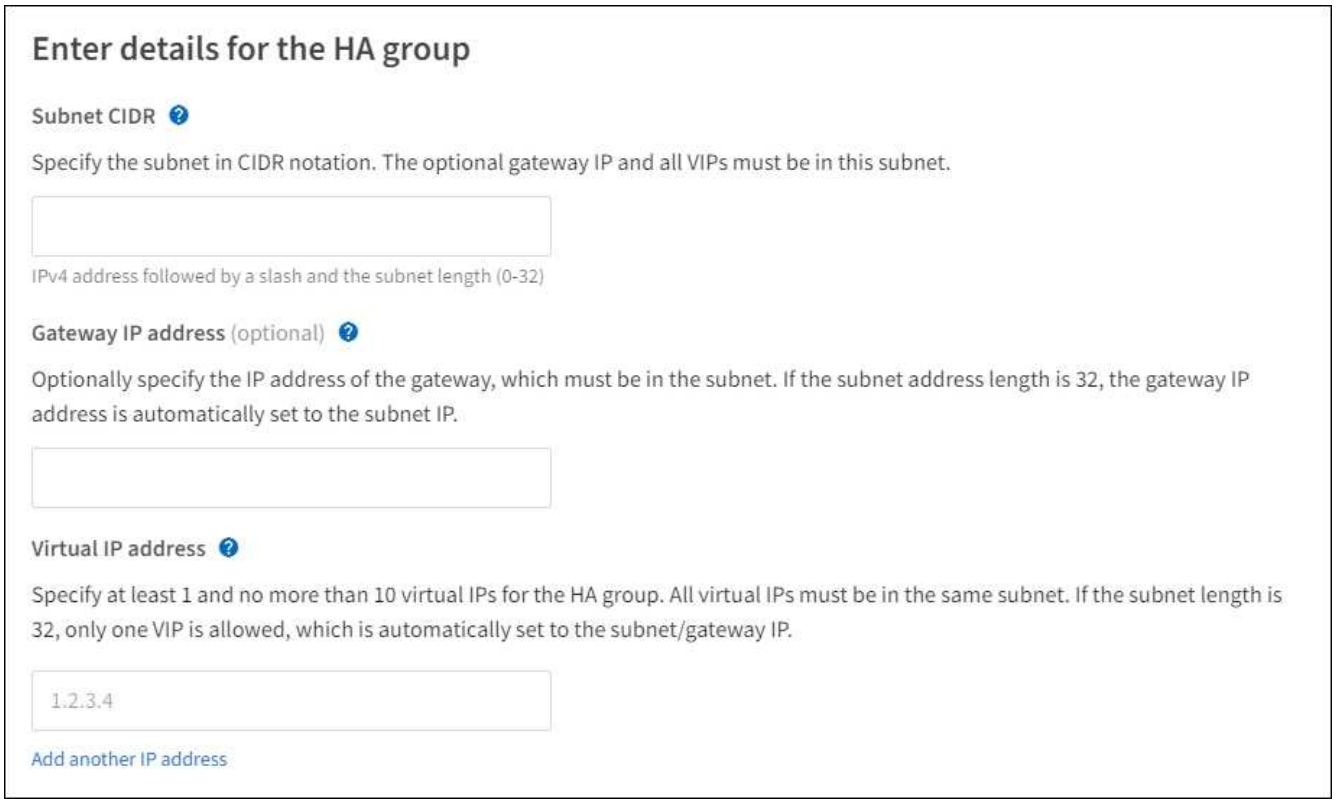
Introduza endereços IP

Passos

1. No campo **Subnet CIDR**, especifique a sub-rede VIP na notação CIDR—um endereço IPv4 seguido de uma barra e o comprimento da sub-rede (0-32).

   O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.

   Se você usar um prefixo de 32 bits, o endereço de rede VIP também serve como endereço de gateway e endereço VIP.



2. Opcionalmente, se qualquer cliente administrativo ou locatário do S3 acessar esses endereços VIP de uma sub-rede diferente, digite o **Endereço IP do Gateway**. O endereço de gateway deve estar dentro da sub-rede VIP.

   Os usuários de cliente e administrador usarão esse gateway para acessar os endereços IP virtuais.

3. Introduza pelo menos um e não mais de dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP e todos estarão ativos ao mesmo tempo na interface ativa.

   Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

4. Selecione **Create HA group** e selecione **Finish**.

   O Grupo HA é criado e agora você pode usar os endereços IP virtuais configurados.

Próximas etapas

Se você usar esse grupo de HA para balanceamento de carga, crie um ponto de extremidade do balanceador de carga para determinar a porta e o protocolo de rede e para anexar todos os certificados necessários. "Configurar pontos de extremidade do balanceador de carga"Consulte .

Edite um grupo de alta disponibilidade

Você pode editar um grupo de alta disponibilidade (HA) para alterar seu nome e descrição, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou atualizar endereços IP virtuais.

Por exemplo, talvez seja necessário editar um grupo de HA se desejar remover o nó associado a uma interface selecionada em um procedimento de desativação de site ou nó.

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.

   A página grupos de alta disponibilidade mostra todos os grupos de HA existentes.

2. Marque a caixa de seleção para o grupo HA que deseja editar.
3. Siga um destes procedimentos, com base no que você deseja atualizar:
   - Selecione **ações** > **Editar endereço IP virtual** para adicionar ou remover endereços VIP.
   - Selecione **ações** > **Editar grupo HA** para atualizar o nome ou a descrição do grupo, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou remover endereços VIP.
4. Se você selecionou **Editar endereço IP virtual**:
   a. Atualize os endereços IP virtuais do grupo HA.
   b. Selecione **Guardar**.
   c. Selecione **Finish**.
5. Se você selecionou **Edit HA group**:
   a. Opcionalmente, atualize o nome ou a descrição do grupo.
   b. Opcionalmente, selecione ou desmarque as caixas de seleção para adicionar ou remover interfaces.

      Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deverá selecionar uma interface no nó Admin primário para ser a interface principal. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal

   c. Opcionalmente, arraste linhas para alterar a ordem de prioridade da interface principal e de quaisquer interfaces de backup para esse grupo de HA.
   d. Opcionalmente, atualize os endereços IP virtuais.
   e. Selecione **Save** e, em seguida, selecione **Finish**.

Remova um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) de cada vez.

> Não é possível remover um grupo de HA se ele estiver vinculado a um ponto de extremidade do balanceador de carga. Para excluir um grupo de HA, você deve removê-lo de todos os pontos de extremidade do balanceador de carga que o usem.

Para evitar interrupções do cliente, atualize os aplicativos de cliente S3 afetados antes de remover um grupo de HA. Atualize cada cliente para se conetar usando outro endereço IP, por exemplo, o endereço IP virtual de um grupo HA diferente ou o endereço IP configurado para uma interface durante a instalação.

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
2. Revise a coluna **Load balancer endpoints** para cada grupo de HA que você deseja remover. Se algum ponto final do balanceador de carga estiver listado:
   a. Aceda a **CONFIGURATION** > **Network** > **Load balancer endpoints**.
   b. Selecione a caixa de verificação para o endpoint.
   c. Selecione **actions** > **Edit endpoint binding mode**
   d. Atualize o modo de encadernação para remover o grupo HA.
   e. Selecione **Salvar alterações**.
3. Se não houver pontos de extremidade do balanceador de carga listados, marque a caixa de seleção para cada grupo de HA que você deseja remover.
4. Selecione **ações** > **Remover grupo HA**.
5. Reveja a mensagem e selecione **Eliminar grupo HA** para confirmar a sua seleção.

   Todos os grupos de HA selecionados são removidos. Um banner verde de sucesso aparece na página grupos de alta disponibilidade.

Gerenciar o balanceamento de carga

Considerações para balanceamento de carga

Você pode usar o balanceamento de carga para lidar com cargas de trabalho de ingestão e recuperação de clientes do S3.

O que é balanceamento de carga?

Quando um aplicativo cliente salva ou recupera dados de um sistema StorageGRID, o StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de obtenção e recuperação. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo a carga de trabalho em vários nós de storage.

O serviço StorageGRID Load Balancer é instalado em todos os nós de administração e em todos os nós de gateway e fornece balanceamento de carga de camada 7. Ele executa o encerramento do TLS (Transport Layer Security) das solicitações do cliente, inspeciona as solicitações e estabelece novas conexões seguras aos nós de storage.

O serviço Load Balancer em cada nó opera de forma independente ao encaminhar o tráfego do cliente para

os nós de storage. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de storage com maior disponibilidade de CPU.

> Embora o serviço de balanceamento de carga StorageGRID seja o mecanismo de balanceamento de carga recomendado, você pode querer integrar um balanceador de carga de terceiros. Para obter informações, contacte o representante da sua conta NetApp ou "TR-4626: Balanceadores de carga globais e de terceiros da StorageGRID" consulte .

Quantos nós de balanceamento de carga eu preciso?

Como prática recomendada geral, cada local no seu sistema StorageGRID deve incluir dois ou mais nós com o serviço de balanceador de carga. Por exemplo, um site pode incluir dois nós de Gateway ou um nó de administrador e um nó de gateway. Certifique-se de que há uma infraestrutura adequada de rede, hardware ou virtualização para cada nó de balanceamento de carga, esteja você usando dispositivos de serviços, nós bare metal ou nós baseados em máquina virtual (VM).

O que é um ponto de extremidade do balanceador de carga?

Um ponto de extremidade do balanceador de carga define a porta e o protocolo de rede (HTTPS ou HTTP) que as solicitações de aplicativos de cliente de entrada e saída usarão para acessar os nós que contêm o serviço Load Balancer. O endpoint também define o tipo de cliente (S3), o modo de encadernação e, opcionalmente, uma lista de inquilinos permitidos ou bloqueados.

Para criar um ponto de extremidade do balanceador de carga, selecione **CONFIGURATION** > **Network** > **Load balancer endpoints** ou conclua o assistente de configuração do FabricPool e do S3. Para obter instruções:

- "Configurar pontos de extremidade do balanceador de carga"
- "Utilize o assistente de configuração S3"
- "Utilize o assistente de configuração do FabricPool"

Considerações para a porta

A porta de um ponto de extremidade do balanceador de carga é padrão para 10433 para o primeiro ponto de extremidade criado, mas você pode especificar qualquer porta externa não utilizada entre 1 e 65535. Se você usar a porta 80 ou 443, o endpoint usará o serviço Load Balancer somente nos nós do Gateway. Essas portas são reservadas em nós de administração. Se você usar a mesma porta para mais de um endpoint, você deve especificar um modo de encadernação diferente para cada endpoint.

As portas usadas por outros serviços de grade não são permitidas. Consulte "Referência da porta de rede".

Considerações para o protocolo de rede

Na maioria dos casos, as conexões entre aplicativos cliente e StorageGRID devem usar criptografia TLS (Transport Layer Security). A conexão com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada, especialmente em ambientes de produção. Ao selecionar o protocolo de rede para o ponto de extremidade do balanceador de carga do StorageGRID, deve selecionar **HTTPS**.

Considerações para certificados de endpoint do balanceador de carga

Se selecionar **HTTPS** como protocolo de rede para o ponto de extremidade do balanceador de carga, tem de fornecer um certificado de segurança. Você pode usar qualquer uma dessas três opções ao criar o ponto de extremidade do balanceador de carga:

- **Carregue um certificado assinado (recomendado)**. Este certificado pode ser assinado por uma autoridade de certificação pública ou privada (CA). Usar um certificado de servidor CA publicamente confiável para proteger a conexão é a melhor prática. Em contraste com os certificados gerados, os certificados assinados por uma CA podem ser girados sem interrupções, o que pode ajudar a evitar problemas de expiração.

  Você deve obter os seguintes arquivos antes de criar o ponto de extremidade do balanceador de carga:

  - O arquivo de certificado do servidor personalizado.
  - O arquivo de chave privada de certificado de servidor personalizado.
  - Opcionalmente, um pacote de CA dos certificados de cada autoridade de certificação de emissão intermediária.
- **Gerar um certificado autoassinado**.
- **Use o certificado global StorageGRID S3**. Você deve carregar ou gerar uma versão personalizada deste certificado antes de selecioná-lo para o ponto de extremidade do balanceador de carga. "Configure os certificados API do S3"Consulte .

Quais valores eu preciso?

Para criar o certificado, você deve saber todos os nomes de domínio e endereços IP que os aplicativos cliente S3 usarão para acessar o endpoint.

A entrada **Assunto DN** (Nome distinto) do certificado deve incluir o nome de domínio totalmente qualificado que o aplicativo cliente usará para o StorageGRID. Por exemplo:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Conforme necessário, o certificado pode usar curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração e nós de gateway que executam o serviço Load Balancer. Por exemplo, `*.storagegrid.example.com` usa o caractere curinga * para representar `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`.

Se você planeja usar S3 solicitações virtuais de estilo hospedado, o certificado também deve incluir uma entrada **Nome alternativo** para cada "Nome de domínio do endpoint S3" um que você configurou, incluindo nomes curinga. Por exemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Se você usar curingas para nomes de domínio, revise o "Diretrizes de fortalecimento para certificados de servidor".

Você também deve definir uma entrada DNS para cada nome no certificado de segurança.

Como faço para gerenciar certificados expirados?

Se o certificado usado para proteger a conexão entre o aplicativo S3 e o StorageGRID expirar, o aplicativo poderá perder temporariamente o acesso ao StorageGRID.

Para evitar problemas de expiração de certificado, siga estas práticas recomendadas:

- Monitore cuidadosamente quaisquer alertas que avisem sobre datas de expiração de certificado que estejam se aproximando, como **validade do certificado de endpoint do balanceador de carga** e **expiração do certificado de servidor global para alertas da API S3**.
- Mantenha sempre as versões do certificado do StorageGRID e do aplicativo S3 sincronizadas. Se você substituir ou renovar o certificado usado para um ponto de extremidade do balanceador de carga, você deve substituir ou renovar o certificado equivalente usado pelo aplicativo S3.
- Use um certificado de CA assinado publicamente. Se você usar um certificado assinado por uma CA, poderá substituir certificados que expirarão em breve sem interrupções.
- Se você gerou um certificado StorageGRID auto-assinado e esse certificado está prestes a expirar, você deve substituir manualmente o certificado no StorageGRID e no aplicativo S3 antes que o certificado existente expire.

Considerações para o modo de encadernação

O modo de encadernação permite controlar quais endereços IP podem ser usados para acessar um ponto de extremidade do balanceador de carga. Se um endpoint usar um modo de encadernação, os aplicativos cliente só poderão acessar o endpoint se usarem um endereço IP permitido ou seu nome de domínio totalmente qualificado (FQDN) correspondente. Os aplicativos clientes que usam qualquer outro endereço IP ou FQDN não podem acessar o endpoint.

Você pode especificar qualquer um dos seguintes modos de encadernação:

- **Global** (padrão): Os aplicativos cliente podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use esta configuração a menos que você precise restringir a acessibilidade de um endpoint.
- **IPs virtuais de grupos HA**. Os aplicativos cliente devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA.
- * Interfaces de nó*. Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas.
- **Tipo de nó**. Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway.

Considerações para acesso ao locatário

O acesso ao locatário é um recurso de segurança opcional que permite controlar quais contas de locatário do StorageGRID podem usar um endpoint do balanceador de carga para acessar seus buckets. Você pode permitir que todos os locatários acessem um endpoint (padrão) ou especificar uma lista dos locatários permitidos ou bloqueados para cada endpoint.

Você pode usar esse recurso para fornecer um melhor isolamento de segurança entre os locatários e seus endpoints. Por exemplo, você pode usar esse recurso para garantir que os materiais mais secretos ou altamente classificados de propriedade de um locatário permaneçam completamente inacessíveis para outros inquilinos.

Para fins de controle de acesso, o locatário é determinado a partir das chaves de acesso usadas na solicitação do cliente, se nenhuma chave de acesso for fornecida como parte da solicitação (como com acesso anônimo) o proprietário do bucket é usado para determinar o locatário.

Exemplo de acesso ao locatário

Para entender como esse recurso de segurança funciona, considere o seguinte exemplo:

1. Você criou dois pontos de extremidade do balanceador de carga, como segue:
   - **Public** endpoint: Usa a porta 10443 e permite o acesso a todos os inquilinos.
   - * Ponto final Top SECRET*: Usa a porta 10444 e permite o acesso apenas ao locatário **Top SECRET**. Todos os outros inquilinos estão bloqueados para acessar este endpoint.
2. O `top-secret.pdf` está em um balde de propriedade do **Top SECRET** inquilino.

Para acessar o `top-secret.pdf`, um usuário no locatário **Top SECRET** pode emitir uma SOLICITAÇÃO GET para `https://w.x.y.z:10444/top-secret.pdf`. Como esse locatário tem permissão para usar o endpoint 10444, o usuário pode acessar o objeto. No entanto, se um usuário pertencente a qualquer outro locatário emitir a mesma solicitação para o mesmo URL, ele receberá uma mensagem de acesso negado imediata. O acesso é negado mesmo que as credenciais e a assinatura sejam válidas.

Disponibilidade da CPU

O serviço Load Balancer em cada nó de administração e nó de gateway opera de forma independente ao encaminhar o tráfego S3 para os nós de storage. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de storage com maior disponibilidade de CPU. As informações de carga da CPU do nó são atualizadas a cada poucos minutos, mas a ponderação pode ser atualizada com mais frequência. Todos os nós de storage recebem um valor mínimo de peso básico, mesmo que um nó informe a utilização de 100% ou não consiga relatar sua utilização.

Em alguns casos, as informações sobre a disponibilidade da CPU estão limitadas ao local onde o serviço Load Balancer está localizado.

Configurar pontos de extremidade do balanceador de carga

Os pontos de extremidade do balanceador de carga determinam as portas e os protocolos de rede que os clientes S3 podem usar ao se conetar ao balanceador de carga StorageGRID nos nós de gateway e administrador. Você também pode usar endpoints para acessar o Gerenciador de Grade, o Gerenciador de Tenant ou ambos.

Os detalhes do Swift foram removidos desta versão do site do doc. "Configurar conexões de cliente S3 e Swift"Consulte .

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Você revisou o "considerações para balanceamento de carga".
- Se você remapeou anteriormente uma porta que pretende usar para o ponto de extremidade do balanceador de carga, você tem "removido o remapeamento da porta"o .

- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Os GRUPOS HA são recomendados, mas não são necessários. "Gerenciar grupos de alta disponibilidade"Consulte .
- Se o ponto final do balanceador de carga for usado "S3 inquilinos para S3 Select"pelo , ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente dispositivos de serviços e nós de software baseados em VMware são permitidos para os pontos de extremidade do balanceador de carga usados para o S3 Select.
- Você configurou todas as interfaces VLAN que planeja usar. "Configurar interfaces VLAN"Consulte .
- Se você estiver criando um endpoint HTTPS (recomendado), você terá as informações para o certificado do servidor.

> As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

  - Para carregar um certificado, você precisa do certificado do servidor, da chave privada do certificado e, opcionalmente, de um pacote de CA.
  - Para gerar um certificado, você precisa de todos os nomes de domínio e endereços IP que os clientes S3 usarão para acessar o endpoint. Você também deve conhecer o assunto (Nome distinto).
  - Se você quiser usar o certificado de API do StorageGRID S3 (que também pode ser usado para conexões diretamente aos nós de storage), você já substituiu o certificado padrão por um certificado personalizado assinado por uma autoridade de certificação externa. "Configure os certificados API do S3"Consulte .

Crie um ponto de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga do cliente S3 especifica uma porta, um tipo de cliente (S3) e um protocolo de rede (HTTP ou HTTPS). Os pontos de extremidade do balanceador de carga da interface de gerenciamento especificam uma porta, tipo de interface e rede cliente não confiável.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Network** > **Load balancer endpoints**.
2. Para criar um endpoint para um cliente S3 ou Swift, selecione a guia **S3 ou Swift client**.
3. Para criar um endpoint para acesso ao Gerenciador de Grade, Gerenciador de Tenant ou ambos, selecione a guia **Interface de Gerenciamento**.
4. Selecione **criar**.

Introduza os detalhes do endpoint

Passos

1. Selecione as instruções apropriadas para inserir detalhes do tipo de endpoint que você deseja criar.

Cliente S3 ou Swift

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página pontos de extremidade do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo é padrão para 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada de 1 a 65535. Se você digitar **80** ou **8443**, o endpoint será configurado somente em nós de Gateway, a menos que você tenha liberado a porta 8443. Em seguida, você pode usar a porta 8443 como um endpoint S3 e a porta será configurada nos nós Gateway e Admin.
Tipo de cliente	O tipo de aplicativo cliente que usará esse endpoint, **S3** ou **Swift**.
Protocolo de rede	O protocolo de rede que os clientes utilizarão ao ligar a este ponto final. • Selecione **HTTPS** para comunicação segura e criptografada TLS (recomendada). Você deve anexar um certificado de segurança antes de salvar o endpoint. • Selecione **HTTP** para comunicação menos segura e não criptografada. Use HTTP apenas para uma grade não-produção.

Interface de gerenciamento

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página pontos de extremidade do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para acessar o Gerenciador de Grade, o Gerenciador do Locatário ou ambos. • Grid Manager: **8443** • Gerente de inquilino: **9443** • Gerente de Grade e Gerente de Locatário: **443** **Nota**: Você pode usar essas portas predefinidas ou outras portas disponíveis.
Tipo de interface	Selecione o botão de opção para a interface do StorageGRID que você acessará usando este endpoint.

Campo	Descrição
Rede cliente não confiável	Selecione **Sim** se este endpoint estiver acessível a redes de clientes não confiáveis. Caso contrário, selecione **não**. Quando você seleciona **Sim**, a porta é aberta em todas as redes de clientes não confiáveis. **Observação**: Você só pode configurar uma porta para ser aberta ou fechada para redes de clientes não confiáveis quando estiver criando o endpoint do balanceador de carga.

1. Selecione **continuar**.

Selecione um modo de encadernação

Passos

1. Selecione um modo de encadernação para o endpoint controlar como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP específicos e interfaces de rede.

   Alguns modos de vinculação estão disponíveis para endpoints de cliente ou endpoints de interface de gerenciamento. Todos os modos para ambos os tipos de endpoint estão listados aqui.

Modo	Descrição
Global (padrão para endpoints do cliente)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global**, a menos que você precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos de HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo de HA para acessar esse endpoint. Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nós	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar esse endpoint.
Tipo de nó (somente endpoints do cliente)	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway para acessar esse ponto final.

Modo	Descrição
Todos os nós de administração (padrão para endpoints de interface de gerenciamento)	Os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin para acessar esse endpoint.

Se mais de um ponto de extremidade utilizar a mesma porta, o StorageGRID utiliza esta ordem de prioridade para decidir qual ponto de extremidade utilizar: **IPs virtuais de grupos de HA** > **interfaces de nó** > **tipo de nó** > **Global**.

Se você estiver criando endpoints de interface de gerenciamento, somente os nós de administrador serão permitidos.

2. Se você selecionou **IPs virtuais de grupos de HA**, selecione um ou mais grupos de HA.

   Se estiver a criar endpoints de interface de gestão, selecione VIPs associados apenas a nós de administração.

3. Se você selecionou **interfaces de nó**, selecione uma ou mais interfaces de nó para cada nó de administrador ou nó de gateway que você deseja associar a esse ponto de extremidade.
4. Se você selecionou **tipo de nó**, selecione os nós de administrador, que incluem o nó de administrador principal e quaisquer nós de administrador não primários ou nós de gateway.

Controle o acesso do locatário

Um endpoint de interface de gerenciamento pode controlar o acesso do locatário somente quando o endpoint tiver o Tipo de interface do Gerenciador de inquilinos.

Passos

1. Para a etapa **Acesso ao locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de inquilino podem usar esse endpoint para acessar seus buckets. Você deve selecionar essa opção se ainda não tiver criado nenhuma conta de locatário. Depois de adicionar contas de locatário, você pode editar o endpoint do balanceador de carga para permitir ou bloquear contas específicas.
Permitir inquilinos selecionados	Somente as contas de locatário selecionadas podem usar esse endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar esse endpoint para acessar seus buckets. Todos os outros inquilinos podem usar este endpoint.

2. Se você estiver criando um endpoint **HTTP**, não será necessário anexar um certificado. Selecione **Create**

para adicionar o novo ponto de extremidade do balanceador de carga. Em seguida, vá Depois de terminarpara . Caso contrário, selecione **continuar** para anexar o certificado.

Anexar certificado

Passos

1. Se você estiver criando um endpoint **HTTPS**, selecione o tipo de certificado de segurança que deseja anexar ao endpoint.

   O certificado protege as conexões entre clientes S3 e o serviço Load Balancer no nó Admin ou nos nós Gateway.

   - * Carregar certificado*. Selecione esta opção se tiver certificados personalizados para carregar.
   - **Gerar certificado**. Selecione esta opção se tiver os valores necessários para gerar um certificado personalizado.
   - **Use o certificado StorageGRID S3**. Selecione essa opção se quiser usar o certificado global da API S3, que também pode ser usado para conexões diretamente aos nós de storage.

     Não é possível selecionar essa opção a menos que você tenha substituído o certificado padrão da API S3, que é assinado pela CA de grade, por um certificado personalizado assinado por uma autoridade de certificação externa. "Configure os certificados API do S3"Consulte .

   - **Use o certificado de interface de gerenciamento**. Selecione esta opção se pretender utilizar o certificado de interface de gestão global, que também pode ser utilizado para ligações diretas a nós de administração.
2. Se não estiver a utilizar o certificado StorageGRID S3, carregue ou gere o certificado.

Carregar certificado

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado do servidor**: O arquivo de certificado do servidor personalizado na codificação PEM.
- **Chave privada de certificado**: O arquivo de chave privada de certificado de servidor personalizado (`.key`).

> As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA**: Um único arquivo opcional contendo 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.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **criar**. O ponto de extremidade do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 ou a interface de gerenciamento e o endpoint.

Gerar certificado

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a incluir no certificado.
Assunto (opcional)	X,509 Assunto ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).

Campo	Descrição
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **criar**.

O ponto final do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 ou a interface de gerenciamento e este endpoint.

Depois de terminar

Passos

1. Se você usar um DNS, verifique se o DNS inclui um Registro para associar o nome de domínio totalmente qualificado (FQDN) do StorageGRID a cada endereço IP que os clientes usarão para fazer conexões.

   O endereço IP inserido no Registro DNS depende se você está usando um grupo HA de nós de balanceamento de carga:

   - Se você tiver configurado um grupo HA, os clientes se conetarão aos endereços IP virtuais desse grupo HA.
   - Se você não estiver usando um grupo de HA, os clientes se conetarão ao serviço do StorageGRID Load Balancer usando o endereço IP de um nó de gateway ou nó de administrador.

     Você também deve garantir que o Registro DNS faça referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes de curinga.

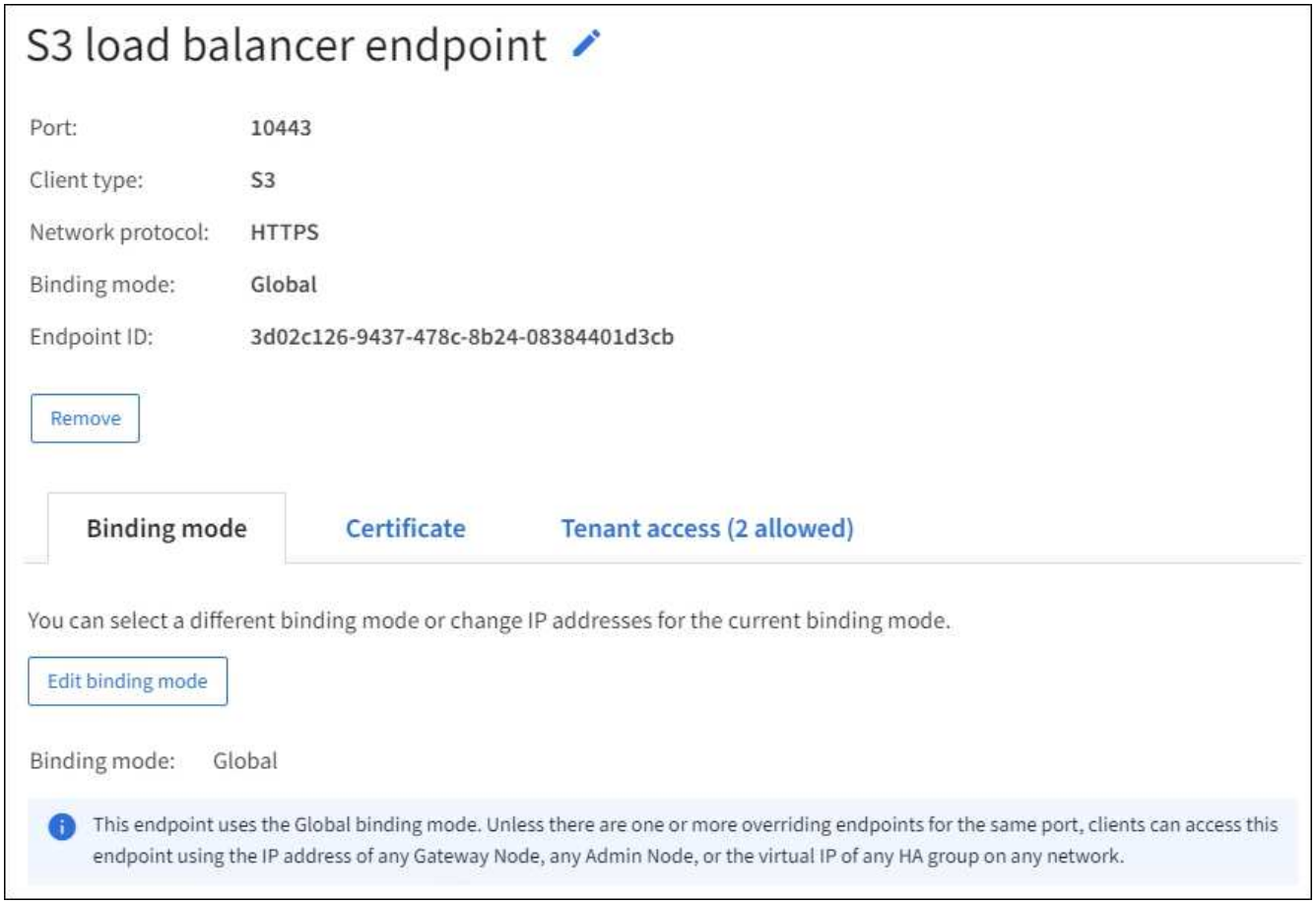
2. Forneça aos clientes S3 as informações necessárias para se conetar ao endpoint:

- Número da porta
- Nome de domínio ou endereço IP totalmente qualificado
- Todos os detalhes necessários do certificado

Visualize e edite pontos de extremidade do balanceador de carga

Você pode exibir detalhes dos endpoints existentes do balanceador de carga, incluindo os metadados do certificado para um endpoint seguro. Você pode alterar certas configurações para um endpoint.

- Para exibir informações básicas de todos os pontos de extremidade do balanceador de carga, revise as tabelas na página pontos de extremidade do balanceador de carga.
- Para exibir todos os detalhes sobre um endpoint específico, incluindo metadados de certificado, selecione o nome do endpoint na tabela. As informações apresentadas variam consoante o tipo de ponto de extremidade e a forma como são configuradas.



- Para editar um endpoint, use o menu **ações** na página pontos de extremidade do balanceador de carga.

> Se você perder o acesso ao Gerenciador de Grade ao editar a porta de um endpoint de interface de gerenciamento, atualize o URL e a porta para recuperar o acesso.

> Depois de editar um endpoint, você pode precisar esperar até 15 minutos para que suas alterações sejam aplicadas a todos os nós.

Tarefa	Menu ações	Página de detalhes
Edite o nome do endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar nome do endpoint**. c. Introduza o novo nome. d. Selecione **Guardar**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione o ícone de edição . c. Introduza o novo nome. d. Selecione **Guardar**.
Editar porta de endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar porta de endpoint** c. Introduza um número de porta válido. d. Selecione **Guardar**.	*n/a*
Editar o modo de encadernação de endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **actions** > **Edit endpoint binding mode** c. Atualize o modo de encadernação conforme necessário. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione **Editar modo de encadernação**. c. Atualize o modo de encadernação conforme necessário. d. Selecione **Salvar alterações**.
Editar certificado de endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar certificado de endpoint**. c. Carregue ou gere um novo certificado personalizado ou comece a utilizar o certificado global S3, conforme necessário. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia **certificado**. c. Selecione **Editar certificado**. d. Carregue ou gere um novo certificado personalizado ou comece a utilizar o certificado global S3, conforme necessário. e. Selecione **Salvar alterações**.
Editar acesso ao locatário	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar acesso ao locatário**. c. Escolha uma opção de acesso diferente, selecione ou remova locatários da lista ou faça ambos. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia **Acesso ao locatário**. c. Selecione **Editar acesso ao locatário**. d. Escolha uma opção de acesso diferente, selecione ou remova locatários da lista ou faça ambos. e. Selecione **Salvar alterações**.

Remova os pontos finais do balanceador de carga

Você pode remover um ou mais endpoints usando o menu **ações** ou remover um único endpoint da página de detalhes.

> Para evitar interrupções do cliente, atualize os aplicativos de cliente S3 afetados antes de remover um endpoint de balanceador de carga. Atualize cada cliente para se conetar usando uma porta atribuída a outro ponto de extremidade do balanceador de carga. Certifique-se de atualizar todas as informações de certificado necessárias também.

> Se você perder o acesso ao Gerenciador de Grade ao remover um endpoint de interface de gerenciamento, atualize o URL.

- Para remover um ou mais pontos finais:
  a. Na página Load balancer, marque a caixa de seleção para cada ponto final que deseja remover.
  b. Selecione **ações** > **Remover**.
  c. Selecione **OK**.
- Para remover um endpoint da página de detalhes:
  a. Na página Load balancer. Selecione o nome do endpoint.
  b. Selecione **Remover** na página de detalhes.
  c. Selecione **OK**.

Configurar nomes de domínio de endpoint S3

Para oferecer suporte a S3 solicitações de estilo hospedado virtual, você deve usar o Gerenciador de Grade para configurar a lista de S3 nomes de domínio de endpoint aos quais os clientes S3 se conetam.

> O uso de um endereço IP para um nome de domínio de endpoint não é suportado. Versões futuras impedirão essa configuração.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você confirmou que uma atualização de grade não está em andamento.

> Não faça alterações na configuração do nome de domínio quando uma atualização de grade estiver em andamento.

Sobre esta tarefa

Para permitir que os clientes usem nomes de domínio de endpoint S3, você deve fazer todas as seguintes ações:

- Use o Gerenciador de Grade para adicionar os nomes de domínio de endpoint S3 ao sistema StorageGRID.
- Certifique-se de que o "Certificado que o cliente usa para conexões HTTPS com o StorageGRID" está

assinado para todos os nomes de domínio que o cliente requer.

Por exemplo, se o endpoint for `s3.company.com`, você deve garantir que o certificado usado para conexões HTTPS inclua o `s3.company.com` endpoint e o nome alternativo do assunto universal (SAN) do endpoint: `*.s3.company.com`.

- Configure o servidor DNS usado pelo cliente. Inclua Registros DNS para os endereços IP que os clientes usam para fazer conexões e verifique se os Registros fazem referência a todos os nomes de domínio de endpoint S3 necessários, incluindo quaisquer nomes de curinga.

> Os clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de gateway, um nó de administrador ou um nó de armazenamento, ou conetando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos cliente se conetam à grade para incluir os endereços IP corretos nos Registros DNS.

Os clientes que usam conexões HTTPS (recomendadas) para a grade podem usar qualquer um destes certificados:

- Os clientes que se conetam a um ponto de extremidade do balanceador de carga podem usar um certificado personalizado para esse ponto de extremidade. Cada ponto de extremidade do balanceador de carga pode ser configurado para reconhecer diferentes nomes de domínio de endpoint S3.
- Os clientes que se conetam a um ponto de extremidade do balanceador de carga ou diretamente a um nó de armazenamento podem personalizar o certificado global da API S3 para incluir todos os nomes de domínio de endpoint S3 necessários.

> Se você não adicionar nomes de domínio de endpoint S3 e a lista estiver vazia, o suporte para solicitações de estilo hospedado virtual S3 será desativado.

Adicione um nome de domínio de endpoint S3

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.
2. Introduza o nome de domínio no campo **Domain Name 1**. Selecione **Adicionar outro nome de domínio** para adicionar mais nomes de domínio.
3. Selecione **Guardar**.
4. Certifique-se de que os certificados de servidor que os clientes utilizam correspondem aos nomes de domínio de endpoint S3 necessários.
   - Se os clientes se conetarem a um ponto de extremidade do balanceador de carga que use seu próprio certificado"atualize o certificado associado ao endpoint", .
   - Se os clientes se conetarem a um ponto de extremidade do balanceador de carga que use o certificado global da API S3 ou diretamente aos nós de storage, "Atualize o certificado global da API S3".
5. Adicione os Registros DNS necessários para garantir que as solicitações de nome de domínio de endpoint possam ser resolvidas.

Resultado

Agora, quando os clientes usam o endpoint *`bucket.s3.company.com`*, o servidor DNS resolve para o endpoint correto e o certificado autentica o endpoint como esperado.

Renomeie um nome de domínio de endpoint S3

Se você alterar um nome usado por aplicativos S3, as solicitações de estilo hospedado virtual falharão.

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.
2. Selecione o campo de nome de domínio que deseja editar e faça as alterações necessárias.
3. Selecione **Guardar**.
4. Selecione **Sim** para confirmar a alteração.

Exclua um nome de domínio de endpoint S3

Se você remover um nome usado por aplicativos S3, as solicitações de estilo hospedado virtual falharão.

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.
2. Selecione o ícone de exclusão ✕ ao lado do nome de domínio.
3. Selecione **Sim** para confirmar a exclusão.

Informações relacionadas

- "USE A API REST DO S3"
- "Ver endereços IP"
- "Configurar grupos de alta disponibilidade"

Resumo: Endereços IP e portas para conexões de clientes

Para armazenar ou recuperar objetos, os aplicativos cliente S3 se conetam ao serviço Load Balancer, que está incluído em todos os nós de administração e nós de gateway, ou ao serviço LDR (roteador de distribuição local), que está incluído em todos os nós de armazenamento.

Os aplicativos clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de grade e o número da porta do serviço nesse nó. Como opção, você pode criar grupos de alta disponibilidade (HA) de nós de balanceamento de carga para fornecer conexões altamente disponíveis que usam endereços IP virtual (VIP). Se você quiser se conetar ao StorageGRID usando um nome de domínio totalmente qualificado (FQDN) em vez de um endereço IP ou VIP, você pode configurar entradas de DNS.

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conetar ao StorageGRID e os endereços IP e as portas usadas para cada tipo de conexão. Se você já criou endpoints do balanceador de carga e grupos de alta disponibilidade (HA), consulte Onde encontrar endereços IP para localizar esses valores no Gerenciador de Grade.

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	Porta atribuída ao ponto de extremidade do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084

Exemplos de URLs

Para conetar um aplicativo cliente ao ponto de extremidade do Load Balancer de um grupo de HA de nós de Gateway, use um URL estruturado como mostrado abaixo:

`https://VIP-of-HA-group:LB-endpoint-port`

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.5 e o número da porta do endpoint do balanceador de carga for 10443, um aplicativo poderá usar o seguinte URL para se conetar ao StorageGRID:

`https://192.0.2.5:10443`

Onde encontrar endereços IP

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Para localizar o endereço IP de um nó de grade:
   a. Selecione **NODES**.
   b. Selecione o nó de administração, nó de gateway ou nó de armazenamento ao qual deseja se conetar.
   c. Selecione a guia **Visão geral**.
   d. Na seção informações do nó, observe os endereços IP do nó.
   e. Selecione **Mostrar mais** para visualizar endereços IPv6 e mapeamentos de interface.

      Você pode estabelecer conexões de aplicativos cliente para qualquer um dos endereços IP na lista:

      - **eth0:** rede de Grade
      - **eth1:** Admin Network (opcional)
      - **eth2:** rede de clientes (opcional)

      > Se você estiver exibindo um nó de administrador ou um nó de gateway e for o nó ativo em um grupo de alta disponibilidade, o endereço IP virtual do grupo de HA será exibido em eth2.

3. Para localizar o endereço IP virtual de um grupo de alta disponibilidade:
   a. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
   b. Na tabela, anote o endereço IP virtual do grupo HA.
4. Para localizar o número da porta de um endpoint do Load Balancer:
   a. Selecione **CONFIGURATION** > **Network** > **Load balancer endpoints**.
   b. Observe o número da porta do endpoint que você deseja usar.

   > Se o número da porta for 80 ou 443, o endpoint será configurado apenas em nós de Gateway, porque essas portas estão reservadas em nós de administração. Todas as outras portas são configuradas nos nós de Gateway e nos de Admin.

   c. Selecione o nome do endpoint na tabela.
   d. Confirme se o **Client type** (S3) corresponde ao aplicativo cliente que usará o endpoint.

Gerencie redes e conexões

Configure as definições de rede

Você pode configurar várias configurações de rede do Gerenciador de Grade para ajustar a operação do sistema StorageGRID.

Configurar interfaces VLAN

Você pode "Crie interfaces de LAN virtual (VLAN)"isolar e particionar o tráfego para segurança, flexibilidade e desempenho. Cada interface VLAN está associada a uma ou mais interfaces pai em nós de administração e nós de gateway. Você pode usar interfaces VLAN em grupos de HA e em endpoints do balanceador de carga para segregar o tráfego de cliente ou administrador por aplicativo ou locatário.

Políticas de classificação de tráfego

Você pode usar "políticas de classificação de tráfego" para identificar e gerenciar diferentes tipos de tráfego de rede, incluindo tráfego relacionado a buckets específicos, locatários, sub-redes de clientes ou pontos de extremidade do balanceador de carga. Essas políticas podem ajudar na limitação e monitoramento de tráfego.

Diretrizes para redes StorageGRID

Você pode usar o Gerenciador de Grade para configurar e gerenciar redes e conexões StorageGRID.

"Configurar conexões de cliente S3"Consulte para saber como conetar clientes S3.

Redes StorageGRID predefinidas

Por padrão, o StorageGRID oferece suporte a três interfaces de rede por nó de grade, permitindo que você configure a rede para cada nó de grade individual de acordo com seus requisitos de segurança e acesso.

Para obter mais informações sobre a topologia de rede, "Diretrizes de rede"consulte .

Rede de rede

Obrigatório. A rede de grade é usada para todo o tráfego interno do StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes.

Rede de administração

Opcional. A rede de administração é normalmente utilizada para administração e manutenção do sistema. Ele também pode ser usado para acesso ao protocolo cliente. A rede Admin é normalmente uma rede privada e não precisa ser roteável entre sites.

Rede de clientes

Opcional. A rede de clientes é uma rede aberta normalmente usada para fornecer acesso a aplicativos clientes S3, de modo que a rede de Grade pode ser isolada e protegida. A rede do cliente pode se comunicar com qualquer sub-rede acessível através do gateway local.

Diretrizes

- Cada nó StorageGRID requer uma interface de rede dedicada, endereço IP, máscara de sub-rede e gateway para cada rede à qual está atribuído.
- Um nó de grade não pode ter mais de uma interface em uma rede.
- Um único gateway, por rede, por nó de grade é suportado e deve estar na mesma sub-rede que o nó. Você pode implementar roteamento mais complexo no gateway, se necessário.
- Em cada nó, cada rede mapeia para uma interface de rede específica.

Rede	Nome da interface
Grelha	eth0
Admin (opcional)	eth1
Cliente (opcional)	eth2

- Se o nó estiver conetado a um dispositivo StorageGRID, portas específicas serão usadas para cada rede. Para obter mais detalhes, consulte as instruções de instalação do seu aparelho.
- A rota padrão é gerada automaticamente, por nó. Se o eth2 estiver ativado, o 0,0.0.0/0 usará a rede do cliente no eth2. Se o eth2 não estiver ativado, o 0,0.0.0/0 usará a rede de Grade no eth0.
- A rede do cliente não se torna operacional até que o nó da grade se junte à grade
- A rede Admin pode ser configurada durante a implantação do nó de grade para permitir o acesso à interface do usuário de instalação antes que a grade esteja totalmente instalada.

Interfaces opcionais

Opcionalmente, você pode adicionar interfaces extras a um nó. Por exemplo, você pode querer adicionar uma interface de tronco a um nó Admin ou Gateway, para que você possa usar "Interfaces VLAN" para segregar o tráfego pertencente a diferentes aplicativos ou locatários. Ou, talvez você queira adicionar uma interface de acesso a ser usada em um "Grupo de alta disponibilidade (HA)".

Para adicionar interfaces de tronco ou acesso, consulte o seguinte:

- **VMware (após a instalação do nó)**: "VMware: Adicione interfaces de tronco ou acesso a um nó"
  - **Red Hat Enterprise Linux (antes de instalar o nó)**: "Criar arquivos de configuração de nó"
  - * Ubuntu ou Debian (antes de instalar o nó)*: "Criar arquivos de configuração de nó"
  - **RHEL, Ubuntu ou Debian (após instalar o nó)**: "Linux: Adicione interfaces de tronco ou acesso a um nó"

Ver endereços IP

Você pode exibir o endereço IP de cada nó de grade em seu sistema StorageGRID. Em seguida, você pode usar esse endereço IP para fazer login no nó da grade na linha de comando e executar vários procedimentos de manutenção.

Antes de começar

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

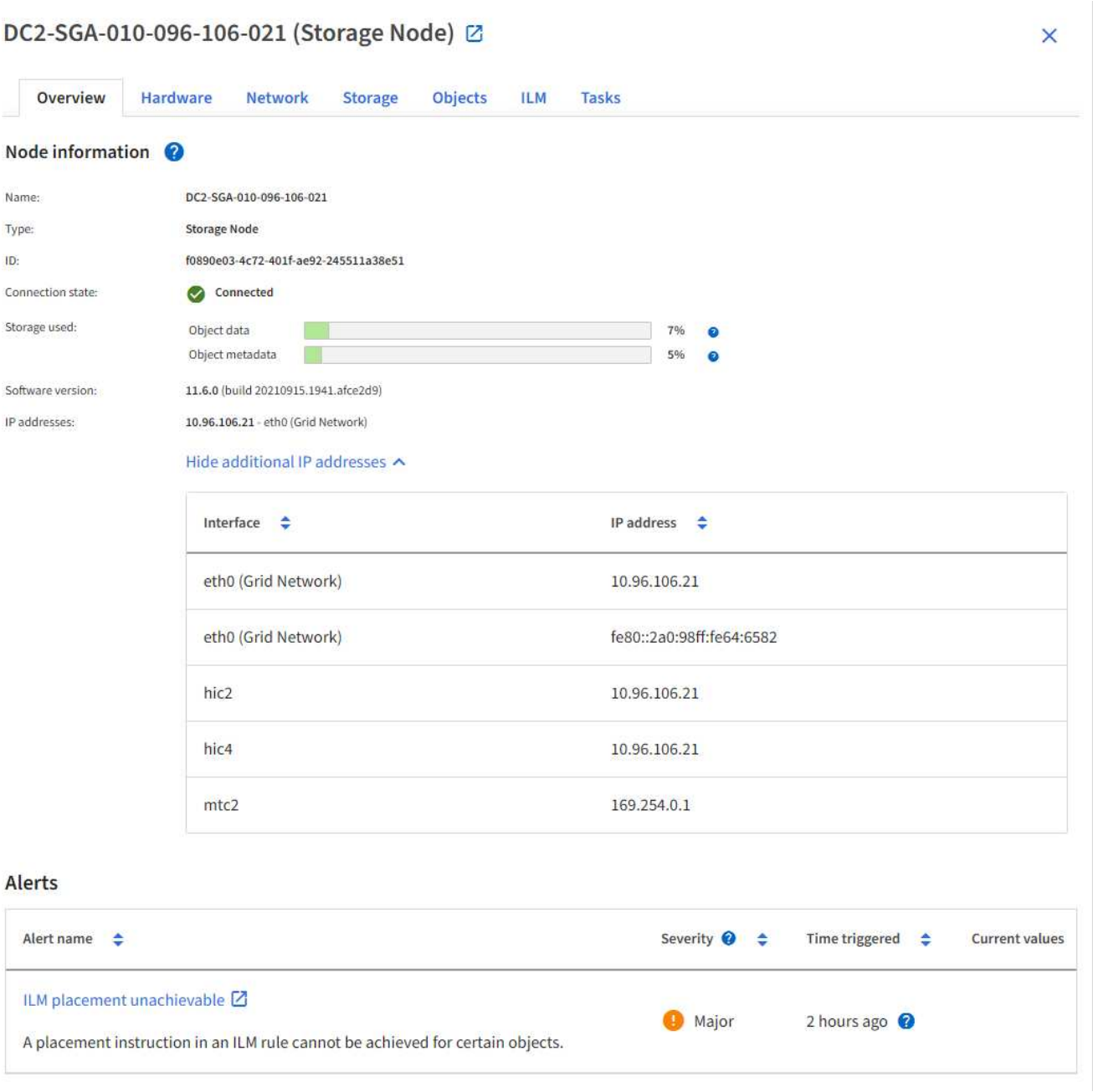
Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, "Configurar endereços IP"consulte .

Passos

1. Selecione **NODES** > ***grid node*** > **Visão geral**.
2. Selecione **Mostrar mais** à direita do título dos endereços IP.

   Os endereços IP desse nó de grade são listados em uma tabela.



Configurar interfaces VLAN

Você pode criar interfaces de LAN virtual (VLAN) em nós de administração e nós de gateway e usá-las em grupos de HA e pontos de extremidade do balanceador de carga para isolar e particionar o tráfego para obter segurança, flexibilidade e desempenho.

Considerações para interfaces VLAN

- Você cria uma interface VLAN inserindo um ID de VLAN e escolhendo uma interface pai em um ou mais nós.
- Uma interface pai deve ser configurada como uma interface de tronco no switch.
- Uma interface pai pode ser a rede de Grade (eth0), a rede de Cliente (eth2) ou uma interface de tronco adicional para a VM ou host bare-metal (por exemplo, ens256).

- Para cada interface VLAN, você pode selecionar apenas uma interface pai para um determinado nó. Por exemplo, você não pode usar a interface de rede de Grade e a interface de rede de cliente no mesmo nó de gateway que a interface pai para a mesma VLAN.
- Se a interface VLAN for para tráfego Admin Node, que inclui tráfego relacionado ao Grid Manager e ao Tenant Manager, selecione interfaces somente em Admin Nodes.
- Se a interface VLAN for para tráfego de cliente S3, selecione interfaces em nós de administração ou nós de gateway.
- Se você precisar adicionar interfaces de tronco, consulte o seguinte para obter detalhes:
  - **VMware (após a instalação do nó)**: "VMware: Adicione interfaces de tronco ou acesso a um nó"
  - **RHEL (antes de instalar o nó)**: "Criar arquivos de configuração de nó"
  - * Ubuntu ou Debian (antes de instalar o nó)*: "Criar arquivos de configuração de nó"
  - **RHEL, Ubuntu ou Debian (após instalar o nó)**: "Linux: Adicione interfaces de tronco ou acesso a um nó"

Crie uma interface VLAN

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Uma interface de tronco foi configurada na rede e conetada ao nó VM ou Linux. Você sabe o nome da interface do tronco.
- Você sabe o ID da VLAN que está configurando.

Sobre esta tarefa

O administrador da rede pode ter configurado uma ou mais interfaces de tronco e uma ou mais VLANs para segregar o tráfego de cliente ou administrador pertencente a diferentes aplicativos ou locatários. Cada VLAN é identificada por um ID numérico ou tag. Por exemplo, sua rede pode usar VLAN 100 para tráfego FabricPool e VLAN 200 para um aplicativo de arquivamento.

Você pode usar o Gerenciador de Grade para criar interfaces de VLAN que permitem que os clientes acessem o StorageGRID em uma VLAN específica. Ao criar interfaces VLAN, você especifica a ID da VLAN e seleciona interfaces pai (tronco) em um ou mais nós.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Selecione **criar**.

Insira os detalhes das interfaces VLAN

Passos

1. Especifique o ID da VLAN na rede. Pode introduzir qualquer valor entre 1 e 4094.

   Os IDs de VLAN não precisam ser exclusivos. Por exemplo, você pode usar VLAN ID 200 para tráfego de administrador em um local e o mesmo VLAN ID para tráfego de cliente em outro local. Você pode criar interfaces VLAN separadas com diferentes conjuntos de interfaces pai em cada local. No entanto, duas interfaces VLAN com o mesmo ID não podem compartilhar a mesma interface em um nó. Se você

especificar uma ID que já foi usada, uma mensagem será exibida.

2. Opcionalmente, insira uma breve descrição para a interface VLAN.
3. Selecione **continuar**.

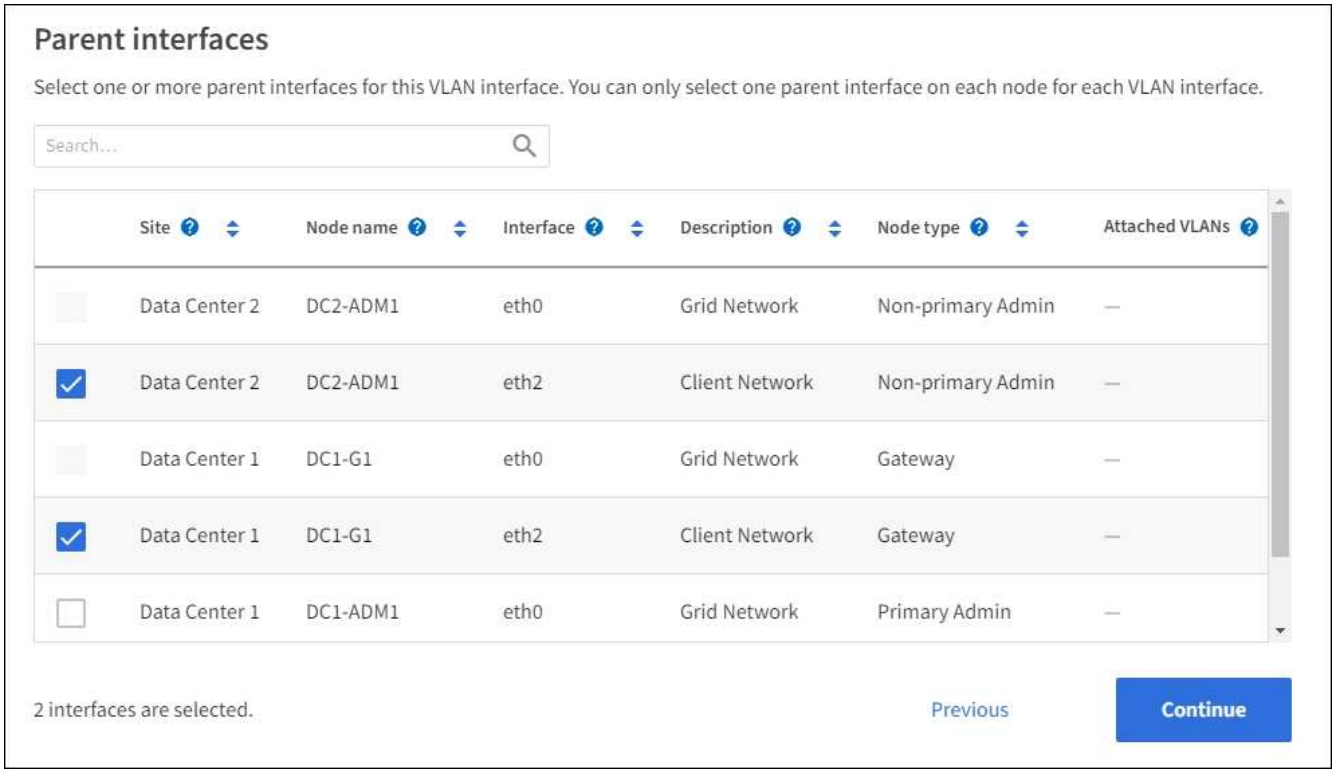
Escolha interfaces pai

A tabela lista as interfaces disponíveis para todos os nós de administração e nós de gateway em cada local da grade. As interfaces Admin Network (eth1) não podem ser usadas como interfaces pai e não são mostradas.

Passos

1. Selecione uma ou mais interfaces pai às quais anexar esta VLAN.

   Por exemplo, você pode querer anexar uma VLAN à interface de rede de cliente (eth2) para um nó de gateway e um nó de administrador.



2. Selecione **continuar**.

Confirme as definições

Passos

1. Revise a configuração e faça quaisquer alterações.
   - Se você precisar alterar a ID ou a descrição da VLAN, selecione **Digite os detalhes da VLAN** na parte superior da página.
   - Se você precisar alterar uma interface pai, selecione **escolha interfaces pai** na parte superior da página ou selecione **anterior**.
   - Se for necessário remover uma interface pai, selecione a lixeira .
2. Selecione **Guardar**.

3. Aguarde até 5 minutos para que a nova interface apareça como uma seleção na página grupos de alta disponibilidade e seja listada na tabela **interfaces de rede** para o nó (**NODES** > ***parent interface node*** > **Network**).

Editar uma interface VLAN

Ao editar uma interface VLAN, você pode fazer os seguintes tipos de alterações:

- Altere a ID ou a descrição da VLAN.
- Adicionar ou remover interfaces pai.

Por exemplo, você pode querer remover uma interface pai de uma interface VLAN se você planeja desativar o nó associado.

Observe o seguinte:

- Não é possível alterar um ID de VLAN se a interface de VLAN for usada em um grupo HA.
- Não é possível remover uma interface pai se essa interface pai for usada em um grupo HA.

  Por exemplo, suponha que a VLAN 200 esteja conetada às interfaces pai nos nós A e B. se um grupo de HA usar a interface VLAN 200 para o nó A e a interface eth2 para o nó B, você poderá remover a interface pai não utilizada para o nó B, mas não poderá remover a interface pai usada para o nó A.

Passos

1. Selecione **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Marque a caixa de seleção para a interface VLAN que deseja editar. Em seguida, selecione **ações** > **Editar**.
3. Opcionalmente, atualize o ID da VLAN ou a descrição. Em seguida, selecione **continuar**.

   Não é possível atualizar um ID de VLAN se a VLAN for usada em um grupo HA.

4. Opcionalmente, marque ou desmarque as caixas de seleção para adicionar interfaces pai ou remover interfaces não utilizadas. Em seguida, selecione **continuar**.
5. Revise a configuração e faça quaisquer alterações.
6. Selecione **Guardar**.

Remova uma interface VLAN

Você pode remover uma ou mais interfaces VLAN.

Não é possível remover uma interface VLAN se ela for usada atualmente em um grupo HA. Você deve remover a interface VLAN do grupo HA antes de removê-la.

Para evitar quaisquer interrupções no tráfego do cliente, considere fazer um dos seguintes procedimentos:

- Adicione uma nova interface VLAN ao grupo HA antes de remover essa interface VLAN.
- Crie um novo grupo HA que não use essa interface VLAN.
- Se a interface VLAN que você deseja remover for atualmente a interface ativa, edite o grupo HA. Mova a interface VLAN que você deseja remover para a parte inferior da lista de prioridades. Aguarde até que a comunicação seja estabelecida na nova interface primária e remova a interface antiga do grupo HA. Finalmente, exclua a interface VLAN nesse nó.

Passos

1. Selecione **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Marque a caixa de seleção para cada interface VLAN que você deseja remover. Em seguida, selecione **ações** > **Excluir**.
3. Selecione **Sim** para confirmar a sua seleção.

   Todas as interfaces VLAN selecionadas são removidas. Um banner verde de sucesso aparece na página interfaces VLAN.

Gerenciar políticas de classificação de tráfego

O que são políticas de classificação de tráfego?

As políticas de classificação de tráfego permitem identificar e monitorar diferentes tipos de tráfego de rede. Essas políticas podem ajudar com a limitação de tráfego e o monitoramento para aprimorar suas ofertas de qualidade do serviço (QoS).

As políticas de classificação de tráfego são aplicadas a pontos de extremidade no serviço de balanceador de carga do StorageGRID para nós de gateway e nós de administração. Para criar políticas de classificação de tráfego, você já deve ter criado pontos de extremidade do balanceador de carga.

Regras correspondentes

Cada política de classificação de tráfego contém uma ou mais regras correspondentes para identificar o tráfego de rede relacionado a uma ou mais das seguintes entidades:

- Baldes
- Sub-rede
- Locatário
- Pontos de extremidade do balanceador de carga

O StorageGRID monitora o tráfego que corresponde a qualquer regra dentro da política de acordo com os objetivos da regra. Qualquer tráfego que corresponda a qualquer regra de uma política é Tratado por essa política. Por outro lado, você pode definir regras para corresponder a todo o tráfego, exceto uma entidade especificada.

Limitação de tráfego

Opcionalmente, você pode adicionar os seguintes tipos de limite a uma política:

- Largura de banda de agregado
- Largura de banda por solicitação
- Solicitações simultâneas
- Taxa de solicitação

Os valores-limite são impostos por balanceador de carga. Se o tráfego for distribuído simultaneamente em vários balanceadores de carga, as taxas máximas totais são vários dos limites de taxa especificados.

Você pode criar políticas para limitar a largura de banda agregada ou limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Os limites de largura de banda agregada podem impor um impactos menor no desempenho adicional no tráfego não limitado.

Para limites de largura de banda agregada ou por solicitação, as solicitações são transmitidas ou enviadas pela taxa definida. O StorageGRID só pode impor uma velocidade, então a correspondência de política mais específica, por tipo matcher, é a aplicada. A largura de banda consumida pela solicitação não conta com outras políticas de correspondência menos específicas que contenham políticas de limite de largura de banda agregada. Para todos os outros tipos de limite, as solicitações do cliente são atrasadas em 250 milissegundos e recebem uma resposta de retardo 503 para solicitações que excedem qualquer limite de política correspondente.

No Gerenciador de Grade, você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

Use políticas de classificação de tráfego com SLAs

Você pode usar políticas de classificação de tráfego em conjunto com limites de capacidade e proteção de dados para aplicar acordos de nível de serviço (SLAs) que fornecem detalhes sobre capacidade, proteção de dados e desempenho.

O exemplo a seguir mostra três níveis de um SLA. Você pode criar políticas de classificação de tráfego para alcançar os objetivos de desempenho de cada nível de SLA.

Nível de serviço	Capacidade	Proteção de dados	Desempenho máximo permitido	Custo
Ouro	1 PB de armazenamento permitido	3 copiar regra ILM	25 K solicitações/seg Largura de banda de 5 GB/seg (40 Gbps)	dólares por mês
Prata	250 TB de armazenamento permitido	2 copiar regra ILM	10 K solicitações/seg Largura de banda de 1,25 GB/seg (10 Gbps)	dólares por mês
Bronze	100 TB de armazenamento permitido	2 copiar regra ILM	5 K solicitações/seg Largura de banda de 1 GB/seg (8 Gbps)	dólares por mês

Crie políticas de classificação de tráfego

Você pode criar políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por bucket, regex de bucket, CIDR, endpoint do

balanceador de carga ou locatário. Opcionalmente, você pode definir limites para uma política com base na largura de banda, no número de solicitações simultâneas ou na taxa de solicitações.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Você criou todos os pontos de extremidade do balanceador de carga que deseja corresponder.
- Você criou quaisquer inquilinos que você deseja combinar.

Passos

1. Selecione **CONFIGURATION** > **Network** > **Traffic Classification**.
2. Selecione **criar**.
3. Introduza um nome e uma descrição (opcional) para a política e selecione **continuar**.

   Por exemplo, descreva ao que esta política de classificação de tráfego se aplica e ao que ela limitará.

4. Selecione **Adicionar regra** e especifique os seguintes detalhes para criar uma ou mais regras correspondentes para a política. Qualquer política que você criar deve ter pelo menos uma regra correspondente. Selecione **continuar**.

Campo	Descrição
Tipo	Selecione os tipos de tráfego aos quais a regra correspondente se aplica. Os tipos de tráfego são bucket, bucket regex, CIDR, terminal balanceador de carga e locatário.
Corresponder valor	Introduza o valor que corresponde ao tipo selecionado. • Balde: Introduza um ou mais nomes de intervalo. • Regex do bucket: Insira uma ou mais expressões regulares usadas para corresponder a um conjunto de nomes de bucket. A expressão regular não está ancorada. Use a âncora para coincidir no início do nome do bucket e use a âncora para coincidir no final do nome. A correspondência regular de expressões suporta um subconjunto da sintaxe PCRE (Perl compatible regular expression). • CIDR: Insira uma ou mais sub-redes IPv4, na notação CIDR, que corresponda à sub-rede desejada. • Ponto de extremidade do balanceador de carga: Selecione um nome de ponto de extremidade. Estes são os pontos de extremidade do balanceador de carga definidos no "Configurar pontos de extremidade do balanceador de carga". • Inquilino: A correspondência de inquilino usa o ID da chave de acesso. Se a solicitação não contiver um ID de chave de acesso (por exemplo, acesso anônimo), a propriedade do intervalo acessado será usada para determinar o locatário.

Campo	Descrição
Correspondência inversa	Se você quiser corresponder todo tráfego de rede *exceto* tráfego consistente com o valor tipo e correspondência definido, marque a caixa de seleção **correspondência inversa**. Caso contrário, deixe a caixa de seleção marcada. Por exemplo, se você quiser que essa política se aplique a todos os pontos finais do balanceador de carga, especifique o ponto final do balanceador de carga a ser excluído e selecione **correspondência inversa**. Para uma política que contenha vários matchers em que pelo menos um é um matcher inverso, tenha cuidado para não criar uma política que corresponda a todas as solicitações.

5. Opcionalmente, selecione **Adicionar um limite** e selecione os seguintes detalhes para adicionar um ou mais limites para controlar o tráfego de rede correspondido por uma regra.

> O StorageGRID coleta métricas mesmo que você não adicione limites, para que você possa entender as tendências de tráfego.

Campo	Descrição
Tipo	O tipo de limite que você deseja aplicar ao tráfego de rede correspondente à regra. Por exemplo, você pode limitar a largura de banda ou a taxa de solicitação. **Nota**: Você pode criar políticas para limitar a largura de banda agregada ou para limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Quando a largura de banda agregada está em uso, a largura de banda por solicitação não está disponível. Por outro lado, quando a largura de banda por solicitação está em uso, a largura de banda agregada não está disponível. Os limites de largura de banda agregada podem impor um impactos menor no desempenho adicional no tráfego não limitado. Para limites de largura de banda, o StorageGRID aplica a política que melhor corresponde ao tipo de limite definido. Por exemplo, se você tem uma política que limita o tráfego em apenas uma direção, então o tráfego na direção oposta será ilimitado, mesmo que haja tráfego que corresponda a políticas adicionais que tenham limites de largura de banda. O StorageGRID implementa as correspondências "melhores" para limites de largura de banda na seguinte ordem: • Endereço IP exato (/máscara 32) • Nome exato do balde • Regex do balde • Locatário • Endpoint • Correspondências CIDR não exatas (não /32) • Correspondências inversas

Campo	Descrição
Aplica-se a	Se esse limite se aplica a solicitações de leitura do cliente (GET ou HEAD) ou solicitações de gravação (PUT, POST ou DELETE).
Valor	O valor ao qual o tráfego de rede será limitado, com base na unidade selecionada. Por exemplo, digite 10 e selecione MIB/s para evitar que o tráfego de rede combinado por esta regra exceda 10 MIB/s. **Nota**: Dependendo da configuração de unidades, as unidades disponíveis serão binárias (por exemplo, GiB) ou decimais (por exemplo, GB). Para alterar a configuração unidades, selecione a lista suspensa usuário no canto superior direito do Gerenciador de Grade e selecione **Preferências do usuário**.
Unidade	A unidade que descreve o valor introduzido.

Por exemplo, se você quiser criar um limite de largura de banda de 40 GB/s para um nível SLA, crie dois limites de largura de banda agregados: GET/HEAD a 40 GB/s e PUT/POST/DELETE a 40 GB/s.

6. Selecione **continuar**.
7. Leia e reveja a política de classificação de tráfego. Use o botão **anterior** para voltar e fazer alterações conforme necessário. Quando estiver satisfeito com a política, selecione **Salvar e continuar**.

   O tráfego do cliente S3 é agora Tratado de acordo com a política de classificação de tráfego.

Depois de terminar

"Exibir métricas de tráfego de rede" para verificar se as políticas estão aplicando os limites de tráfego que você espera.

Editar política de classificação de tráfego

Você pode editar uma política de classificação de tráfego para alterar seu nome ou descrição, ou para criar, editar ou excluir quaisquer regras ou limites para a política.

Antes de começar

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

Passos

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

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

2. Edite a política usando o menu ações ou a página de detalhes. Consulte "crie políticas de classificação de tráfego" para saber o que introduzir.

Menu ações

a. Selecione a caixa de verificação da política.

b. Selecione **ações** > **Editar**.

Página de detalhes

a. Selecione o nome da política.

b. Selecione o botão **Editar** ao lado do nome da política.

3. Para a etapa Digite o nome da política, edite opcionalmente o nome ou a descrição da política e selecione **continuar**.
4. Para a etapa Adicionar regras de correspondência, adicione uma regra ou edite o **tipo** e **valor de correspondência** da regra existente e selecione **continuar**.
5. Para a etapa Definir limites, opcionalmente adicione, edite ou exclua um limite e selecione **continuar**.
6. Revise a política atualizada e selecione **Salvar e continuar**.

   As alterações feitas na política são salvas e o tráfego de rede é agora Tratado de acordo com as políticas de classificação de tráfego. Você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

Eliminar uma política de classificação de tráfego

Você pode excluir uma política de classificação de tráfego se não precisar mais dela. Certifique-se de excluir a política certa porque uma política não pode ser recuperada quando excluída.

Antes de começar

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

Passos

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

   A página políticas de classificação de tráfego é exibida com as políticas existentes listadas em uma tabela.

2. Exclua a política usando o menu ações ou a página de detalhes.

   Menu ações

   a. Selecione a caixa de verificação da política.

   b. Selecione **ações** > **Remover**.

   Página de detalhes da política

   a. Selecione o nome da política.

   b. Selecione o botão **Remover** ao lado do nome da política.

3. Selecione **Sim** para confirmar que deseja excluir a política.

A política é eliminada.

Exibir métricas de tráfego de rede

Pode monitorizar o tráfego de rede visualizando os gráficos disponíveis na página políticas de classificação de tráfego.

Antes de começar

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

Sobre esta tarefa

Para qualquer política de classificação de tráfego existente, você pode exibir métricas para o serviço de balanceador de carga para determinar se a política está limitando com êxito o tráfego na rede. Os dados nos gráficos podem ajudá-lo a determinar se você precisa ajustar a política.

Mesmo que nenhum limite seja definido para uma política de classificação de tráfego, as métricas são coletadas e os gráficos fornecem informações úteis para entender as tendências de tráfego.

Passos

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

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

2. Selecione o nome da política de classificação de tráfego para o qual deseja exibir as métricas.
3. Selecione a guia **Metrics**.

   São apresentados os gráficos da política de classificação de tráfego. Os gráficos exibem métricas apenas para o tráfego que corresponde à política selecionada.

   Os gráficos a seguir estão incluídos na página.

   - Taxa de solicitação: Este gráfico fornece a quantidade de largura de banda que corresponde a essa política tratada por todos os balanceadores de carga. Os dados recebidos incluem cabeçalhos de solicitação para todas as solicitações e tamanho de dados do corpo para respostas que têm dados do corpo. Enviado inclui cabeçalhos de resposta para todas as solicitações e tamanho de dados do corpo de resposta para solicitações que incluem dados do corpo na resposta.

     > Quando as solicitações são concluídas, este gráfico mostra somente o uso da largura de banda. Para solicitações de objetos lentos ou grandes, a largura de banda instantânea real pode diferir dos valores relatados neste gráfico.

   - Taxa de resposta de erro: Este gráfico fornece uma taxa aproximada na qual as solicitações correspondentes a esta política estão retornando erros (código de status HTTP > 400) para clientes.
   - Duração média da solicitação (não-erro): Este gráfico fornece uma duração média de solicitações bem-sucedidas correspondentes a essa política.
   - Uso de largura de banda da política: Este gráfico fornece a quantidade de largura de banda que corresponde a essa política tratada por todos os balanceadores de carga. Os dados recebidos incluem cabeçalhos de solicitação para todas as solicitações e tamanho de dados do corpo para respostas que têm dados do corpo. Enviado inclui cabeçalhos de resposta para todas as solicitações e tamanho de dados do corpo de resposta para solicitações que incluem dados do corpo na resposta.

4. Posicione o cursor sobre um gráfico de linhas para ver um pop-up de valores em uma parte específica do gráfico.
5. Selecione **Painel Grafana** logo abaixo do título Metrics para visualizar todos os gráficos de uma política. Além dos quatro gráficos da guia **Metrics**, você pode ver mais dois gráficos:
   - Taxa de solicitação de gravação por tamanho do objeto: A taxa de solicitações DE PUT/POST/DELETE que correspondem a essa política. Posicionamento em uma célula individual mostra taxas por segundo. As taxas mostradas na exibição de hover são truncadas para contagens de inteiros e podem reportar 0 quando há solicitações não zero no intervalo.
   - Ler taxa de solicitação por tamanho do objeto: A taxa de SOLICITAÇÕES GET/HEAD correspondentes a essa política. Posicionamento em uma célula individual mostra taxas por segundo. As taxas mostradas na exibição de hover são truncadas para contagens de inteiros e podem reportar 0 quando há solicitações não zero no intervalo.
6. Em alternativa, aceda aos gráficos a partir do menu **SUPPORT**.
   a. Selecione **SUPPORT** > **Tools** > **Metrics**.
   b. Selecione **Política de classificação de tráfego** na seção **Grafana**.
   c. Selecione a política no menu no canto superior esquerdo da página.
   d. Posicione o cursor sobre um gráfico para ver um pop-up que mostra a data e a hora da amostra, os tamanhos de objetos que são agregados na contagem e o número de solicitações por segundo durante esse período de tempo.

      As políticas de classificação de tráfego são identificadas pelo seu ID. Os IDs de política são listados na página políticas de classificação de tráfego.
7. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustar a política.

Cifras suportadas para conexões TLS de saída

O sistema StorageGRID oferece suporte a um conjunto limitado de conjuntos de codificação para conexões TLS (Transport Layer Security) com os sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

Versões suportadas do TLS

O StorageGRID oferece suporte ao TLS 1,2 e TLS 1,3 para conexões a sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

As cifras TLS que são suportadas para utilização com sistemas externos foram selecionadas para garantir a compatibilidade com uma gama de sistemas externos. A lista é maior do que a lista de cifras que são suportadas para uso com aplicativos cliente S3. Para configurar cifras, vá para **CONFIGURATION** > **Security** > **Security settings** e selecione **TLS e SSH policies**.

> As opções de configuração TLS, como versões de protocolo, cifras, algoritmos de troca de chaves e algoritmos MAC, não são configuráveis no StorageGRID. Entre em Contato com o representante da sua conta do NetApp se você tiver solicitações específicas sobre essas configurações.

Benefícios de conexões HTTP ativas, ociosas e simultâneas

Como configurar conexões HTTP pode afetar o desempenho do sistema StorageGRID. As configurações diferem dependendo se a conexão HTTP está ativa ou inativa ou se você tem várias conexões simultâneas.

Você pode identificar os benefícios de desempenho para os seguintes tipos de conexões HTTP:

- Conexões HTTP ociosas
- Conexões HTTP ativas
- Conexões HTTP simultâneas

Benefícios de manter conexões HTTP ociosas abertas

Você deve manter as conexões HTTP abertas mesmo quando os aplicativos cliente estiverem ociosos para permitir que os aplicativos cliente executem transações subsequentes pela conexão aberta. Com base nas medições do sistema e na experiência de integração, você deve manter uma conexão HTTP inativa aberta por um máximo de 10 minutos. O StorageGRID pode fechar automaticamente uma conexão HTTP que é mantida aberta e inativa por mais de 10 minutos.

Conexões HTTP abertas e ociosas fornecem os seguintes benefícios:

- Latência reduzida desde o tempo em que o sistema StorageGRID determina que ele tem que executar uma transação HTTP para o tempo em que o sistema StorageGRID pode executar a transação

  A latência reduzida é a principal vantagem, especialmente pelo tempo necessário para estabelecer conexões TCP/IP e TLS.

- Aumento da taxa de transferência de dados por priming do algoritmo de início lento TCP/IP com transferências realizadas anteriormente
- Notificação instantânea de várias classes de condições de falha que interrompem a conetividade entre o aplicativo cliente e o sistema StorageGRID

Determinar por quanto tempo manter uma conexão inativa aberta é uma troca entre os benefícios do início lento que está associado à conexão existente e à alocação ideal da conexão com os recursos internos do sistema.

Benefícios de conexões HTTP ativas

Para conexões diretamente aos nós de armazenamento, você deve limitar a duração de uma conexão HTTP ativa a um máximo de 10 minutos, mesmo que a conexão HTTP realize transações continuamente.

Determinar a duração máxima em que uma conexão deve ser mantida aberta é um trade-off entre os benefícios da persistência da conexão e a alocação ideal da conexão aos recursos internos do sistema.

Para conexões de cliente a nós de storage, limitar conexões HTTP ativas fornece os seguintes benefícios:

- Permite o balanceamento de carga ideal em todo o sistema StorageGRID.

  Ao longo do tempo, uma conexão HTTP pode não ser mais ótima, pois os requisitos de balanceamento de carga mudam. O sistema executa seu melhor balanceamento de carga quando os aplicativos clientes estabelecem uma conexão HTTP separada para cada transação, mas isso nega os ganhos muito mais valiosos associados às conexões persistentes.

- Permite que aplicativos cliente direcionem transações HTTP para serviços LDR que têm espaço disponível.
- Permite iniciar os procedimentos de manutenção.

  Alguns procedimentos de manutenção começam somente depois que todas as conexões HTTP em andamento estiverem concluídas.

Para conexões de clientes ao serviço Load Balancer, limitar a duração das conexões abertas pode ser útil para permitir que alguns procedimentos de manutenção sejam iniciados prontamente. Se a duração das conexões do cliente não for limitada, pode levar vários minutos para que as conexões ativas sejam automaticamente encerradas.

Benefícios de conexões HTTP simultâneas

Você deve manter várias conexões TCP/IP ao sistema StorageGRID abertas para permitir paralelismo, o que aumenta o desempenho. O número ideal de conexões paralelas depende de uma variedade de fatores.

As conexões HTTP simultâneas oferecem os seguintes benefícios:

- Latência reduzida

  As transações podem começar imediatamente em vez de esperar que outras transações sejam concluídas.

- Maior taxa de transferência

  O sistema StorageGRID pode executar transações paralelas e aumentar a taxa de transferência de transações agregadas.

Os aplicativos clientes devem estabelecer várias conexões HTTP. Quando um aplicativo cliente tem que executar uma transação, ele pode selecionar e usar imediatamente qualquer conexão estabelecida que não esteja processando uma transação no momento.

A topologia de cada sistema StorageGRID tem um throughput de pico diferente para transações e conexões simultâneas antes que o desempenho comece a degradar. A taxa de transferência de pico depende de fatores como recursos de computação, recursos de rede, recursos de armazenamento e links WAN. O número de servidores e serviços e o número de aplicativos suportados pelo sistema StorageGRID também são fatores.

Os sistemas StorageGRID geralmente suportam vários aplicativos clientes. Você deve ter isso em mente quando determinar o número máximo de conexões simultâneas usadas por um aplicativo cliente. Se o aplicativo cliente consistir em várias entidades de software que estabelecem conexões com o sistema StorageGRID, você deve adicionar todas as conexões entre as entidades. Talvez seja necessário ajustar o número máximo de conexões simultâneas nas seguintes situações:

- A topologia do sistema StorageGRID afeta o número máximo de transações simultâneas e conexões que o sistema pode suportar.
- Os aplicativos clientes que interagem com o sistema StorageGRID em uma rede com largura de banda limitada podem ter que reduzir o grau de simultaneidade para garantir que as transações individuais sejam concluídas em um tempo razoável.
- Quando muitos aplicativos clientes compartilham o sistema StorageGRID, você pode ter que reduzir o grau de simultaneidade para evitar exceder os limites do sistema.

Separação de pools de conexão HTTP para operações de leitura e gravação

Você pode usar pools separados de conexões HTTP para operações de leitura e gravação e controlar quanto de um pool usar para cada um. Pools separados de conexões HTTP permitem que você controle melhor as transações e equilibre as cargas.

Os aplicativos clientes podem criar cargas que são retrieve-dominant (read) ou store-dominant (write). Com pools separados de conexões HTTP para transações de leitura e gravação, você pode ajustar quanto de cada pool a dedicar para transações de leitura ou gravação.

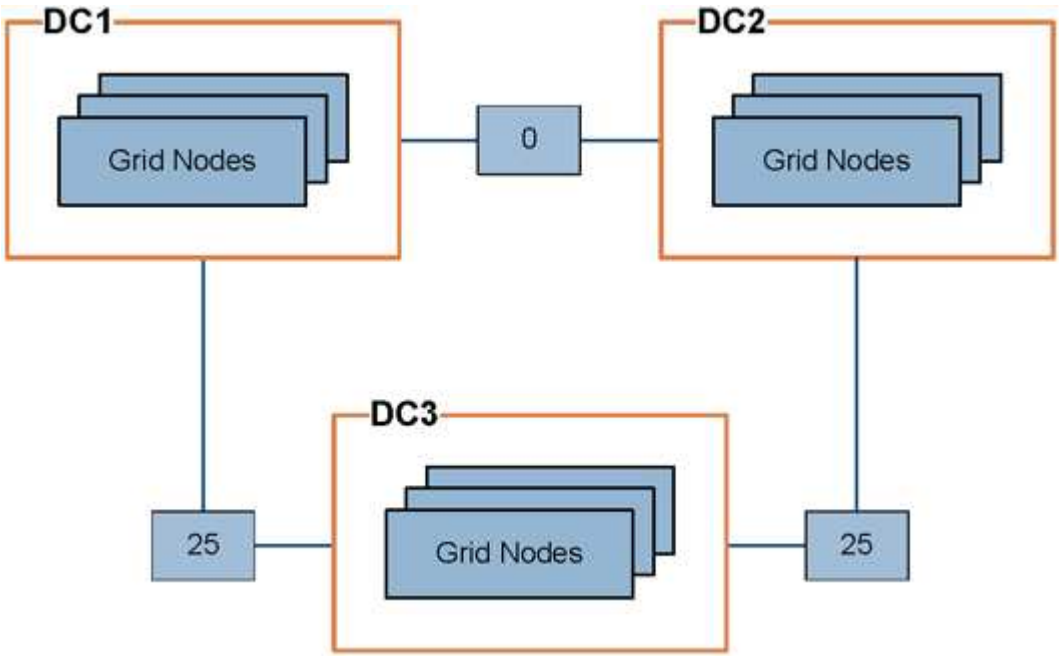
Gerenciar custos de link

Os custos de link permitem que você priorize qual local do data center fornece um serviço solicitado quando existem dois ou mais locais de data center. Você pode ajustar os custos de link para refletir a latência entre sites.

O que são custos de link?

- Os custos de link são usados para priorizar qual cópia de objeto é usada para cumprir recuperações de objetos.
- Os custos de link são usados pela API de gerenciamento de grade e pela API de gerenciamento de locatário para determinar quais serviços internos do StorageGRID devem ser usados.
- Os custos de link são usados pelo serviço Load Balancer em nós de administração e nós de gateway para direcionar as conexões do cliente. "Considerações para balanceamento de carga"Consulte .

O diagrama mostra uma grade de três sites que tem custos de link configurados entre sites:



- O serviço Load Balancer em nós de administração e nós de gateway distribui igualmente as conexões de clientes para todos os nós de storage no mesmo local do data center e para qualquer local do data center com um custo de link de 0.

  No exemplo, um nó de gateway no local do data center 1 (DC1) distribui igualmente as conexões de cliente para nós de storage em DC1 e para nós de storage em DC2. Um nó de gateway em DC3 envia conexões de cliente somente para nós de storage em DC3.

- Ao recuperar um objeto que existe como várias cópias replicadas, o StorageGRID recupera a cópia no data center que tem o menor custo de link.

  No exemplo, se um aplicativo cliente em DC2 recupera um objeto que é armazenado em DC1 e DC3, o objeto é recuperado de DC1, porque o custo do link de DC1 para DC2 é 0, o que é menor do que o custo do link de DC3 para DC2 (25).

Os custos de ligação são números relativos arbitrários sem unidade de medida específica. Por exemplo, um custo de link de 50 é usado menos preferencialmente do que um custo de link de 25. A tabela mostra os custos de link comumente usados.

Link	Custo da ligação	Notas
Entre locais de data center físico	25 (predefinição)	Data centers conectados por um link WAN.
Entre locais lógicos de data center no mesmo local físico	0	Data centers lógicos no mesmo prédio físico ou campus conetados por uma LAN.

Atualizar custos de link

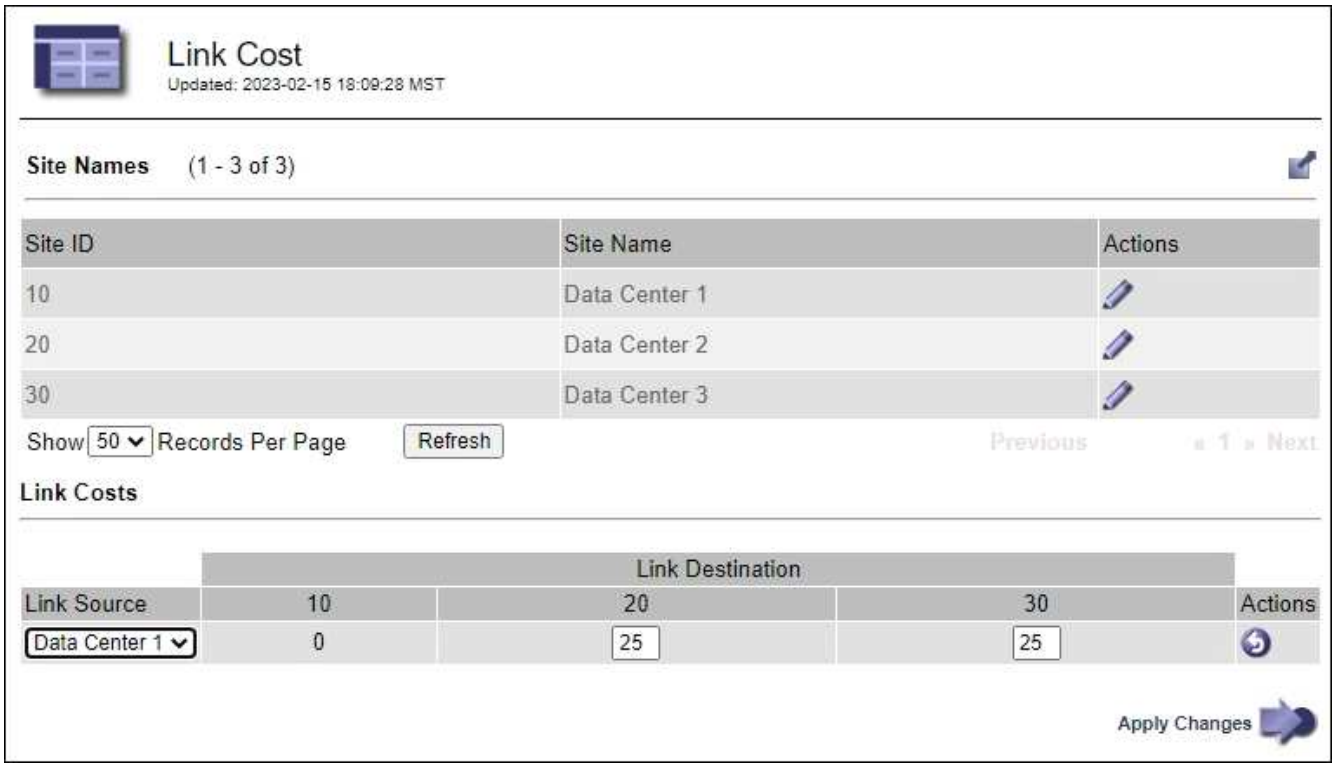
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de configuração de página de topologia de grade".

Passos

1. Selecione **SUPPORT** > **Other** > **Link Cost**.



2. Selecione um site em **Link Source** e insira um valor de custo entre 0 e 100 em **Link Destination**.

   Não é possível alterar o custo do link se a origem for a mesma do destino.

   Para cancelar as alterações, selecione **Revert**.

3. Selecione **aplicar alterações**.

Use o AutoSupport

O que é o AutoSupport?

O recurso AutoSupport permite que o StorageGRID envie pacotes de integridade e status para o suporte técnico da NetApp.

O uso do AutoSupport pode acelerar significativamente a determinação e resolução de problemas. O suporte técnico também pode monitorar as necessidades de storage do seu sistema e ajudá-lo a determinar se precisa adicionar novos nós ou sites. Opcionalmente, você pode configurar pacotes AutoSupport para serem enviados para um destino adicional.

StorageGRID tem dois tipos de AutoSupport:

- **StorageGRID AutoSupport** relata problemas de software StorageGRID. Ativado por padrão quando você instala o StorageGRID pela primeira vez. Você pode"Altere a configuração padrão do AutoSupport", se necessário.

> Se o StorageGRID AutoSupport não estiver ativado, uma mensagem será exibida no painel Gerenciador de Grade. A mensagem inclui um link para a página de configuração do AutoSupport. Se você fechar a mensagem, ela não aparecerá novamente até que o cache do navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

- **O Appliance hardware AutoSupport** relata problemas com o StorageGRID Appliance. Você deve "Configure o hardware AutoSupport em cada dispositivo".

O que é o Active IQ?

O Active IQ é um consultor digital baseado na nuvem que utiliza as análises preditivas e o conhecimento da comunidade da base instalada da NetApp. Suas avaliações de risco contínuas, alertas preditivos, orientações prescritivas e ações automatizadas ajudam a evitar problemas antes que eles ocorram, levando a uma melhor integridade do sistema e maior disponibilidade do sistema.

Para usar os painéis e a funcionalidade do Active IQ no site de suporte da NetApp, é necessário habilitar o AutoSupport.

"Documentação do consultor digital da Active IQ"

Informações incluídas no pacote AutoSupport

Um pacote AutoSupport contém os seguintes arquivos e detalhes.

Nome do ficheiro	Campos	Descrição
AutoSupport-HISTORY.xml	AutoSupport número de sequência e destino para este AutoSupport, Estado de entrega e tentativas de entrega, AutoSupport Assunto e URI de entrega último erro, AutoSupport COLOCAR nome de ficheiro, tempo de geração, AutoSupport tamanho comprimido e AutoSupport tamanho descomprimido e tempo total de recolha (ms)	Ficheiro de histórico do AutoSupport.
AutoSupport.xml	Endereço de suporte e estado do AutoSupport OnDemand, URL do servidor do AutoSupport OnDemand e intervalo de votação do AutoSupport OnDemand	Ficheiro de estado do AutoSupport. Fornece detalhes do protocolo usado, URL e endereço de suporte técnico, intervalo de polling e OnDemand AutoSupport, se ativado ou desativado.
BUCKETS.XML	ID do bucket e ID da conta, versão de compilação e restrição de localização Configuração e conformidade ativada e S3 bloqueio de objeto ativado e S3 Configuração de bloqueio de objeto ativado	Fornece detalhes de configuração e estatísticas no nível do intervalo. Exemplos de configurações de bucket incluem serviços de plataforma, conformidade e consistência do bucket.

Nome do ficheiro	Campos	Descrição
GRID-CONFIGURATIONS.XML	ID do atributo e Nome do atributo, valor e índice, ID da tabela e nome da tabela	Arquivo de informações de configuração em toda a grade. Contém informações sobre certificados de grade, espaço reservado de metadados, configurações em toda a grade (conformidade, bloqueio de objeto S3, compactação de objetos, alertas, configuração syslog e ILM), detalhes do perfil de codificação de apagamento, nome DNS e "Nome NMS".
GRID-SPEC.XML	Especificações de grade, XML bruto	Usado para configurar e implantar o StorageGRID. Contém especificações de grade, IP do servidor NTP, IP do servidor DNS, topologia de rede e perfis de hardware dos nós.
GRID-TAREFA.XML	Nome do atributo, valor, índice, ID da tabela e nome da tabela	Ficheiro de estado das tarefas de grelha (procedimentos de manutenção). Fornece detalhes das tarefas ativas, terminadas, concluídas, falhadas e pendentes da grade.
GRID.JSON	Licença e senhas, DNS e NTP, sites e nós	Informação da grelha.
ILM-CONFIGURATION.XML	ID do atributo e Nome do atributo, valor e índice, ID da tabela e nome da tabela	Lista de atributos para configurações ILM.
ILM-STATUS.XML	Nome do atributo, valor, índice, ID da tabela e nome da tabela	Arquivo de informações de métricas ILM. Contém taxas de avaliação de ILM para cada nó e métricas em toda a grade.
ILM.XML	XML bruto ILM	Ficheiro de política ativa ILM. Contém detalhes sobre as políticas de ILM ativas, como ID do pool de armazenamento, comportamento de ingestão, filtros, regras e descrição.
LOG.TGZ	*n/a*	Ficheiro de registo transferível. Contém `bycast-err.log` e `servermanager.log` de cada nó.

Nome do ficheiro	Campos	Descrição
MANIFEST.XML	Descrição deste item de dados, número de bytes coletados, tempo gasto na coleta, AutoSupport status deste item de dados, descrição do erro e tipo de conteúdo AutoSupport para esses dados	Contém metadados AutoSupport e descrições breves de todos os arquivos AutoSupport.
NMS-ENTITIES.XML	Índice de atributos, OID da entidade, ID do nó, ID do modelo do dispositivo, versão do modelo do dispositivo e nome da entidade	Entidades de grupo e de serviço no "Árvore NMS". Fornece detalhes da topologia da grade. O nó pode ser determinado com base nos serviços executados no nó.
OBJECTS-STATUS.XML	Nome do atributo, valor, índice, ID da tabela e nome da tabela	Estado do objeto, incluindo o estado da verificação em segundo plano, transferência ativa, taxa de transferência, transferências totais, taxa de eliminação, fragmentos corrompidos, objetos perdidos, objetos em falta, tentativa de reparação, taxa de digitalização, período de digitalização estimado e estado de conclusão de reparação.
SERVER-STATUS.XML	Nome do atributo, valor, índice, ID da tabela e nome da tabela	Configurações do servidor. Contém esses detalhes para cada nó: Tipo de plataforma, sistema operacional, memória instalada, memória disponível, conetividade de armazenamento, número de série do chassi do dispositivo de armazenamento, contagem de unidades com falha no controlador de armazenamento, temperatura do chassi do controlador de computação, hardware de computação, número de série do controlador de computação, fonte de alimentação, tamanho da unidade e tipo de unidade.
SERVICE-STATUS.XML	Nome do atributo, valor, índice, ID da tabela e nome da tabela	Arquivo de informações do nó de serviço. Contém detalhes como espaço alocado na tabela, espaço livre na tabela, métricas do Reaper do banco de dados, duração do reparo do segmento, duração do trabalho de reparo, reinicializações automáticas do trabalho e término automático do trabalho.

Nome do ficheiro	Campos	Descrição
STORAGE-GRADES.XML	ID do grau de armazenamento, nome do grau de armazenamento, ID do nó de armazenamento e caminho do nó de armazenamento	Arquivo de definições de grau de armazenamento para cada nó de storage.
SUMMARY-ATTRIBUTES.XML	ID do atributo do grupo, ID do atributo do resumo, nome do atributo do resumo, valor e índice, ID da tabela e nome da tabela	Dados de alto nível de status do sistema que resumem as informações de uso do StorageGRID. Fornece detalhes como nome da grade, nomes de sites, número de nós de storage por grade e por site, tipo de licença, capacidade e uso da licença, termos de suporte a software e detalhes de operações do S3.
SYSTEM-ALERTS.XML	Nome, gravidade, Nome do nó, Estado de Alerta, Nome do Site, tempo acionado por Alerta, tempo resolvido por Alerta, ID da regra, ID do nó, ID do Site e outras anotações e outras etiquetas	Alertas atuais do sistema que indicam potenciais problemas no sistema StorageGRID.
USERAGENTS.XML	O agente do usuário, o número de dias, o total de solicitações HTTP, o total de bytes ingeridos, o total de bytes recuperados, SOLICITAÇÕES DE INSERÇÃO, solicitações DE EXCLUSÃO, solicitações DE CABEÇALHO, solicitações de OPÇÕES, tempo médio de SOLICITAÇÃO (ms), tempo MÉDIO de solicitação DE COLOCAÇÃO (ms), tempo médio de solicitação de RECEBIMENTO (ms), tempo médio de solicitação de EXCLUSÃO (ms)	Estatísticas baseadas nos agentes do usuário do aplicativo. Por exemplo, o número de OPERAÇÕES PUT/GET/DELETE/HEAD por agente de usuário e o tamanho total de bytes de cada operação.
X-HEADER-DATA	X-NetApp-asup-servível X-NetApp-asup-server, X-NetApp-asup-server, X-NetApp-asup-server-num, X-NetApp-asup-subject, X-NetApp-asup-server-id e X-NetApp-asup-modelo-name	Dados do cabeçalho AutoSupport.

Configurar o AutoSupport

Por padrão, o recurso StorageGRID AutoSupport é ativado quando você instala o StorageGRID pela primeira vez. No entanto, você deve configurar o hardware AutoSupport em cada dispositivo. Conforme necessário, você pode alterar a configuração do AutoSupport.

Se você quiser alterar a configuração do StorageGRID AutoSupport, faça as alterações somente no nó de administração principal. Tem de Configurar AutoSupport de hardware utilizar em cada aparelho.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Se você usar HTTPS para enviar pacotes AutoSupport, você forneceu acesso de saída à Internet para o nó de administração principal, diretamente ou "usando um servidor proxy" (conexões de entrada não necessárias).
- Se HTTP estiver selecionado na página StorageGRID AutoSupport, você "configurado um servidor proxy" terá que encaminhar pacotes AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitarão pacotes enviados usando HTTP.
- Se você usar SMTP como protocolo para pacotes AutoSupport, você configurou um servidor de email SMTP.

Sobre esta tarefa

Você pode usar qualquer combinação das seguintes opções para enviar pacotes AutoSupport para suporte técnico:

- **Semanal**: Enviar automaticamente pacotes AutoSupport uma vez por semana. Predefinição: Activado.
- **Event-dispolled**: Envie pacotes AutoSupport automaticamente a cada hora ou quando ocorrerem eventos significativos do sistema. Predefinição: Activado.
- **Sob demanda**: Permita que o suporte técnico solicite que seu sistema StorageGRID envie pacotes AutoSupport automaticamente, o que é útil quando eles estão trabalhando ativamente em um problema (requer protocolo de transmissão HTTPS AutoSupport). Predefinição: Desativada.
- **User-Triggered**: Envie manualmente pacotes AutoSupport a qualquer momento.

Especifique o protocolo para pacotes AutoSupport

Você pode usar qualquer um dos seguintes protocolos para enviar pacotes AutoSupport:

- **HTTPS**: Esta é a configuração padrão e recomendada para novas instalações. Este protocolo utiliza a porta 443. Se pretender Ative o recurso AutoSupport On Demand, tem de utilizar HTTPS.
- * HTTP*: Se você selecionar HTTP, você deve configurar um servidor proxy para encaminhar pacotes AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitam pacotes enviados usando HTTP. Este protocolo utiliza a porta 80.
- **SMTP**: Use esta opção se quiser que os pacotes AutoSupport sejam enviados por e-mail.

O protocolo definido é utilizado para enviar todos os tipos de pacotes AutoSupport.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport** > **Settings**.

2. Selecione o protocolo que pretende utilizar para enviar pacotes AutoSupport.
3. Se você selecionou **HTTPS**, selecione se deseja usar um certificado de suporte NetApp (certificado TLS) para proteger a conexão com o servidor de suporte técnico.
   - **Verify certificate** (default): Garante que a transmissão de pacotes AutoSupport é segura. O certificado de suporte do NetApp já está instalado com o software StorageGRID.
   - **Não verifique o certificado**: Selecione esta opção somente quando tiver um bom motivo para não usar a validação do certificado, como quando houver um problema temporário com um certificado.
4. Selecione **Guardar**. Todos os pacotes semanais, acionados pelo usuário e acionados por eventos são enviados usando o protocolo selecionado.

Desativar AutoSupport semanal

Por padrão, o sistema StorageGRID é configurado para enviar um pacote AutoSupport para o suporte técnico uma vez por semana.

Para determinar quando o pacote AutoSupport semanal será enviado, vá para a guia **AutoSupport** > **resultados**. Na seção **Weekly AutoSupport**, observe o valor para **Next Scheduled Time**.

Você pode desativar o envio automático de pacotes AutoSupport semanais a qualquer momento.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport** > **Settings**.
2. Desmarque a caixa de seleção **Enable Weekly** (Ativar AutoSupport semanal*).
3. Selecione **Guardar**.

Desative o AutoSupport acionado por evento

Por padrão, o sistema StorageGRID é configurado para enviar um pacote AutoSupport para suporte técnico a cada hora.

Você pode desativar o AutoSupport acionado por evento a qualquer momento.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport** > **Settings**.
2. Desmarque a caixa de seleção **Enable Event-Triggered** (Ativar AutoSupport ativado por evento*).
3. Selecione **Guardar**.

Habilite o AutoSupport sob demanda

O AutoSupport On Demand pode ajudar a resolver problemas nos quais o suporte técnico está trabalhando ativamente.

Por padrão, o AutoSupport On Demand está desativado. Ativar este recurso permite que o suporte técnico solicite que seu sistema StorageGRID envie pacotes AutoSupport automaticamente. O suporte técnico também pode definir o intervalo de tempo de polling para consultas AutoSupport On Demand.

O suporte técnico não pode ativar ou desativar o AutoSupport sob demanda.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport** > **Settings**.

2. Selecione **HTTPS** para o protocolo.
3. Marque a caixa de seleção **Enable Weekly** (Ativar AutoSupport semanal*).
4. Marque a caixa de seleção **Enable on Demand** (Ativar AutoSupport on Demand*).
5. Selecione **Guardar**.

   O AutoSupport On Demand está ativado e o suporte técnico pode enviar solicitações AutoSupport On Demand para o StorageGRID.

Desativar verificações para atualizações de software

Por predefinição, o StorageGRID contacta o NetApp para determinar se estão disponíveis atualizações de software para o seu sistema. Se estiver disponível um hotfix do StorageGRID ou uma nova versão, a nova versão será exibida na página Atualização do StorageGRID.

Conforme necessário, você pode opcionalmente desativar a verificação de atualizações de software. Por exemplo, se o sistema não tiver acesso à WAN, desative a verificação para evitar erros de download.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport** > **Settings**.
2. Desmarque a caixa de verificação **verificar atualizações de software**.
3. Selecione **Guardar**.

Adicione um destino AutoSupport adicional

Quando você ativa o AutoSupport, os pacotes heath e status são enviados para o suporte técnico. Você pode especificar um destino adicional para todos os pacotes AutoSupport.

Para verificar ou alterar o protocolo usado para enviar pacotes AutoSupport, consulte as instruções para Especifique o protocolo para pacotes AutoSupport.

> Não é possível usar o protocolo SMTP para enviar pacotes AutoSupport para um destino adicional.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport** > **Settings**.
2. Selecione **Ativar destino AutoSupport Adicional**.
3. Especifique o seguinte:

   Nome do anfitrião

   O nome do host do servidor ou endereço IP de um servidor de destino AutoSupport adicional.

   > Pode introduzir apenas um destino adicional.

   Porta

   A porta usada para se conetar a um servidor de destino AutoSupport adicional. A predefinição é a porta 80 para HTTP ou a porta 443 para HTTPS.

Validação do certificado

Se um certificado TLS é usado para proteger a conexão com o destino adicional.

- Selecione **Verify certificate** (verificar certificado) para utilizar a validação do certificado.
- Selecione **não verificar certificado** para enviar seus pacotes AutoSupport sem validação de certificado.

  Selecione esta opção apenas quando tiver um bom motivo para não utilizar a validação do certificado, como por exemplo, quando houver um problema temporário com um certificado.

4. Se você selecionou **Verify certificate**, faça o seguinte:
   a. Navegue até o local do certificado da CA.
   b. Carregue o ficheiro de certificado da CA.

   Os metadados do certificado da CA são exibidos.
5. Selecione **Guardar**.

   Todos os pacotes AutoSupport semanais, acionados por eventos e acionados pelo usuário futuros serão enviados para o destino adicional.

Configurar o AutoSupport para dispositivos

O AutoSupport for Appliances relata problemas de hardware do StorageGRID e o StorageGRID AutoSupport relata problemas de software do StorageGRID, com uma exceção: Para o SGF6112, o StorageGRID AutoSupport relata problemas de hardware e software. Você deve configurar o AutoSupport em cada dispositivo, exceto o SGF6112, que não requer configuração adicional. O AutoSupport é implementado de maneira diferente para dispositivos de serviços e dispositivos de storage.

Você usa o SANtricity para ativar o AutoSupport para cada dispositivo de storage. Você pode configurar o SANtricity AutoSupport durante a configuração inicial do dispositivo ou depois que um dispositivo tiver sido instalado:

- Para aparelhos SG6000 e SG5700, "Configure o AutoSupport no Gerenciador de sistemas do SANtricity"

Os pacotes AutoSupport de dispositivos e-Series podem ser incluídos no StorageGRID AutoSupport se você configurar a entrega do AutoSupport por proxy no "Gerente do sistema da SANtricity".

O StorageGRID AutoSupport não relata problemas de hardware, como falhas de DIMM ou placa de interface do host (HIC). No entanto, algumas falhas de componentes podem acionar "alertas de hardware". Para dispositivos StorageGRID com um controlador de gerenciamento de placa base (BMC), você pode configurar traps de e-mail e SNMP para relatar falhas de hardware:

- "Configurar notificações por e-mail para alertas do BMC"
- "Configure as definições SNMP para BMC"

Informações relacionadas

"Suporte à NetApp"

Acione manualmente um pacote AutoSupport

Para ajudar o suporte técnico na solução de problemas com o sistema StorageGRID,

você pode acionar manualmente um pacote AutoSupport a ser enviado.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você deve ter a permissão de acesso root ou outra configuração de grade.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Na guia **ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

   O StorageGRID tenta enviar um pacote AutoSupport para o site de suporte da NetApp. Se a tentativa for bem-sucedida, os valores **resultado mais recente** e **último tempo bem-sucedido** na guia **resultados** serão atualizados. Se houver um problema, o valor **resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar o pacote AutoSupport novamente.

   Depois de enviar um pacote AutoSupport acionado pelo usuário, atualize a página AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Solucionar problemas de pacotes do AutoSupport

Se uma tentativa de enviar um pacote AutoSupport falhar, o sistema StorageGRID executa ações diferentes dependendo do tipo de pacote AutoSupport. Pode verificar o estado dos pacotes AutoSupport selecionando **SUPPORT** > **Tools** > **AutoSupport** > **results**.

Quando o pacote AutoSupport não é enviado, "Falha" aparece na guia **resultados** da página **AutoSupport**.

Se você configurou um servidor proxy para encaminhar pacotes do AutoSupport para o NetApp, você deve "verifique se as configurações do servidor proxy estão corretas".

Falha semanal do pacote AutoSupport

Se um pacote AutoSupport semanal falhar ao enviar, o sistema StorageGRID executa as seguintes ações:

1. Atualiza o atributo de resultado mais recente para tentar novamente.
2. Tenta reenviar o pacote AutoSupport 15 vezes a cada quatro minutos durante uma hora.
3. Após uma hora de falhas de envio, atualiza o atributo de resultado mais recente para Falha.
4. Tenta enviar um pacote AutoSupport novamente na próxima hora programada.
5. Mantém a programação regular do AutoSupport se o pacote falhar porque o serviço NMS não está disponível e se um pacote é enviado antes de sete dias passar.
6. Quando o serviço NMS estiver disponível novamente, envia um pacote AutoSupport imediatamente se um pacote não tiver sido enviado por sete dias ou mais.

Falha do pacote AutoSupport acionado pelo usuário ou acionado por evento

Se um pacote AutoSupport acionado pelo usuário ou acionado por evento não for enviado, o sistema StorageGRID executará as seguintes ações:

1. Exibe uma mensagem de erro se o erro for conhecido. Por exemplo, se um usuário selecionar o protocolo SMTP sem fornecer as configurações corretas de e-mail, o seguinte erro é exibido: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Não tenta enviar o pacote novamente.
3. Regista o erro no `nms.log`.

Se ocorrer uma falha e o SMTP for o protocolo selecionado, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o servidor de e-mail está em execução (**SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**). A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Aprenda a "configure as definições do servidor de correio eletrónico".

Corrija uma falha do pacote AutoSupport

Se ocorrer uma falha e o SMTP for o protocolo selecionado, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o servidor de e-mail está em execução. A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envie pacotes e-Series AutoSupport através do StorageGRID

Você pode enviar pacotes do e-Series SANtricity System Manager AutoSupport para suporte técnico por meio de um nó de administração do StorageGRID, em vez da porta de gerenciamento do dispositivo de storage.

```
https://docs.netapp.com/us-en/e-series-santricity/sm-support/autosupport-feature-overview.html["AutoSupport de hardware e-Series"^]Consulte para obter mais informações sobre como usar o AutoSupport com dispositivos e-Series.
```

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Administrador do dispositivo de storage ou permissão de acesso à raiz".
- Você configurou o SANtricity AutoSupport:
  - Para aparelhos SG6000 e SG5700, "Configure o AutoSupport no Gerenciador de sistemas do SANtricity"

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

Sobre esta tarefa

Os pacotes e-Series AutoSupport contêm detalhes do hardware de armazenamento e são mais específicos do que outros pacotes AutoSupport enviados pelo sistema StorageGRID.

Você pode configurar um endereço de servidor proxy especial no Gerenciador de sistema do SANtricity para

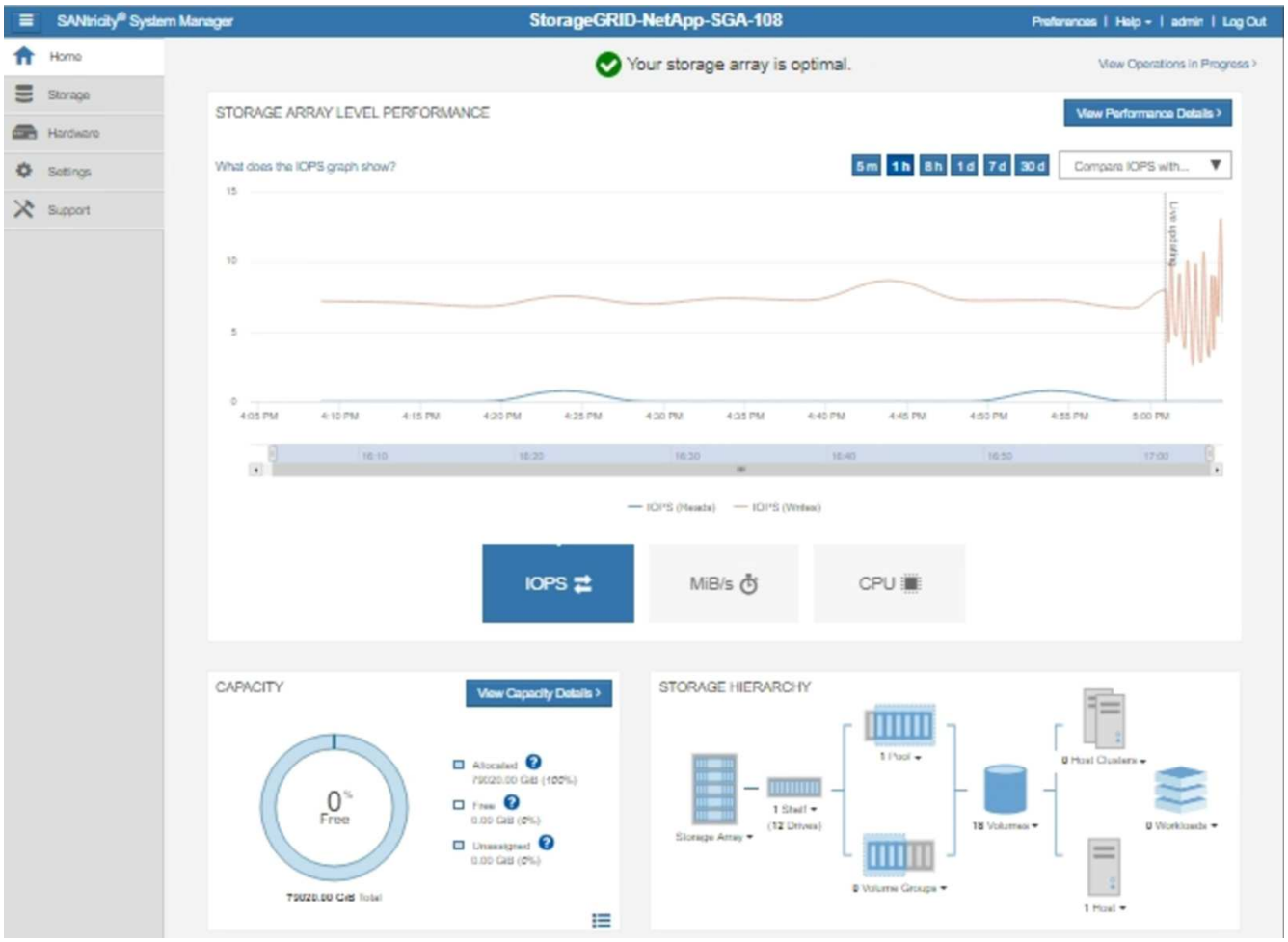
transmitir pacotes do AutoSupport por meio de um nó de administração do StorageGRID sem o uso da porta de gerenciamento do dispositivo. Os pacotes AutoSupport transmitidos desta forma são enviados pelo "Nó Admin. Remetente preferido", e usam qualquer um "configurações de proxy de administrador" que tenha sido configurado no Gerenciador de Grade.

> Este procedimento destina-se apenas à configuração de um servidor proxy StorageGRID para pacotes e-Series AutoSupport. Para obter detalhes adicionais sobre a configuração do e-Series AutoSupport, consulte "Documentação do NetApp e-Series e do SANtricity".

Passos

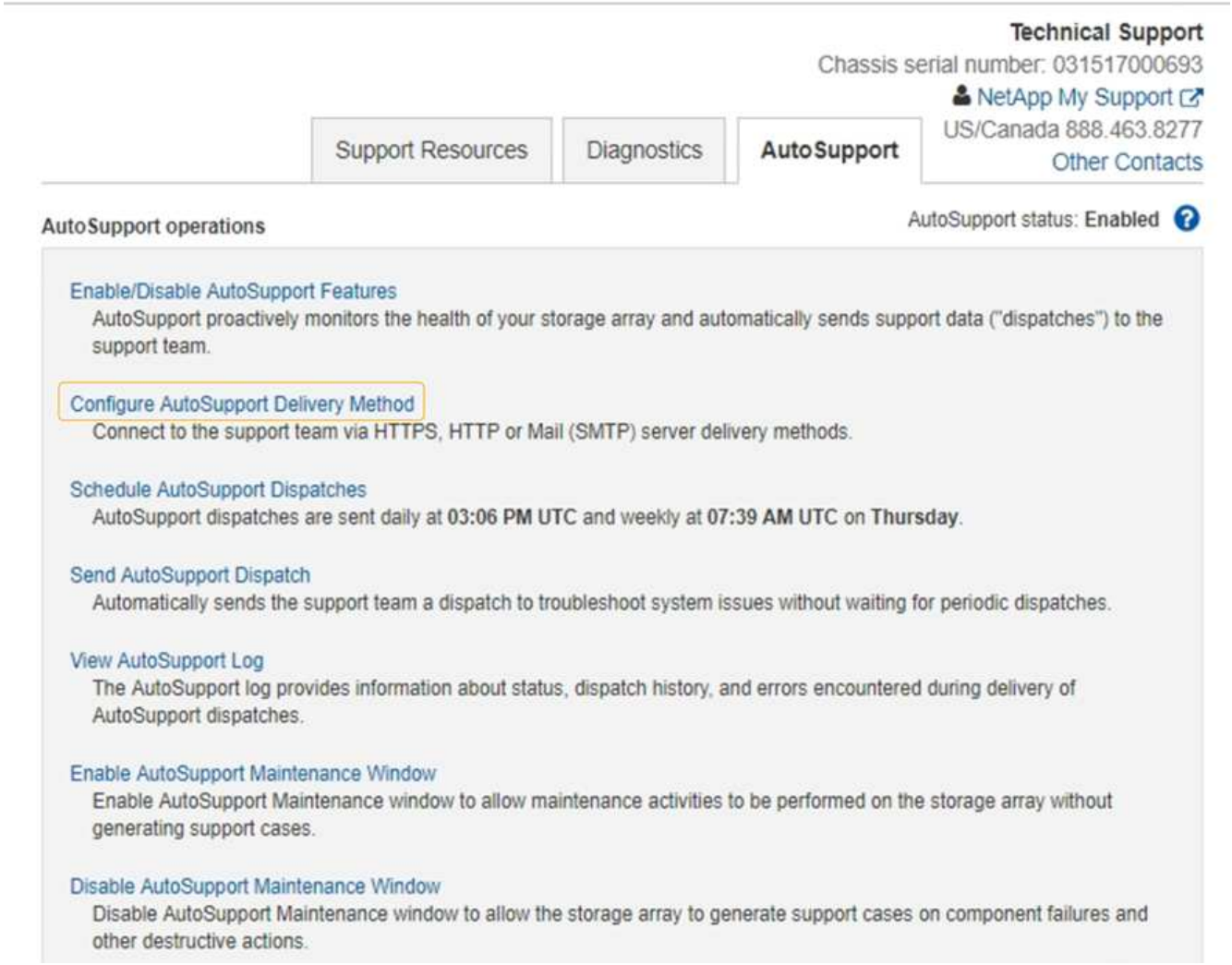
1. No Gerenciador de Grade, selecione **NÓS**.
2. Na lista de nós à esquerda, selecione o nó do dispositivo de storage que deseja configurar.
3. Selecione **Gerenciador do sistema SANtricity**.

   É apresentada a página inicial do Gestor do sistema SANtricity.



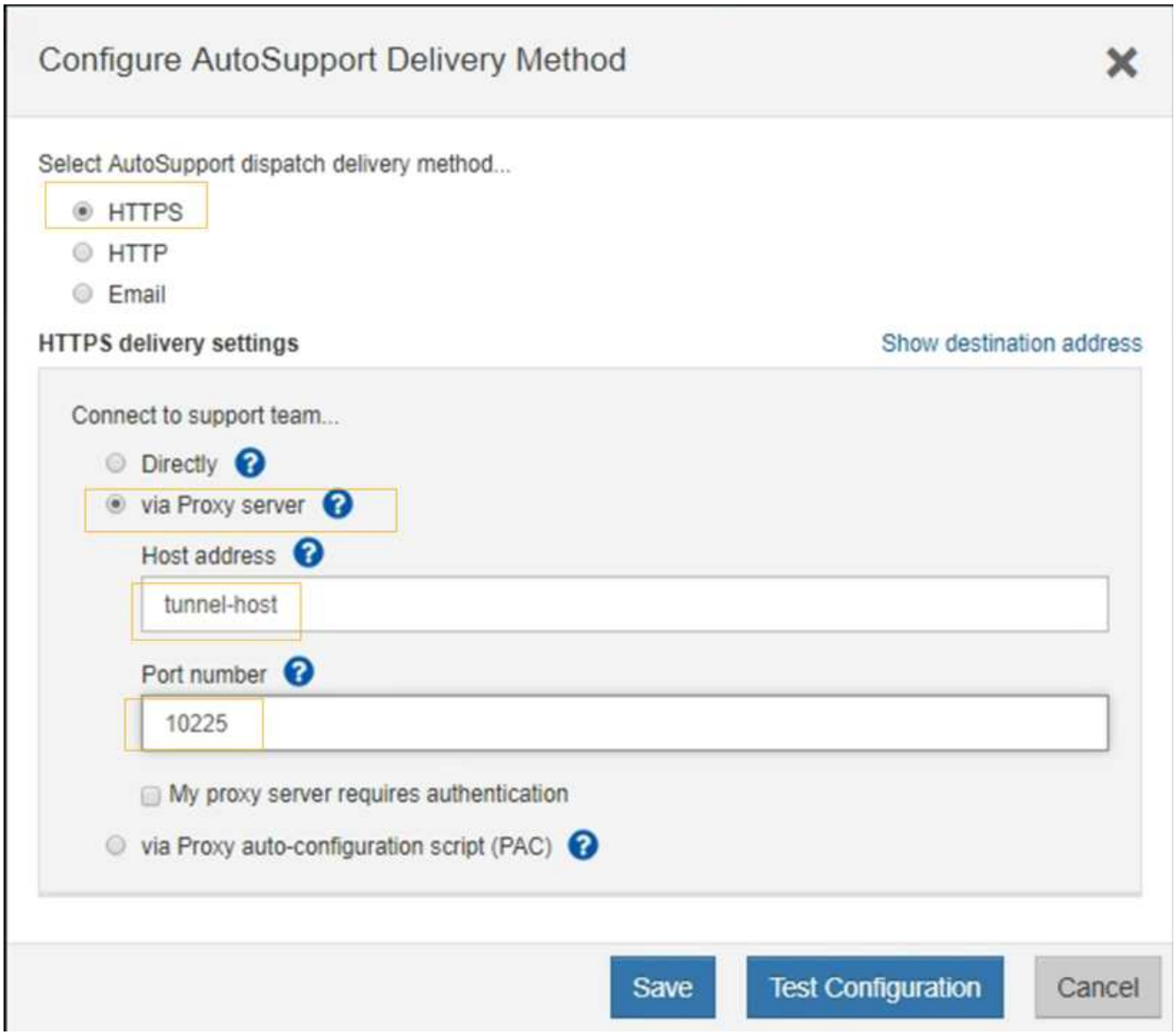
4. Selecione **SUPPORT** > **SUPPORT Center** > **AutoSupport**.

   É apresentada a página operations (operações de AutoSupport).



5. Selecione **Configurar método de entrega AutoSupport**.

   A página Configurar método de entrega AutoSupport é exibida.



6. Selecione **HTTPS** para o método de entrega.

   O certificado que ativa o HTTPS está pré-instalado.

7. Selecione **via servidor Proxy**.
8. Introduza `tunnel-host` o **Endereço anfitrião**.

   `tunnel-host` É o endereço especial para usar um nó de administrador para enviar pacotes e-Series AutoSupport.

9. Introduza `10225` o **número da porta**.

   `10225` É o número da porta no servidor proxy StorageGRID que recebe pacotes AutoSupport do controlador e-Series no dispositivo.

10. Selecione **Configuração de teste** para testar o roteamento e a configuração do servidor proxy AutoSupport.

    Se estiver correto, uma mensagem em um banner verde será exibida: "Sua configuração do AutoSupport

foi verificada."

Se o teste falhar, uma mensagem de erro será exibida em um banner vermelho. Verifique as configurações de DNS e a rede do StorageGRID, verifique se o "Nó Admin. Remetente preferido" pode se conetar ao site de suporte da NetApp e tente o teste novamente.

11. Selecione **Guardar**.

    A configuração é guardada e é apresentada uma mensagem de confirmação: "O método de entrega AutoSupport foi configurado."

Gerenciar nós de storage

Gerenciar nós de storage

Os nós de storage fornecem capacidade e serviços de storage em disco. O gerenciamento de nós de storage implica o seguinte:

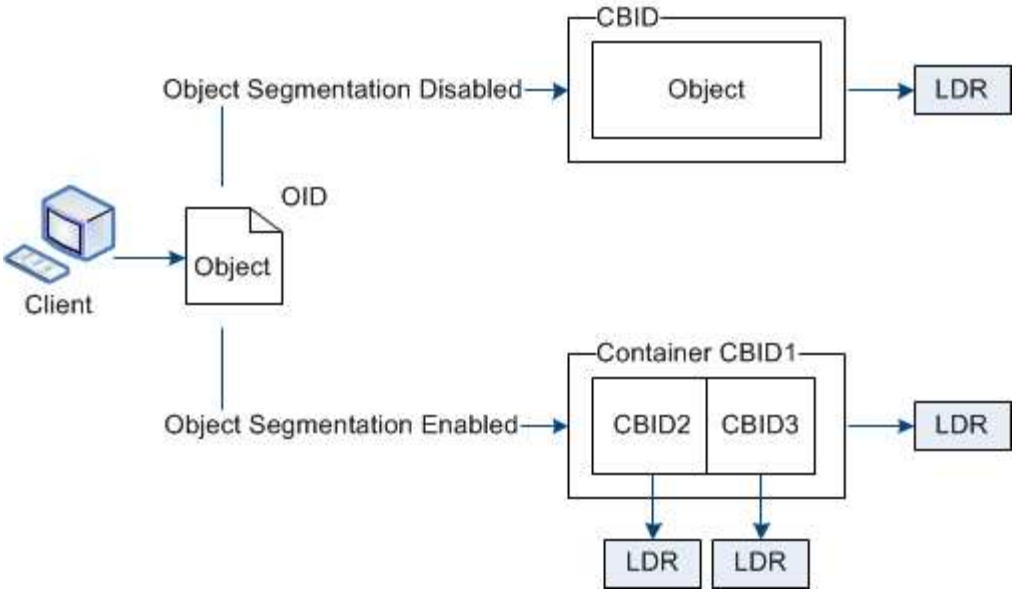
- Gerenciamento de opções de armazenamento
- Compreender quais são as marcas d'água do volume de storage e como você pode usar substituições de marca d'água para controlar quando os nós de armazenamento se tornam somente leitura
- Monitoramento e gerenciamento do espaço usado para metadados de objetos
- Configuração de configurações globais para objetos armazenados
- Aplicando as configurações do nó de armazenamento
- Gerenciamento de nós de storage completos

Use as opções de armazenamento

O que é segmentação de objetos?

A segmentação de objetos é o processo de dividir um objeto em uma coleção de objetos menores de tamanho fixo para otimizar o armazenamento e o uso de recursos para objetos grandes. O upload de várias partes do S3 também cria objetos segmentados, com um objeto representando cada parte.

Quando um objeto é ingerido no sistema StorageGRID, o serviço LDR divide o objeto em segmentos e cria um contentor de segmento que lista as informações do cabeçalho de todos os segmentos como conteúdo.



Ao recuperar um contentor de segmento, o serviço LDR monta o objeto original de seus segmentos e retorna o objeto ao cliente.

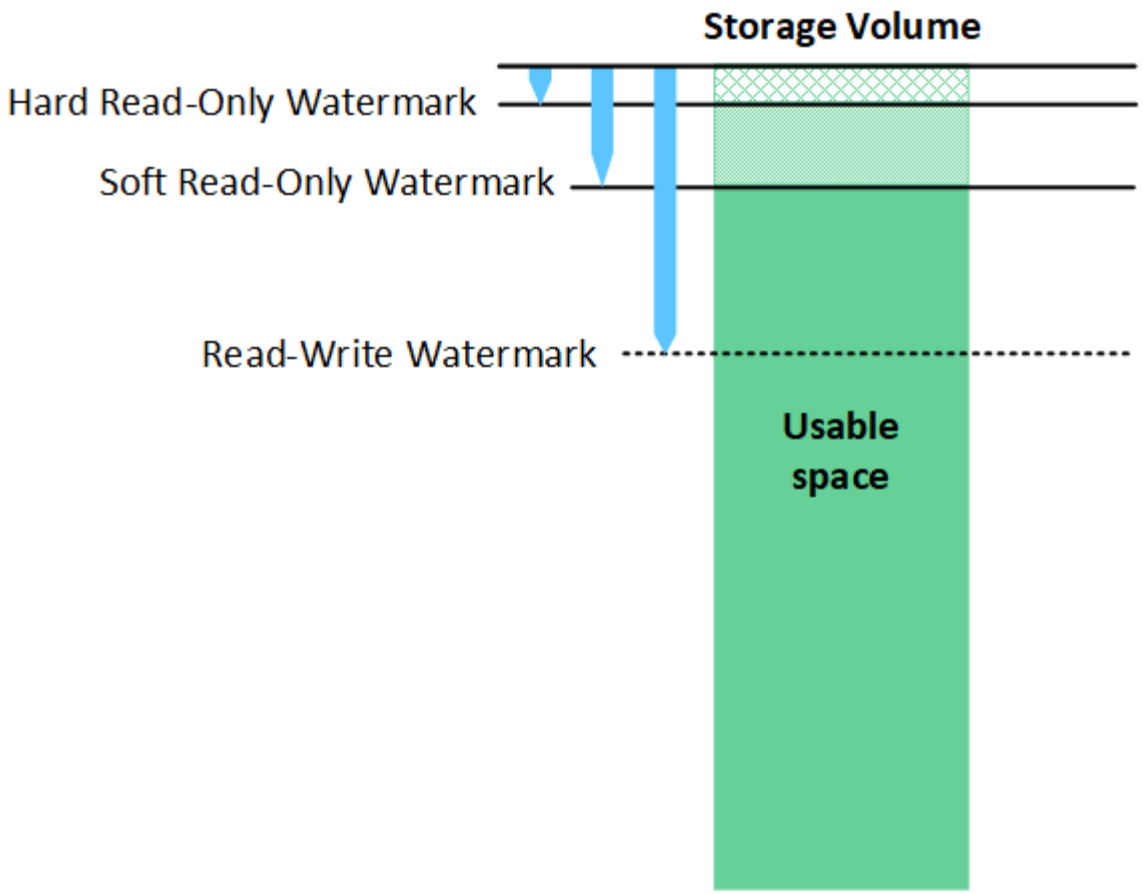
O contentor e os segmentos não são necessariamente armazenados no mesmo nó de armazenamento. O contentor e os segmentos podem ser armazenados em qualquer nó de armazenamento dentro do conjunto de armazenamento especificado na regra ILM.

Cada segmento é Tratado pelo sistema StorageGRID de forma independente e contribui para a contagem de atributos, como objetos gerenciados e objetos armazenados. Por exemplo, se um objeto armazenado no sistema StorageGRID for dividido em dois segmentos, o valor de objetos gerenciados aumentará em três após a ingestão ser concluída, da seguinte forma:

```
segment container + segment 1 + segment 2 = three stored objects
```

O que são marcas d'água de volume de armazenamento?

O StorageGRID usa três marcas d'água de volume de storage para garantir que os nós de storage sejam transferidos com segurança para um estado somente leitura antes que eles sejam executados com muito pouco espaço e para permitir que os nós de storage que foram transferidos para um estado somente leitura sejam novamente lidos.



As marcas d'água do volume de armazenamento aplicam-se apenas ao espaço utilizado para dados de objetos replicados e codificados por apagamento. Para saber mais sobre o espaço reservado para metadados de objetos no volume 0, vá para "Gerenciar o storage de metadados de objetos".

Qual é a marca d'água somente leitura suave?

A marca d'água de somente leitura suave do volume de armazenamento* é a primeira marca d'água a indicar que o espaço utilizável de um nó de armazenamento para dados de objetos está se tornando cheio.

Se cada volume em um nó de armazenamento tiver menos espaço livre do que a marca d'água somente leitura suave desse volume, o nó de armazenamento será transferido para o modo *somente leitura*. O modo somente leitura significa que o nó de storage anuncia serviços somente leitura para o resto do sistema StorageGRID, mas atende a todas as solicitações de gravação pendentes.

Por exemplo, suponha que cada volume em um nó de armazenamento tenha uma marca d'água somente leitura suave de 10 GB. Assim que cada volume tiver menos de 10 GB de espaço livre, o nó de armazenamento passa para o modo somente leitura suave.

Qual é a marca d'água apenas de leitura dura?

A marca d'água de somente leitura de volume de armazenamento* é a próxima marca d'água para indicar que o espaço utilizável de um nó para dados de objeto está se tornando cheio.

Se o espaço livre em um volume for menor do que a marca d'água somente leitura do volume, as gravações no volume falharão. No entanto, as gravações em outros volumes podem continuar até que o espaço livre nesses volumes seja menor do que suas marcas d'água apenas de leitura dura.

Por exemplo, suponha que cada volume em um nó de armazenamento tenha uma marca d'água somente leitura de 5 GB. Assim que cada volume tiver menos de 5 GB de espaço livre, o nó de armazenamento não aceita mais nenhuma solicitação de gravação.

A marca d'água apenas de leitura dura é sempre inferior à marca d'água apenas de leitura suave.

Qual é a marca d'água de leitura e escrita?

A marca d'água de leitura e gravação do volume de armazenamento* aplica-se apenas aos nós de armazenamento que fizeram a transição para o modo somente leitura. Ele determina quando o nó pode se tornar leitura-gravação novamente. Quando o espaço livre em qualquer volume de armazenamento em um nó de armazenamento é maior do que a marca d'água de leitura e gravação desse volume, o nó faz a transição automaticamente para o estado de leitura e gravação.

Por exemplo, suponha que o nó de armazenamento tenha sido transferido para o modo somente leitura. Suponha também que cada volume tenha uma marca d'água de leitura e gravação de 30 GB. Assim que o espaço livre para qualquer volume aumentar para 30 GB, o nó torna-se leitura-gravação novamente.

A marca d'água de leitura-escrita é sempre maior do que a marca d'água apenas de leitura suave e a marca d'água apenas de leitura dura.

Ver marcas de água do volume de armazenamento

Você pode visualizar as configurações atuais da marca d'água e os valores otimizados pelo sistema. Se não estiverem a ser utilizadas marcas de água otimizadas, pode determinar se pode ou deve ajustar as definições.

Antes de começar

- Concluiu a atualização para o StorageGRID 11,6 ou superior.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Ver as definições atuais da marca d'água

Você pode exibir as configurações atuais de marca d'água de armazenamento no Gerenciador de Grade.

Passos

1. Selecione **SUPPORT** > **Other** > **Storage watermarks**.
2. Na página marcas d'água de armazenamento, observe a caixa de seleção usar valores otimizados.
    - Se a caixa de verificação estiver selecionada, todas as três marcas de água são otimizadas para cada volume de armazenamento em cada nó de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

      Esta é a configuração padrão e recomendada. Não atualize estes valores. Opcionalmente, você pode Ver marcas de água de armazenamento otimizadas.

    - Se a caixa de seleção usar valores otimizados não estiver selecionada, marcas de água personalizadas (não otimizadas) estão sendo usadas. Não é recomendável usar configurações personalizadas de marca d'água. Use as instruções para "Solução de problemas de baixa substituição de marca d'água somente leitura alertas"determinar se você pode ou deve ajustar as configurações.

      Quando especificar definições de marca d'água personalizadas, tem de introduzir valores superiores a 0.

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 de somente leitura suave do volume de armazenamento. 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 otimizado mínimo da marca d'água somente leitura suave para todos os volumes de armazenamento em cada nó de armazenamento. Se esse valor for maior do que a configuração personalizada para a marca d'água de somente leitura suave do volume de armazenamento, o alerta **Substituição da marca d'água somente leitura baixa** será acionado para o nó de armazenamento.

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 otimizado máximo da marca d'água somente leitura suave para todos os volumes de armazenamento em cada nó de armazenamento.

Gerenciar o storage de metadados de objetos

A capacidade de metadados de objetos de um sistema StorageGRID controla o número máximo de objetos que podem ser armazenados nesse sistema. Para garantir que seu sistema StorageGRID tenha espaço adequado para armazenar novos objetos, você deve entender onde e como o StorageGRID armazena os metadados de objetos.

O que é metadados de objetos?

Metadados de objetos são qualquer informação que descreva um objeto. O StorageGRID usa metadados de objetos para rastrear os locais de todos os objetos na grade e gerenciar o ciclo de vida de cada objeto ao longo do tempo.

Para um objeto no StorageGRID, os metadados de objeto incluem os seguintes tipos de informações:

- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket do S3, 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

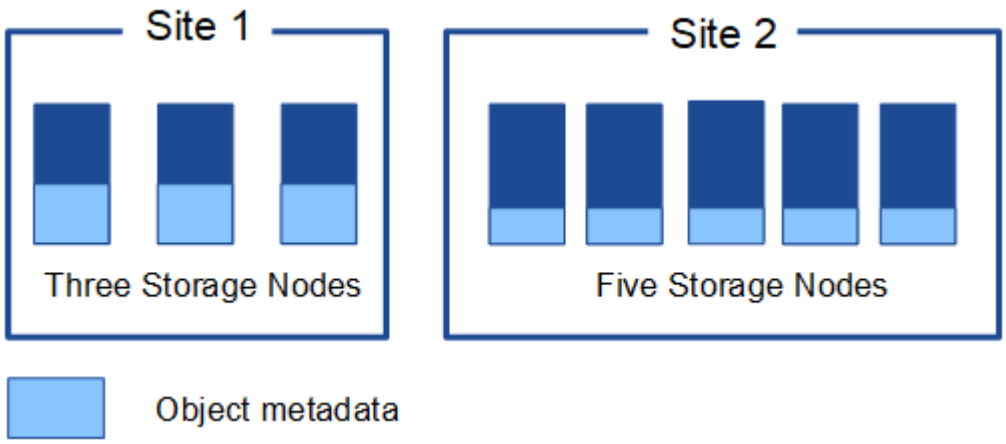
e o identificador exclusivo do objeto.

- Para objetos segmentados e objetos multipartes, identificadores de segmento e tamanhos de dados.

Como os metadados de objetos são armazenados?

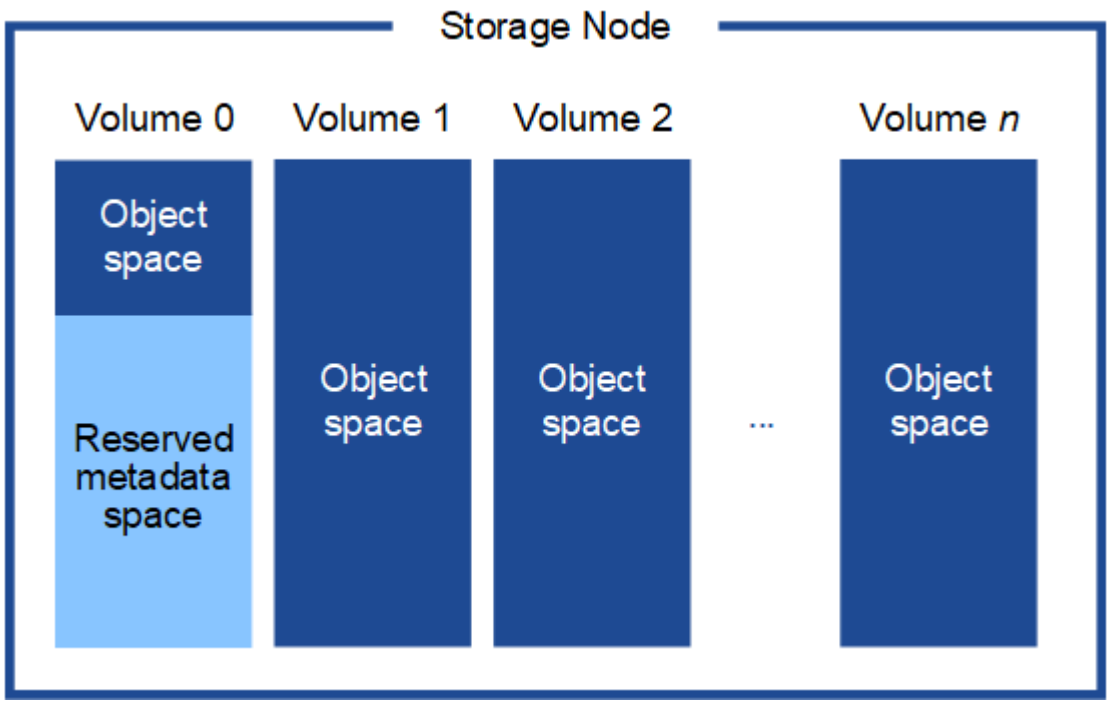
O StorageGRID mantém metadados de objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados do objeto. Para fornecer redundância e proteger os metadados de objetos contra perda, o StorageGRID armazena três cópias dos metadados de todos os objetos no sistema em cada local.

Essa figura representa os nós de storage em dois locais. Cada local tem a mesma quantidade de metadados de objetos, e os metadados de cada local são subdivididos entre todos os nós de storage nesse local.



Onde os metadados de objetos são armazenados?

Essa figura representa os volumes de storage de um único nó de storage.



Como mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de storage 0 de cada nó de storage. Ele usa o espaço reservado para armazenar metadados de objetos e executar

operações essenciais de banco de dados. Qualquer espaço restante no volume de storage 0 e todos os outros volumes de storage no nó de storage são usados exclusivamente para dados de objetos (cópias replicadas e fragmentos codificados por apagamento).

A quantidade de espaço reservada para metadados de objetos em um nó de storage específico depende de vários fatores, os quais são descritos abaixo.

Definição de espaço reservado de metadados

O *Metadata reserved space* é uma configuração em todo o sistema que representa a quantidade de espaço que será reservada para metadados no volume 0 de cada nó de armazenamento. Como mostrado na tabela, o valor padrão dessa configuração é baseado em:

- A versão de software que você estava usando quando você instalou o StorageGRID inicialmente.
- A quantidade de RAM em cada nó de armazenamento.

Versão utilizada para a instalação inicial do StorageGRID	Quantidade de RAM nos nós de storage	Configuração de espaço reservado de metadados padrão
11,5 a 11,9	128 GB ou mais em cada nó de storage na grade	8 TB (8.000 GB)
	Menos de 128 GB em qualquer nó de armazenamento na grade	3 TB (3.000 GB)
11,1 a 11,4	128 GB ou mais em cada nó de armazenamento em qualquer local	4 TB (4.000 GB)
	Menos de 128 GB em qualquer nó de storage em cada local	3 TB (3.000 GB)
11,0 ou anterior	Qualquer valor	2 TB (2.000 GB)

Exibir a configuração de espaço reservado de metadados

Siga estas etapas para visualizar a configuração espaço reservado metadados para o seu sistema StorageGRID.

Passos

1. Selecione **CONFIGURATION** > **System** > **Storage settings**.
2. Na página Configurações de armazenamento, expanda a seção **espaço reservado de metadados**.

Para o StorageGRID 11,8 ou superior, o valor de espaço reservado de metadados deve ser de pelo menos 100 GB e não mais de 1 PB.

A configuração padrão para uma nova instalação do StorageGRID 11,6 ou superior na qual cada nó de armazenamento tem 128 GB ou mais de RAM é de 8.000 GB (8 TB).

Espaço reservado real para metadados

Em contraste com a configuração espaço reservado de metadados em todo o sistema, o *espaço reservado real* para metadados de objetos é determinado para cada nó de armazenamento. Para qualquer nó de armazenamento, o espaço reservado real para metadados depende do tamanho do volume 0 para o nó e da configuração de espaço reservado metadados em todo o sistema.

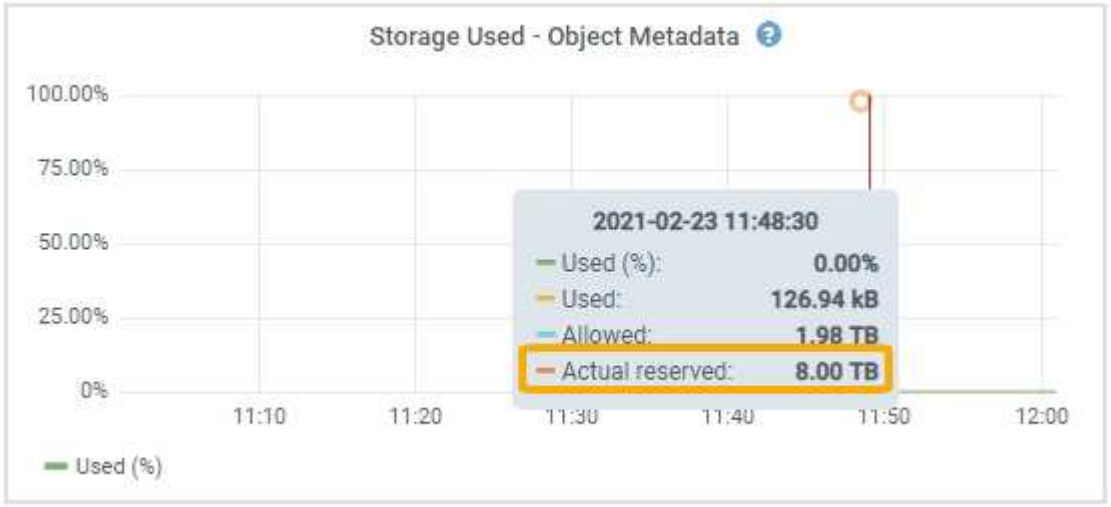
Tamanho do volume 0 para o nó	Espaço reservado real para metadados
Menos de 500 GB (uso não-produção)	10% do volume 0
500 GB ou mais ou mais nós de storage somente de metadados	O menor desses valores: • Volume 0 • Definição de espaço reservado de metadados **Nota**: Somente um rangedb é necessário para nós de storage somente metadados.

Veja o espaço reservado real para metadados

Siga estas etapas para exibir o espaço reservado real para metadados em um nó de armazenamento específico.

Passos

1. No Gerenciador de Grade, selecione **NÓS** > ***Storage Node***.
2. Selecione a guia **armazenamento**.
3. Posicione o cursor sobre o gráfico armazenamento usado - metadados de objetos e localize o valor **Real reservado**.



Na captura de tela, o valor **atual reservado** é de 8 TB. Esta captura de tela é para um nó de armazenamento grande em uma nova instalação do StorageGRID 11,6. Como a configuração espaço reservado de metadados em todo o sistema é menor que o volume 0 para este nó de armazenamento, o espaço reservado real para esse nó é igual à configuração espaço reservado de metadados.

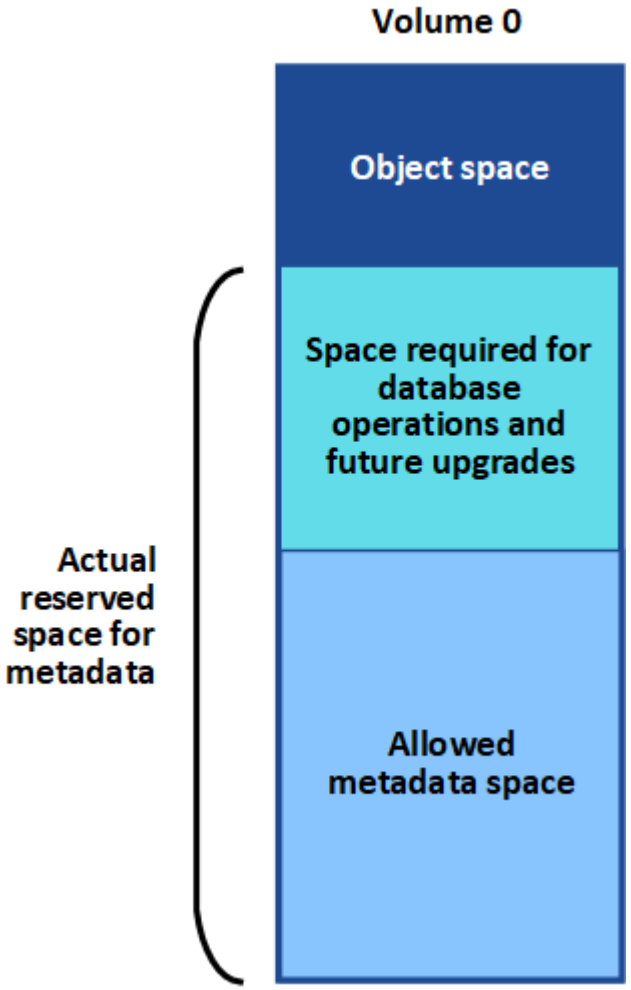
Exemplo de espaço reservado real de metadados

Suponha que você instale um novo sistema StorageGRID usando a versão 11,7 ou posterior. Para este exemplo, suponha que cada nó de armazenamento tem mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) é de 6 TB. Com base nestes valores:

- O **espaço reservado de metadados** em todo o sistema está definido para 8 TB. (Este é o valor padrão para uma nova instalação do StorageGRID 11,6 ou superior se cada nó de armazenamento tiver mais de 128 GB de RAM.)
- O espaço reservado real para metadados para SN1 é de 6 TB. (Todo o volume é reservado porque o volume 0 é menor do que a configuração **espaço reservado de metadados**.)

Espaço de metadados permitido

O espaço reservado real de cada nó de storage para metadados é subdividido no espaço disponível para metadados de objetos (o espaço de metadados permitido_) e no espaço necessário para operações essenciais de banco de dados (como compactação e reparo) e futuras atualizações de hardware e software. O espaço de metadados permitido rege a capacidade geral do objeto.



A tabela a seguir mostra como o StorageGRID calcula o espaço de metadados permitido* para diferentes nós de armazenamento, com base na quantidade de memória do nó e no espaço reservado real para metadados.

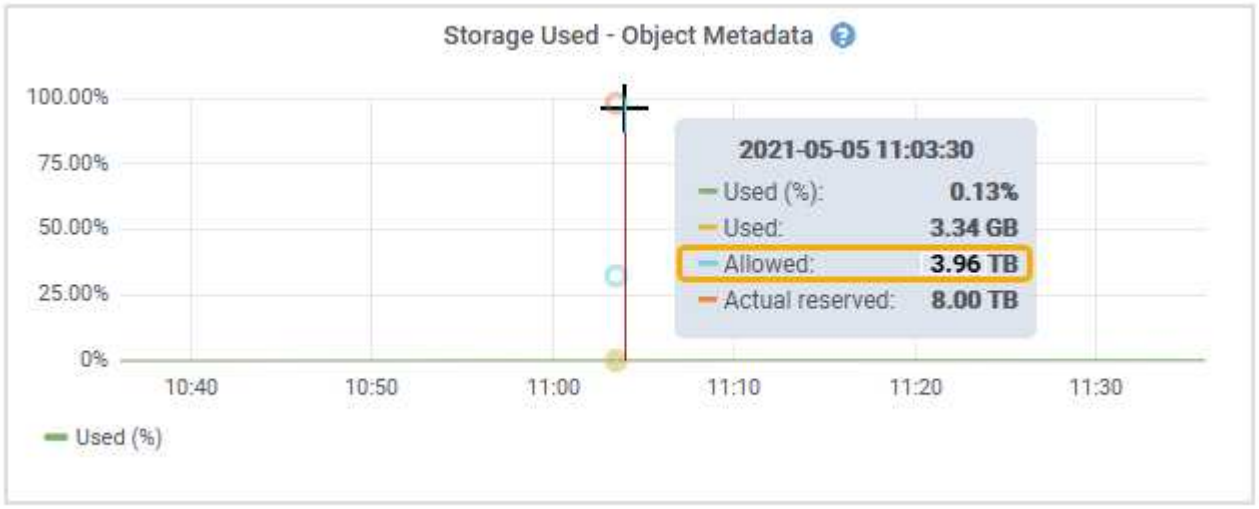
		Quantidade de memória no nó de armazenamento	
	≪ 128 GB	≫ 128 GB	**Espaço reservado real para metadados**
≪ 4 TB	60% do espaço reservado real para metadados, até um máximo de 1,32 TB	60% do espaço reservado real para metadados, até um máximo de 1,98 TB	≫ 4 TB

Exibir espaço permitido de metadados

Siga estas etapas para exibir o espaço de metadados permitido para um nó de armazenamento.

Passos

1. No Gerenciador de Grade, selecione **NÓS**.
2. Selecione o nó de armazenamento.
3. Selecione a guia **armazenamento**.
4. Posicione o cursor sobre o gráfico armazenamento usado - metadados de objetos e localize o valor **permitido**.



Na captura de tela, o valor **permitido** é de 3,96 TB, que é o valor máximo para um nó de armazenamento cujo espaço reservado real para metadados é superior a 4 TB.

O valor **allowed** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemplo de espaço permitido de metadados

Suponha que você instale um sistema StorageGRID usando a versão 11,6. Para este exemplo, suponha que

cada nó de armazenamento tem mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) é de 6 TB. Com base nestes valores:

- O **espaço reservado de metadados** em todo o sistema está definido para 8 TB. (Este é o valor padrão para o StorageGRID 11,6 ou superior quando cada nó de armazenamento tem mais de 128 GB de RAM.)
- O espaço reservado real para metadados para SN1 é de 6 TB. (Todo o volume é reservado porque o volume 0 é menor do que a configuração **espaço reservado de metadados**.)
- O espaço permitido para metadados no SN1 é de 3 TB, com base no cálculo mostrado no tabela para espaço permitido para metadados: (espaço reservado real para metadados - 1 TB) x 60%, até um máximo de 3,96 TB.

Como os nós de storage de diferentes tamanhos afetam a capacidade do objeto

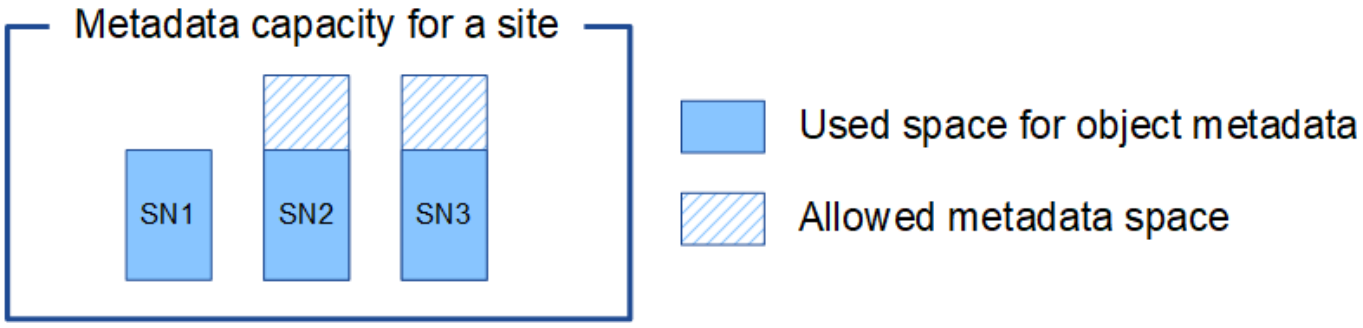
Como descrito acima, o StorageGRID distribui uniformemente os metadados de objetos nos nós de storage em cada local. Por esse motivo, se um site contiver nós de storage de tamanhos diferentes, o menor nó do local determinará a capacidade de metadados do local.

Considere o seguinte exemplo:

- Você tem uma grade de local único que contém três nós de storage de tamanhos diferentes.
- A configuração **espaço reservado de metadados** é de 4 TB.
- Os nós de storage têm os seguintes valores para o espaço de metadados reservado real e o espaço de metadados permitido.

Nó de storage	Tamanho do volume 0	Espaço reservado real de metadados	Espaço de metadados permitido
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Como os metadados de objetos são distribuídos uniformemente pelos nós de storage em um local, cada nó neste exemplo pode conter apenas 1,32 TB de metadados. Os 0,66 TB adicionais de espaço permitido de metadados para SN2 e SN3 não podem ser usados.



Da mesma forma, como o StorageGRID mantém todos os metadados de objetos para um sistema StorageGRID em cada local, a capacidade geral de metadados de um sistema StorageGRID é determinada pela capacidade de metadados de objetos do menor local.

E como a capacidade de metadados de objetos controla a contagem máxima de objetos, quando um nó fica sem capacidade de metadados, a grade fica efetivamente cheia.

Informações relacionadas

- Para saber como monitorar a capacidade de metadados de objetos para cada nó de armazenamento, consulte as instruções para "Monitorização do StorageGRID".
- Para aumentar a capacidade dos metadados de objetos do seu sistema, "expanda uma grade"adicionando novos nós de storage.

Aumentar a configuração espaço reservado metadados

Você pode aumentar a configuração do sistema Metadata Reserved Space se seus nós de armazenamento atenderem a requisitos específicos de RAM e espaço disponível.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso root ou a Configuração da Página de topologia de Grade e outras permissões de Configuração de Grade".

> A página de topologia de Grade foi obsoleta e será removida em uma versão futura.

Sobre esta tarefa

Você pode aumentar manualmente a configuração de espaço reservado de metadados em todo o sistema até 8 TB.

Você só pode aumentar o valor da configuração espaço reservado de metadados em todo o sistema se ambas as instruções forem verdadeiras:

- Os nós de storage em qualquer local do seu sistema têm 128 GB ou mais de RAM.
- Cada um dos nós de storage em qualquer local do sistema tem espaço disponível suficiente no volume de storage 0.

Esteja ciente de que, se você aumentar essa configuração, reduzirá simultaneamente o espaço disponível para storage de objetos no volume de storage 0 de todos os nós de storage. Por esse motivo, você pode preferir definir o espaço reservado de metadados para um valor menor que 8 TB, com base nos requisitos esperados de metadados de objeto.

> Em geral, é melhor usar um valor mais alto em vez de um valor mais baixo. Se a configuração espaço reservado de metadados for muito grande, você poderá diminuí-la mais tarde. Em contraste, se você aumentar o valor mais tarde, o sistema pode precisar mover dados de objeto para liberar espaço.

Para obter uma explicação detalhada de como a configuração espaço reservado metadados afeta o espaço permitido para armazenamento de metadados de objetos em um nó de armazenamento específico, "Gerenciar o storage de metadados de objetos"consulte .

Passos

1. Determine a configuração atual espaço reservado de metadados.
   a. Selecione **CONFIGURATION** > **System** > **Storage options**.
   b. Na seção Storage watermarks (marcas d'água de armazenamento), observe o valor de **Metadata**

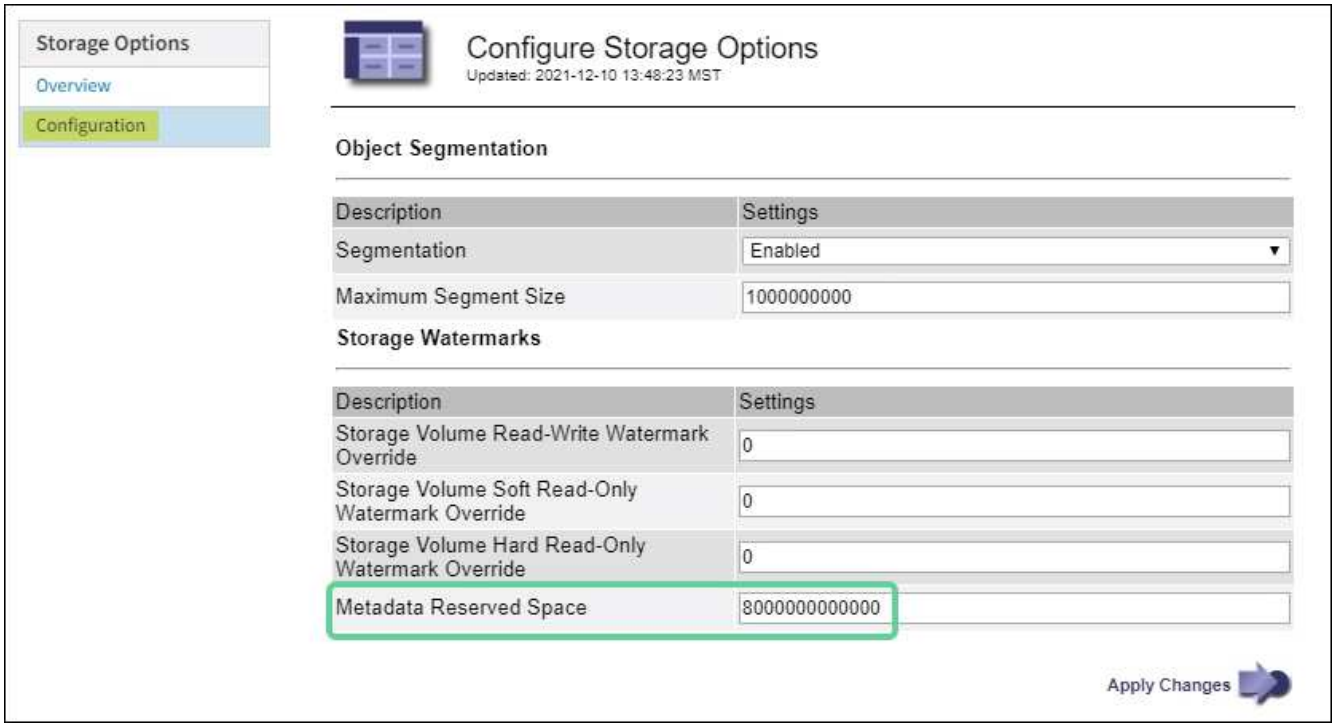
Reserved Space (espaço reservado de metadados).

2. Certifique-se de que tem espaço disponível suficiente no volume de armazenamento 0 de cada nó de armazenamento para aumentar este valor.
   a. Selecione **NODES**.
   b. Selecione o primeiro nó de armazenamento na grade.
   c. Selecione a guia armazenamento .
   d. Na seção volumes, localize a entrada **/var/local/rangedb/0**.
   e. Confirme se o valor disponível é igual ou superior à diferença entre o novo valor que pretende utilizar e o valor de espaço reservado de metadados atual.

      Por exemplo, se a configuração espaço reservado de metadados for atualmente de 4 TB e você quiser aumentá-la para 6 TB, o valor disponível deverá ser de 2 TB ou superior.

   f. Repita estas etapas para todos os nós de storage.
      - Se um ou mais nós de armazenamento não tiverem espaço disponível suficiente, o valor espaço reservado de metadados não poderá ser aumentado. Não prossiga com este procedimento.
      - Se cada nó de armazenamento tiver espaço disponível suficiente no volume 0, vá para a próxima etapa.
3. Certifique-se de que tem pelo menos 128 GB de RAM em cada nó de armazenamento.
   a. Selecione **NODES**.
   b. Selecione o primeiro nó de armazenamento na grade.
   c. Selecione a guia **hardware**.
   d. Passe o cursor sobre o gráfico de uso da memória. Certifique-se de que **Total Memory** é de pelo menos 128 GB.
   e. Repita estas etapas para todos os nós de storage.
      - Se um ou mais nós de armazenamento não tiverem memória total disponível suficiente, o valor de espaço reservado de metadados não poderá ser aumentado. Não prossiga com este procedimento.
      - Se cada nó de armazenamento tiver pelo menos 128 GB de memória total, vá para a próxima etapa.
4. Atualize a configuração espaço reservado metadados.
   a. Selecione **CONFIGURATION** > **System** > **Storage options**.
   b. Selecione o separador Configuration (Configuração).
   c. Na seção Storage watermarks (marcas d'água de armazenamento), selecione **Metadata Reserved Space** (espaço reservado de metadados).
   d. Introduza o novo valor.

      Por exemplo, para introduzir 8 TB, que é o valor máximo suportado, introduza **8000000000000** (8, seguido de 12 zeros)



a. Selecione **aplicar alterações**.

Comprimir objetos armazenados

Você pode ativar a compactação de objetos para reduzir o tamanho dos objetos armazenados no StorageGRID, para que os objetos consumam menos storage.

Antes de começar

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

Sobre esta tarefa

Por padrão, a compactação de objetos está desativada. Se você ativar a compactação, o StorageGRID tentará compactar cada objeto ao salvá-lo, usando a compactação sem perda.

> ⓘ Se alterar esta definição, demora cerca de um minuto para a nova definição ser aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

Antes de ativar a compressão de objetos, tenha em atenção o seguinte:

- Você não deve selecionar **Compress Stored Objects** a menos que você saiba que os dados que estão sendo armazenados são compressíveis.
- Os aplicativos que salvam objetos no StorageGRID podem compactar objetos antes de salvá-los. Se um aplicativo cliente já tiver compactado um objeto antes de salvá-lo no StorageGRID, selecionar essa opção não reduzirá ainda mais o tamanho de um objeto.
- Não selecione **Compress Stored Objects** se você estiver usando o NetApp FabricPool com o StorageGRID.
- Se **Compress Stored Objects** estiver selecionado, os aplicativos cliente S3 devem evitar executar operações GetObject que especificem um intervalo de bytes que sejam retornados. Essas operações de

"leitura de intervalo" são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GetObject que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

Se os intervalos forem lidos a partir de objetos compatados, as solicitações do cliente podem expirar.

> Se você precisar compactar objetos e seu aplicativo cliente precisar usar leituras de intervalo, aumente o tempo limite de leitura para o aplicativo.

Passos

1. Selecione **CONFIGURATION** > **System** > **Storage settings** > **Object Compression**.
2. Marque a caixa de seleção **Compress Stored Objects**.
3. Selecione **Guardar**.

Gerencie nós de storage completos

À medida que os nós de storage atingem a capacidade, você precisa expandir o sistema StorageGRID com a adição de um novo storage. Há três opções disponíveis: Adicionar volumes de storage, adicionar compartimentos de expansão de storage e adicionar nós de storage.

Adicione volumes de armazenamento

Cada nó de storage oferece suporte a um número máximo de volumes de storage. O máximo definido varia de acordo com a plataforma. Se um nó de armazenamento contiver menos do que o número máximo de volumes de armazenamento, pode adicionar volumes para aumentar a sua capacidade. Consulte as instruções para "Expandindo um sistema StorageGRID".

Adicione compartimentos de expansão de storage

Alguns nós de storage de dispositivos StorageGRID, como o SG6060 ou SG6160, podem dar suporte a gavetas de storage adicionais. Se você tiver dispositivos StorageGRID com funcionalidades de expansão que ainda não foram expandidas para a capacidade máxima, poderá adicionar compartimentos de storage para aumentar a capacidade. Consulte as instruções para "Expandindo um sistema StorageGRID".

Adicionar nós de storage

Você pode aumentar a capacidade de storage adicionando nós de storage. Deve-se ter em consideração cuidadosamente as regras de ILM e os requisitos de capacidade atualmente ativos ao adicionar armazenamento. Consulte as instruções para "Expandindo um sistema StorageGRID".

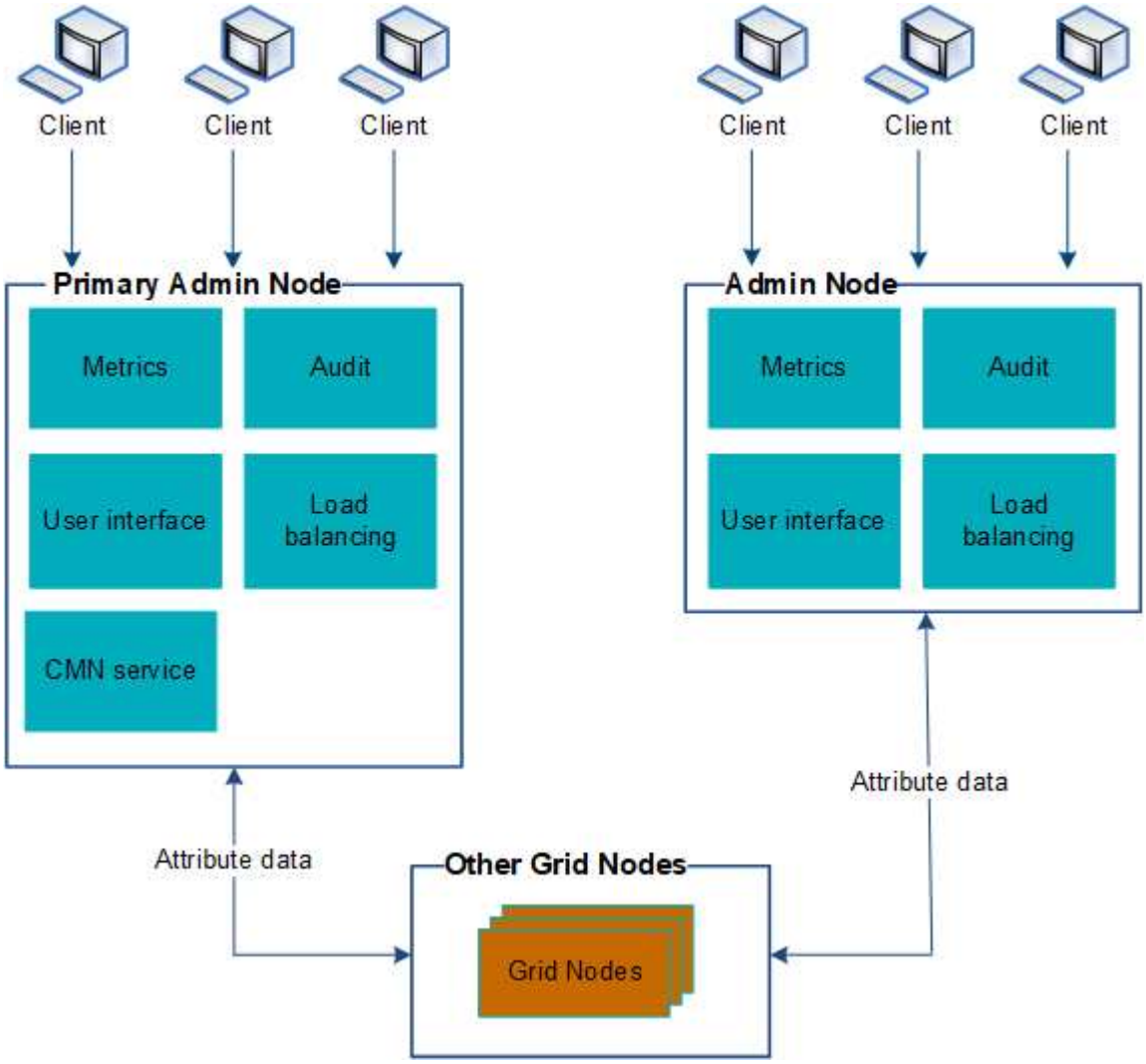
Gerenciar nós de administração

Use vários nós de administração

Um sistema StorageGRID pode incluir vários nós de administração para permitir que você monitore e configure continuamente seu sistema StorageGRID, mesmo se um nó de administração falhar.

Se um nó Admin ficar indisponível, o processamento de atributos continua, os alertas ainda são acionados e

as notificações por e-mail e os pacotes AutoSupport ainda são enviados. No entanto, ter vários nós de administração não fornece proteção contra failover, exceto notificações e pacotes de AutoSupport.



Existem duas opções para continuar a visualizar e configurar o sistema StorageGRID se um nó de administrador falhar:

- Os clientes da Web podem se reconetar a qualquer outro nó de administração disponível.
- Se um administrador do sistema tiver configurado um grupo de nós de administração de alta disponibilidade, os clientes da Web poderão continuar a aceder ao Gestor de grelha ou ao Gestor de inquilinos utilizando o endereço IP virtual do grupo HA. "Gerenciar grupos de alta disponibilidade"Consulte .

> Ao usar um grupo de HA, o acesso é interrompido se o nó Admin ativo falhar. Os usuários devem fazer login novamente após o failover do endereço IP virtual do grupo HA para outro nó Admin no grupo.

Algumas tarefas de manutenção só podem ser executadas usando o nó de administração principal. Se o nó de administração principal falhar, ele deve ser recuperado antes que o sistema StorageGRID esteja totalmente funcional novamente.

Identifique o nó de administração principal

O nó de administração principal fornece mais funcionalidade do que os nós de administração não primários. Por exemplo, alguns procedimentos de manutenção devem ser executados usando o nó de administração principal.

Para obter mais informações sobre nós de administração, "O que é um nó Admin"consulte .

Antes de começar

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

Passos

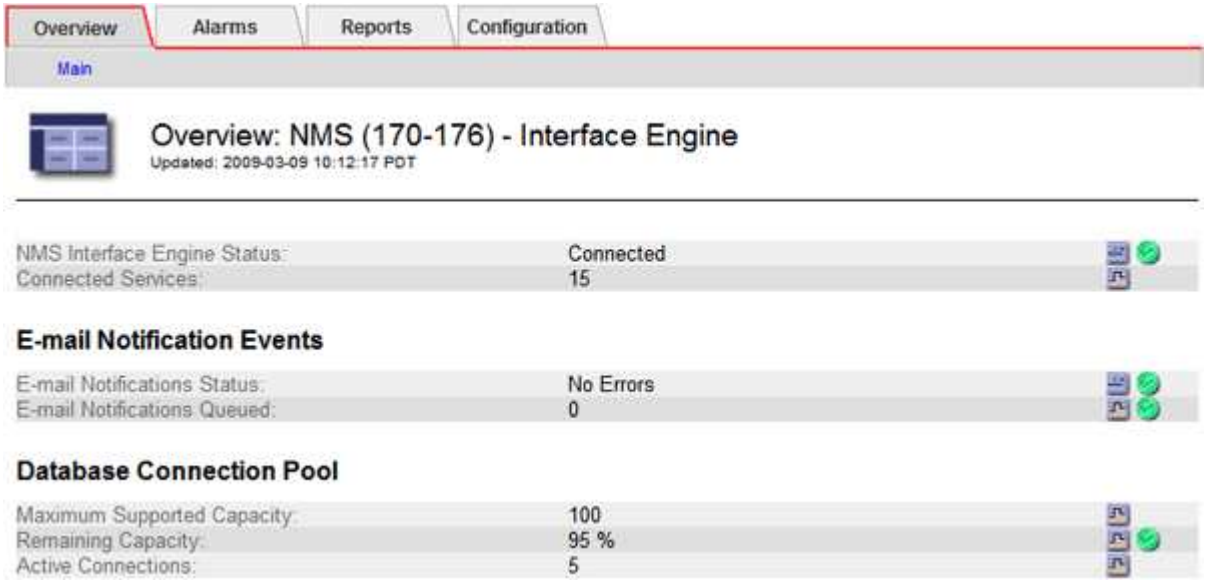
1. Selecione **NODES**.
2. Digite **Primary** na caixa de pesquisa.

   Nos resultados da pesquisa, identifique o nó com "nó Admin principal" exibido na coluna tipo. Um nó de administração principal deve ser listado.

Exibir status de notificação e filas

O serviço do sistema de gerenciamento de rede (NMS) nos nós de administração envia notificações para o servidor de e-mail. Você pode visualizar o status atual do serviço NMS e o tamanho de sua fila de notificações na página mecanismo de interface.

Para acessar a página mecanismo de interface, selecione **SUPPORT** > **Tools** > **Grid topoly**. Em seguida, selecione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



As notificações são processadas através da fila de notificações de e-mail e são enviadas para o servidor de e-mail uma após a outra na ordem em que são acionadas. Se houver um problema (por exemplo, um erro de conexão de rede) e o servidor de e-mail não estiver disponível quando a tentativa for feita para enviar a notificação, uma tentativa de reenviar a notificação para o servidor de e-mail continuará por um período de 60 segundos. Se a notificação não for enviada para o servidor de correio após 60 segundos, a notificação será retirada da fila de notificações e será feita uma tentativa de enviar a próxima notificação na fila.

Gerenciar objetos com ILM

Gerenciar objetos com ILM

As regras de gerenciamento do ciclo de vida das informações (ILM) em uma política de ILM instruem o StorageGRID a criar e distribuir cópias de dados de objetos e como gerenciar essas cópias ao longo do tempo.

Sobre estas instruções

Projetar e implementar regras e políticas de ILM requer um Planejamento cuidadoso. Você precisa entender seus requisitos operacionais, a topologia do sistema StorageGRID, suas necessidades de proteção de objetos e os tipos de storage disponíveis. Em seguida, você deve determinar como deseja que diferentes tipos de objetos sejam copiados, distribuídos e armazenados.

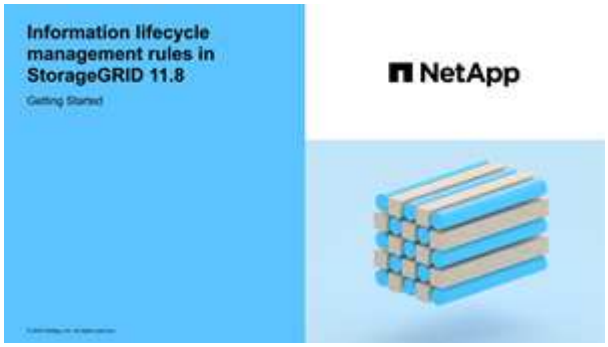
Use estas instruções para:

- Saiba mais sobre o StorageGRID ILM, "Como o ILM opera ao longo da vida de um objeto"incluindo .
- Saiba como configurar "pools de armazenamento", "Pools de storage de nuvem"e "Regras do ILM".
- Saiba como "Crie, simule e ative uma política ILM"isso protegerá os dados de objetos em um ou mais sites.
- Saiba como "Gerencie objetos com o S3 Object Lock", o que ajuda a garantir que os objetos em buckets específicos do S3 não sejam excluídos ou substituídos por um período de tempo especificado.

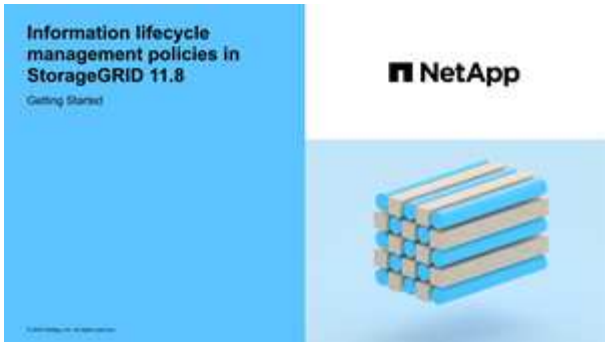
Saiba mais

Para saber mais, reveja estes vídeos:

- "Vídeo: Visão geral das regras do ILM".



- "Vídeo: Visão geral das políticas do ILM"



ILM e ciclo de vida do objeto

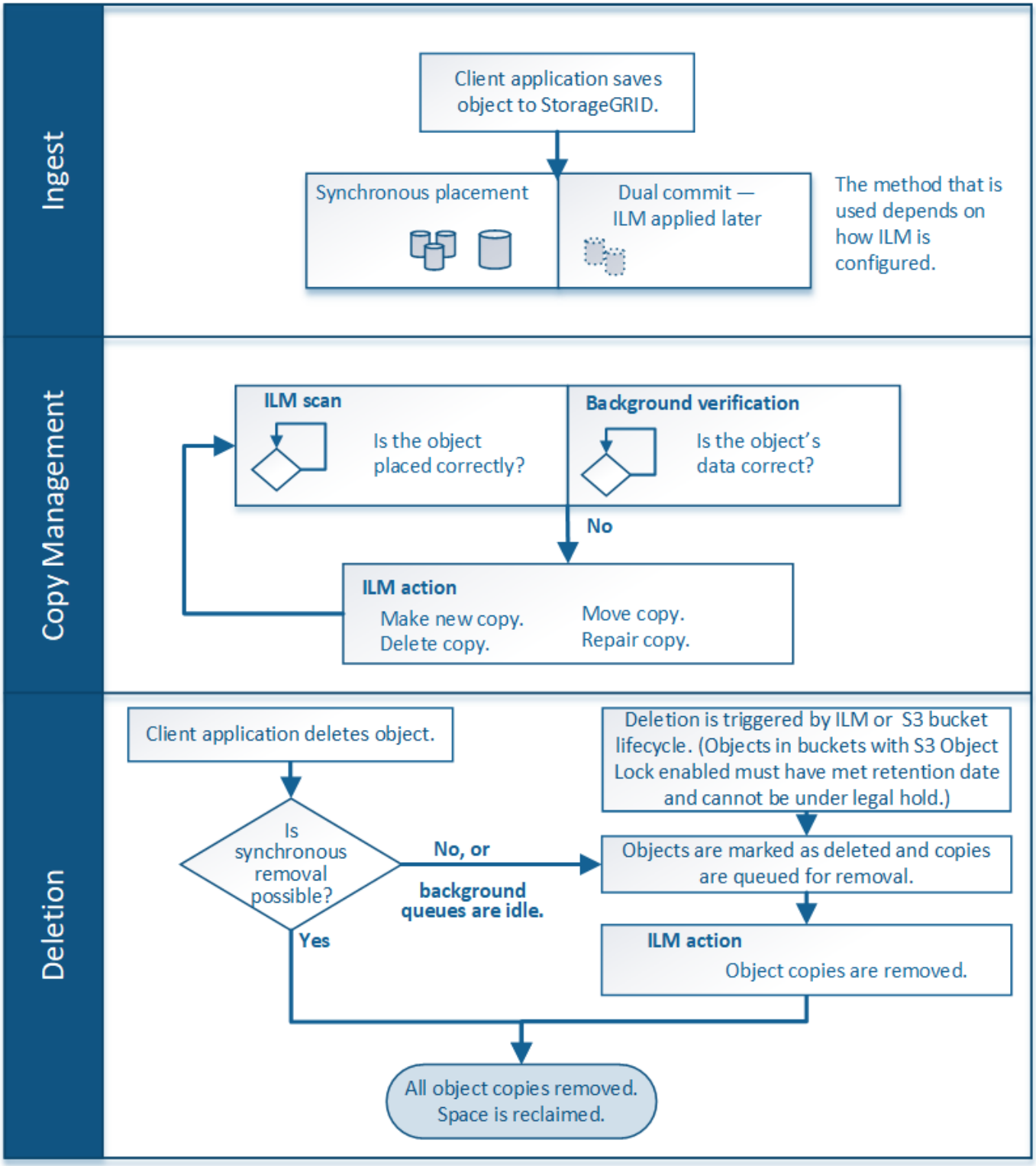
Como o ILM opera ao longo da vida de um objeto

Entender como o StorageGRID usa o ILM para gerenciar objetos durante cada estágio de sua vida pode ajudá-lo a projetar uma política mais eficaz.

- **Ingest**: Ingest começa quando um aplicativo cliente S3 estabelece uma conexão para salvar um objeto no sistema StorageGRID e é concluído quando o StorageGRID retorna uma mensagem "ingest successful" para o cliente. Os dados de objeto são protegidos durante a ingestão, aplicando instruções de ILM imediatamente (posicionamento síncrono) ou criando cópias provisórias e aplicando ILM mais tarde (commit duplo), dependendo de como os requisitos de ILM foram especificados.
- **Gerenciamento de cópias**: Depois de criar o número e o tipo de cópias de objetos especificados nas instruções de colocação do ILM, o StorageGRID gerencia locais de objetos e protege objetos contra perda.
  - * Digitalização e avaliação ILM*: O StorageGRID verifica continuamente a lista de objetos armazenados na grade e verifica se as cópias atuais atendem aos requisitos do ILM. Quando diferentes tipos, números ou locais de cópias de objetos são necessários, o StorageGRID cria, exclui ou move cópias conforme necessário.
  - * Verificação em segundo plano*: O StorageGRID realiza continuamente a verificação em segundo plano para verificar a integridade dos dados do objeto. Se um problema for encontrado, o StorageGRID criará automaticamente uma nova cópia de objeto ou um fragmento de objeto codificado de apagamento de substituição em um local que atenda aos requisitos atuais do ILM. "Verifique a integridade do objeto"Consulte .
- **Exclusão de objeto**: O gerenciamento de um objeto termina quando todas as cópias são removidas do sistema StorageGRID. Os objetos podem ser removidos como resultado de uma solicitação de exclusão por um cliente, ou como resultado de exclusão por ILM ou exclusão causada pela expiração de um ciclo de vida de bucket do S3.

> Os objetos em um bucket que tem o bloqueio de objeto S3 ativado não podem ser excluídos se estiverem sob uma retenção legal ou se uma data de retenção até tiver sido especificada, mas ainda não cumprida.

O diagrama resume como o ILM opera ao longo do ciclo de vida de um objeto.



Como os objetos são ingeridos

Opções de ingestão

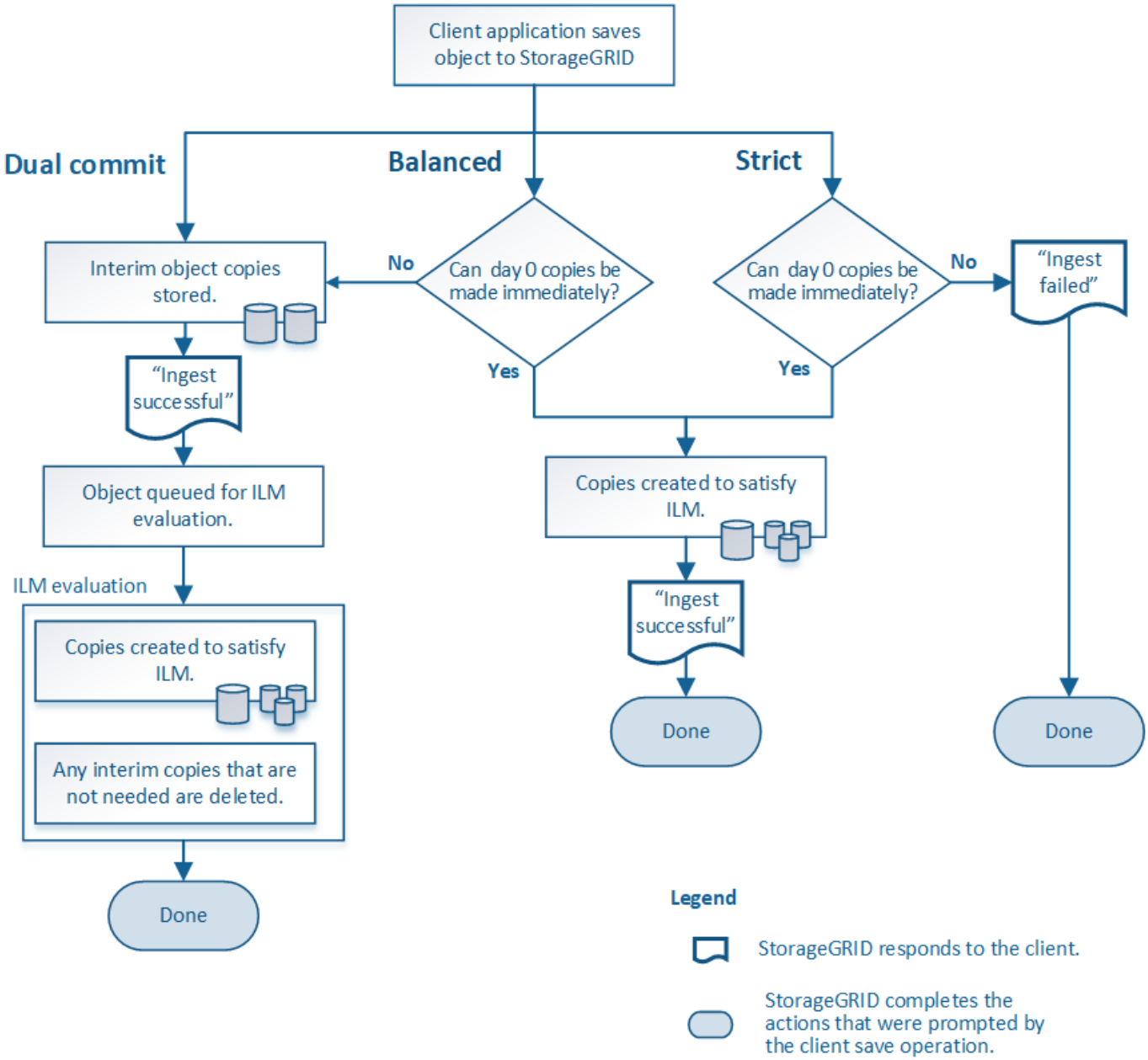
Ao criar uma regra ILM, você especifica uma das três opções para proteger objetos na ingestão: Commit duplo, estrito ou balanceado.

Dependendo de sua escolha, o StorageGRID faz cópias provisórias e coloca os objetos em fila para avaliação

do ILM mais tarde, ou usa o posicionamento síncrono e faz cópias imediatamente para atender aos requisitos do ILM.

Fluxograma das opções de ingestão

O fluxograma mostra o que acontece quando os objetos são combinados por uma regra ILM que usa cada uma das três opções de ingestão.



Commit duplo

Quando você seleciona a opção de confirmação dupla, o StorageGRID imediatamente faz cópias provisórias de objetos em dois nós de armazenamento diferentes e retorna uma mensagem de "ingestão bem-sucedida" ao cliente. O objeto é colocado em fila para avaliação ILM e cópias que atendem às instruções de colocação da regra são feitas posteriormente. Se a política de ILM não puder ser processada imediatamente após a confirmação dupla, a proteção contra perda de site pode levar algum tempo para ser alcançada.

Use a opção de confirmação dupla em qualquer um desses casos:

- Você está usando regras de ILM de vários sites e a latência de ingestão de clientes é sua principal consideração. Ao usar o Dual Commit, você deve garantir que sua grade possa executar o trabalho adicional de criar e remover as cópias de duplo commit se elas não satisfizerem o ILM. Especificamente:
  - A carga na grade deve ser baixa o suficiente para evitar um backlog ILM.
  - A grade deve ter recursos de hardware em excesso (IOPS, CPU, memória, largura de banda da rede, etc.).
- Você está usando regras ILM de vários sites e a conexão WAN entre os sites geralmente tem alta latência ou largura de banda limitada. Nesse cenário, usar a opção de confirmação dupla pode ajudar a evitar tempos limite do cliente. Antes de escolher a opção Dual Commit, você deve testar o aplicativo cliente com cargas de trabalho realistas.

Equilibrado (padrão)

Quando você seleciona a opção equilibrada, o StorageGRID também usa o posicionamento síncrono na ingestão e faz imediatamente todas as cópias especificadas nas instruções de posicionamento da regra. Em contraste com a opção estrita, se o StorageGRID não puder fazer imediatamente todas as cópias, ele usará o Dual Commit. Se a política de ILM usar colocações em vários sites e a proteção imediata contra perda de sites não puder ser alcançada, o alerta **posicionamento ILM inalcançável** é acionado.

Use a opção equilibrada para obter a melhor combinação de proteção de dados, desempenho de grade e sucesso de ingestão. Balanced é a opção padrão no assistente criar regra ILM.

Rigoroso

Quando você seleciona a opção estrita, o StorageGRID usa o posicionamento síncrono na ingestão e faz imediatamente todas as cópias de objetos especificadas nas instruções de posicionamento da regra. A ingestão falha se o StorageGRID não puder criar todas as cópias, por exemplo, porque um local de armazenamento necessário está temporariamente indisponível. O cliente deve tentar novamente a operação.

Use a opção estrita se você tiver um requisito operacional ou regulamentar para armazenar imediatamente objetos apenas nos locais descritos na regra ILM. Por exemplo, para atender a um requisito regulatório, talvez seja necessário usar a opção estrita e um filtro avançado de restrição de localização para garantir que os objetos nunca sejam armazenados em determinados data centers.

"Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"Consulte .

Vantagens, desvantagens e limitações das opções de ingestão

Compreender as vantagens e desvantagens de cada uma das três opções de proteção de dados na ingestão (equilibrada, rigorosa ou dupla confirmação) pode ajudá-lo a decidir qual escolher para uma regra ILM.

Para obter uma visão geral das opções de ingestão, "Opções de ingestão"consulte .

Vantagens das opções equilibradas e estritas

Quando comparado ao Dual Commit, que cria cópias provisórias durante a ingestão, as duas opções de posicionamento síncrono podem oferecer as seguintes vantagens:

- **Melhor segurança de dados**: Os dados do objeto são imediatamente protegidos conforme especificado nas instruções de colocação da regra ILM, que podem ser configurados para proteger contra uma ampla variedade de condições de falha, incluindo a falha de mais de um local de armazenamento. A confirmação dupla só pode proteger contra a perda de uma única cópia local.

- **Operação de grade mais eficiente**: Cada objeto é processado apenas uma vez, pois é ingerido. Como o sistema StorageGRID não precisa rastrear ou excluir cópias provisórias, há menos carga de processamento e menos espaço no banco de dados é consumido.
- * (Equilibrado) recomendado*: A opção equilibrada proporciona uma eficiência ideal de ILM. O uso da opção Balanced é recomendado, a menos que um comportamento de ingestão rigoroso seja necessário ou a grade atenda a todos os critérios para usar o Dual Commit.
- **(strict) certeza sobre locais de objetos**: A opção strict garante que os objetos são imediatamente armazenados de acordo com as instruções de colocação na regra ILM.

Desvantagens das opções equilibradas e estritas

Quando comparado ao Dual Commit, as opções equilibradas e estritas têm algumas desvantagens:

- * Maiores ingerências de clientes*: As latências de ingestão de clientes podem ser mais longas. Quando você usa as opções balanceadas ou rigorosas, uma mensagem "ingerir bem-sucedida" não será retornada ao cliente até que todos os fragmentos codificados por apagamento ou cópias replicadas sejam criados e armazenados. No entanto, os dados de objetos provavelmente alcançarão seu posicionamento final muito mais rápido.
- **(strict) taxas mais altas de falha de ingestão**: Com a opção estrita, a ingestão falha sempre que o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra ILM. Você pode ver altas taxas de falha de ingestão se um local de armazenamento necessário estiver temporariamente off-line ou se problemas de rede causarem atrasos na cópia de objetos entre sites.
- **(strict) S3 colocações de upload de várias partes podem não ser como esperado em algumas circunstâncias**: Com strict, você espera que objetos sejam colocados como descrito pela regra ILM ou para que a ingestão falhe. No entanto, com um upload multipart S3, o ILM é avaliado para cada parte do objeto à medida que ele é ingerido e para o objeto como um todo quando o upload multipart é concluído. Nas seguintes circunstâncias, isso pode resultar em colocações que são diferentes do que você espera:
  - **Se o ILM mudar enquanto um upload multipart S3 está em andamento**: Porque cada parte é colocada de acordo com a regra que está ativa quando a peça é ingerida, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multipart é concluído. Nesses casos, a ingestão do objeto não falha. Em vez disso, qualquer peça que não seja colocada corretamente é colocada na fila para reavaliação ILM e é movida para o local correto mais tarde.
  - **Quando as regras do ILM filtram no tamanho**: Ao avaliar o ILM para uma peça, o StorageGRID filtra o tamanho da peça, não o tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos de ILM para o objeto como um todo. Por exemplo, se uma regra especifica que todos os objetos de 10 GB ou maior são armazenados em DC1 enquanto todos os objetos menores são armazenados em DC2, na ingestão cada parte de 1 GB de um upload multipart de 10 partes é armazenado em DC2. Quando ILM é avaliado para o objeto, todas as partes do objeto são movidas para DC1.
- **(strict) ingest não falha quando tags de objeto ou metadados são atualizados e não é possível fazer posicionamentos recém-solicitados**: Com strict, você espera que objetos sejam colocados conforme descrito pela regra ILM ou para falha de ingestão. No entanto, quando você atualiza metadados ou tags para um objeto que já está armazenado na grade, o objeto não é reingerido. Isso significa que quaisquer alterações no posicionamento de objetos que são acionadas pela atualização não são feitas imediatamente. As alterações de posicionamento são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano. Se as alterações de posicionamento necessárias não puderem ser feitas (por exemplo, porque um local recém-solicitado não está disponível), o objeto atualizado mantém seu posicionamento atual até que as alterações de posicionamento sejam possíveis.

Limitações em posicionamentos de objetos com opções equilibradas e estritas

As opções equilibradas ou estritas não podem ser usadas para regras de ILM que tenham qualquer uma destas instruções de colocação:

- Colocação em um pool de storage de nuvem no dia 0.
- Posicionamentos em um pool de armazenamento em nuvem quando a regra tiver um tempo de criação definido pelo usuário como seu tempo de referência.

Essas restrições existem porque o StorageGRID não pode fazer cópias sincronamente para um pool de armazenamento em nuvem, e um tempo de criação definido pelo usuário pode ser resolvido até o momento.

Como as regras de ILM e a consistência interagem para afetar a proteção de dados

Tanto sua regra ILM quanto sua escolha de consistência afetam a forma como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, o comportamento de ingestão selecionado para uma regra ILM afeta o posicionamento inicial de cópias de objetos, enquanto a consistência usada quando um objeto é armazenado afeta o posicionamento inicial dos metadados de objetos. Como o StorageGRID requer acesso aos dados e metadados de um objeto para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para o comportamento de consistência e ingestão pode fornecer melhor proteção de dados iniciais e respostas do sistema mais previsíveis.

Aqui está um breve resumo dos valores de consistência que estão disponíveis no StorageGRID:

- **Todos**: Todos os nós recebem metadados de objeto imediatamente ou a solicitação falhará.
- **Strong-global**: Metadados de objetos são imediatamente distribuídos para todos os sites. Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- **Strong-site**: Metadados de objetos são imediatamente distribuídos para outros nós no site. Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
- **Read-after-novo-write**: Fornece consistência de leitura após gravação para novos objetos e consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
- **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

> Antes de selecionar um valor de consistência, "leia a descrição completa da consistência". Você deve entender os benefícios e limitações antes de alterar o valor padrão.

Exemplo de como a consistência e as regras do ILM podem interagir

Suponha que você tenha uma grade de dois locais com a seguinte regra ILM e a seguinte consistência:

- **Regra ILM**: Crie duas cópias de objeto, uma no local e outra em um local remoto. Use um comportamento rigoroso de ingestão.
- **Consistência**: Strong-global (metadados de objetos são imediatamente distribuídos para todos os sites).

Quando um cliente armazena um objeto na grade, o StorageGRID faz cópias de objeto e distribui metadados para ambos os sites antes de retornar sucesso ao cliente.

O objeto é totalmente protegido contra perda no momento da mensagem de ingestão bem-sucedida. Por exemplo, se o local for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existem no local remoto. O objeto é totalmente recuperável.

Se, em vez disso, você usou a mesma regra ILM e a consistência do site forte, o cliente pode receber uma mensagem de sucesso depois que os dados do objeto são replicados para o site remoto, mas antes que os metadados do objeto sejam distribuídos lá. Nesse caso, o nível de proteção dos metadados de objetos não corresponde ao nível de proteção dos dados de objeto. Se o site local for perdido logo após a ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Informações relacionadas

"Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"

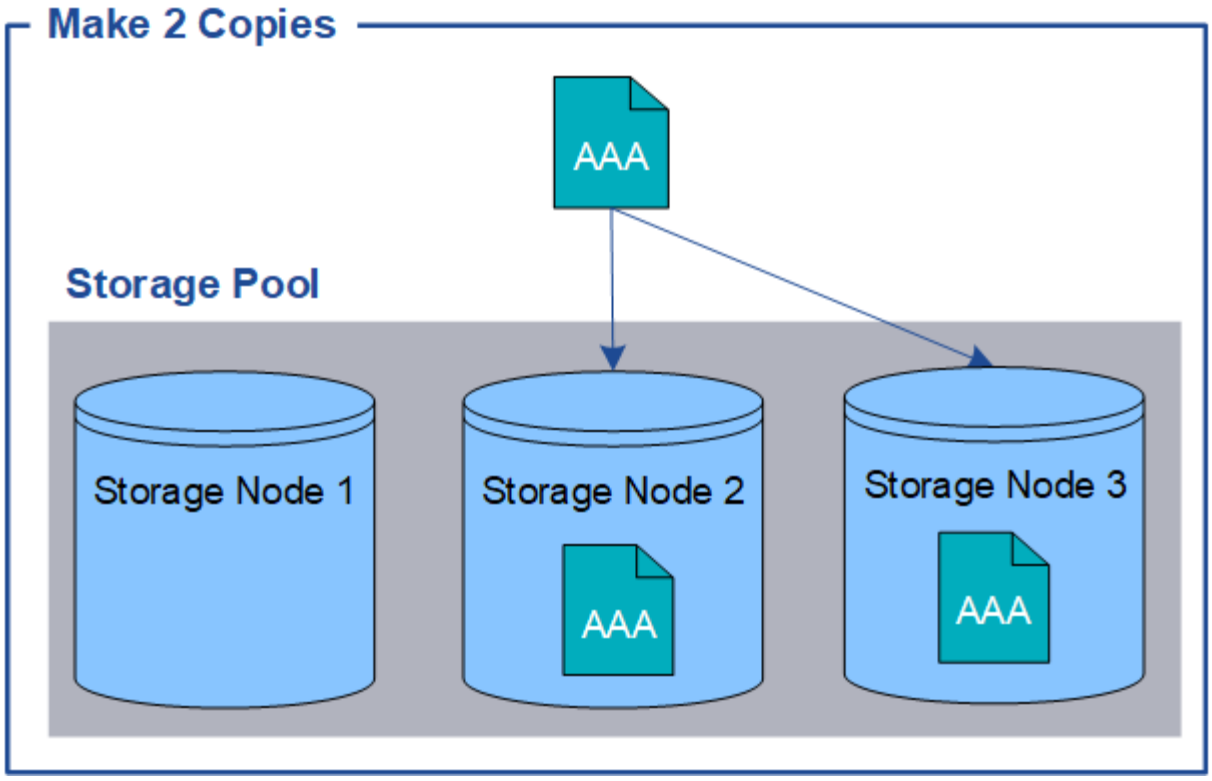
Como os objetos são armazenados (replicação ou codificação de apagamento)

O que é replicação?

A replicação é um dos dois métodos usados pelo StorageGRID para armazenar dados de objetos (a codificação de apagamento é o outro método). Quando os objetos correspondem a uma regra de ILM que usa replicação, o sistema cria cópias exatas de dados de objetos e armazena as cópias em nós de storage.

Quando você configura uma regra ILM para criar cópias replicadas, você especifica quantas cópias devem ser criadas, onde essas cópias devem ser colocadas e por quanto tempo as cópias devem ser armazenadas em cada local.

No exemplo a seguir, a regra ILM especifica que duas cópias replicadas de cada objeto serão colocadas em um pool de storage que contém três nós de storage.



Quando o StorageGRID faz a correspondência de objetos a essa regra, ele cria duas cópias do objeto, colocando cada cópia em um nó de storage diferente no pool de storage. As duas cópias podem ser colocadas em qualquer um dos três nós de storage disponíveis. Nesse caso, a regra colocou cópias de objeto nos nós de storage 2 e 3. Como há duas cópias, o objeto pode ser recuperado se algum dos nós no pool de storage falhar.

> O StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer nó de storage. Se sua grade incluir três nós de storage e você criar uma regra de ILM de 4 cópias, apenas três cópias serão feitas - uma cópia para cada nó de storage. O alerta **ILM Placement Unachievable** é acionado para indicar que a regra ILM não pôde ser completamente aplicada.

Informações relacionadas

- "O que é codificação de apagamento"
- "O que é um pool de armazenamento"
- "Habilite a proteção contra perda de site usando replicação e codificação de apagamento"

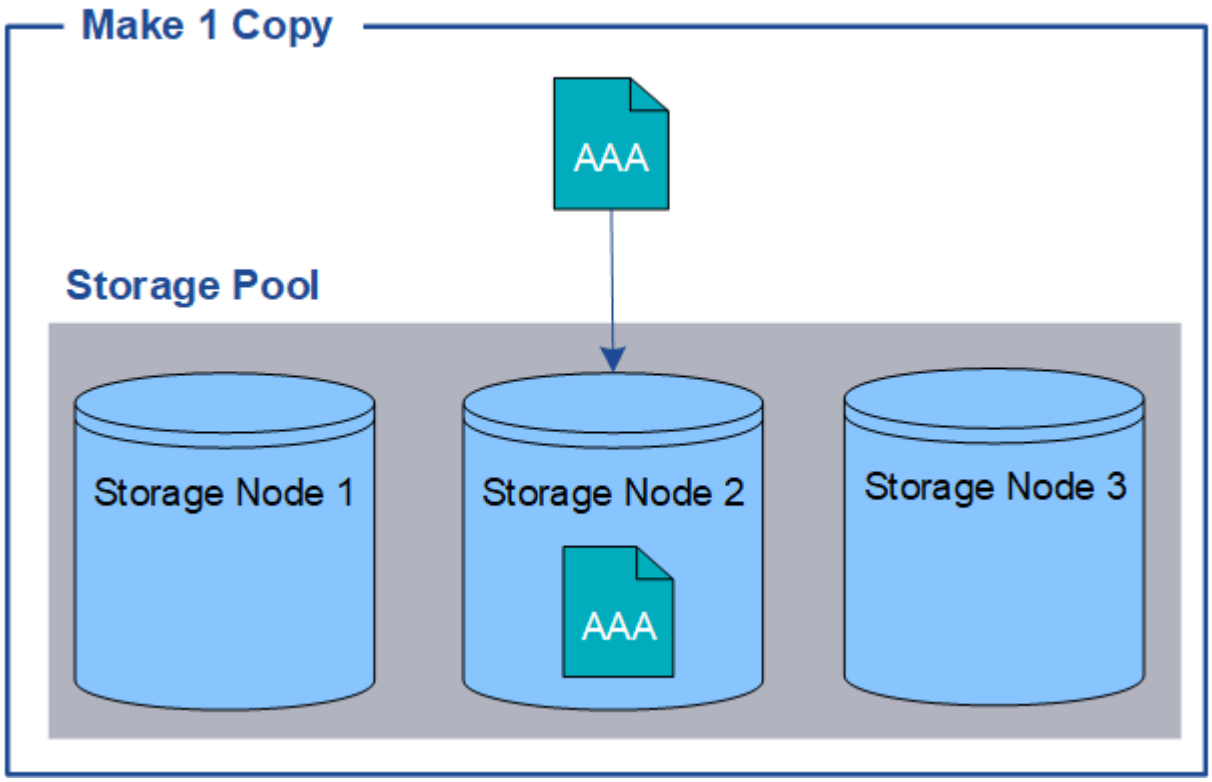
Por que você não deve usar replicação de cópia única

Ao criar uma regra ILM para criar cópias replicadas, você deve sempre especificar pelo menos duas cópias para qualquer período de tempo nas instruções de colocação.

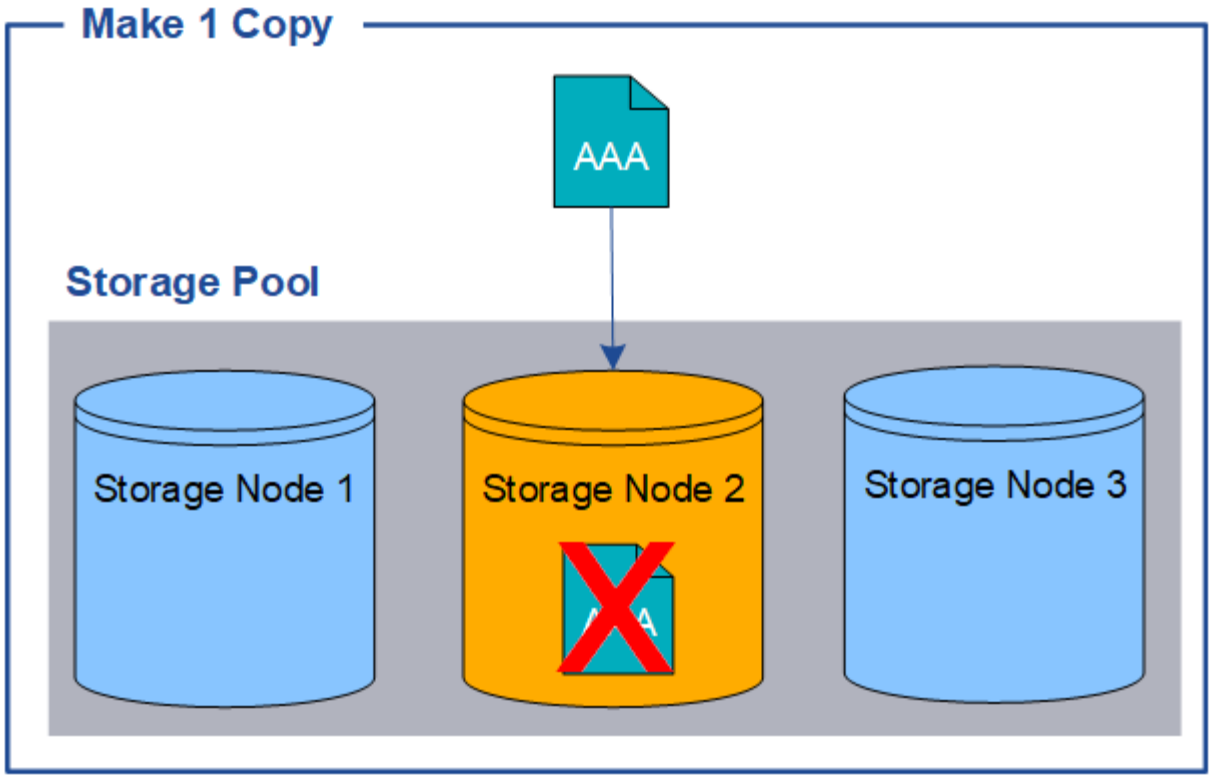
> Não use uma regra ILM que crie apenas uma cópia replicada para qualquer período de tempo. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

No exemplo a seguir, a regra Make 1 Copy ILM especifica que uma cópia replicada de um objeto seja colocada em um pool de storage que contém três nós de storage. Quando um objeto é ingerido que

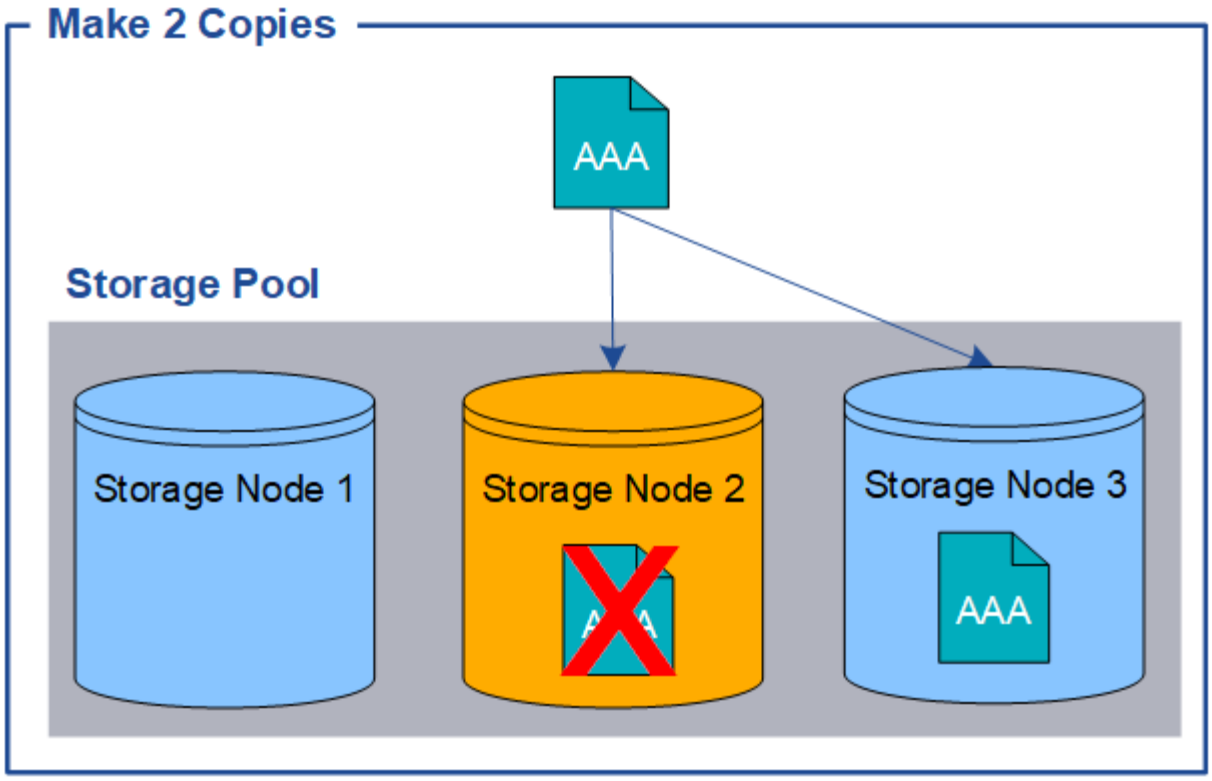
corresponde a essa regra, o StorageGRID coloca uma única cópia em apenas um nó de storage.



Quando uma regra ILM cria apenas uma cópia replicada de um objeto, o objeto fica inacessível quando o nó de armazenamento não está disponível. Neste exemplo, você perderá temporariamente o acesso ao objeto AAA sempre que o nó de armazenamento 2 estiver offline, como durante uma atualização ou outro procedimento de manutenção. Você perderá o objeto AAA inteiramente se o nó de storage 2 falhar.



Para evitar a perda de dados de objetos, você sempre deve fazer pelo menos duas cópias de todos os objetos que deseja proteger com a replicação. Se existirem duas ou mais cópias, ainda poderá aceder ao objeto se um nó de armazenamento falhar ou ficar offline.



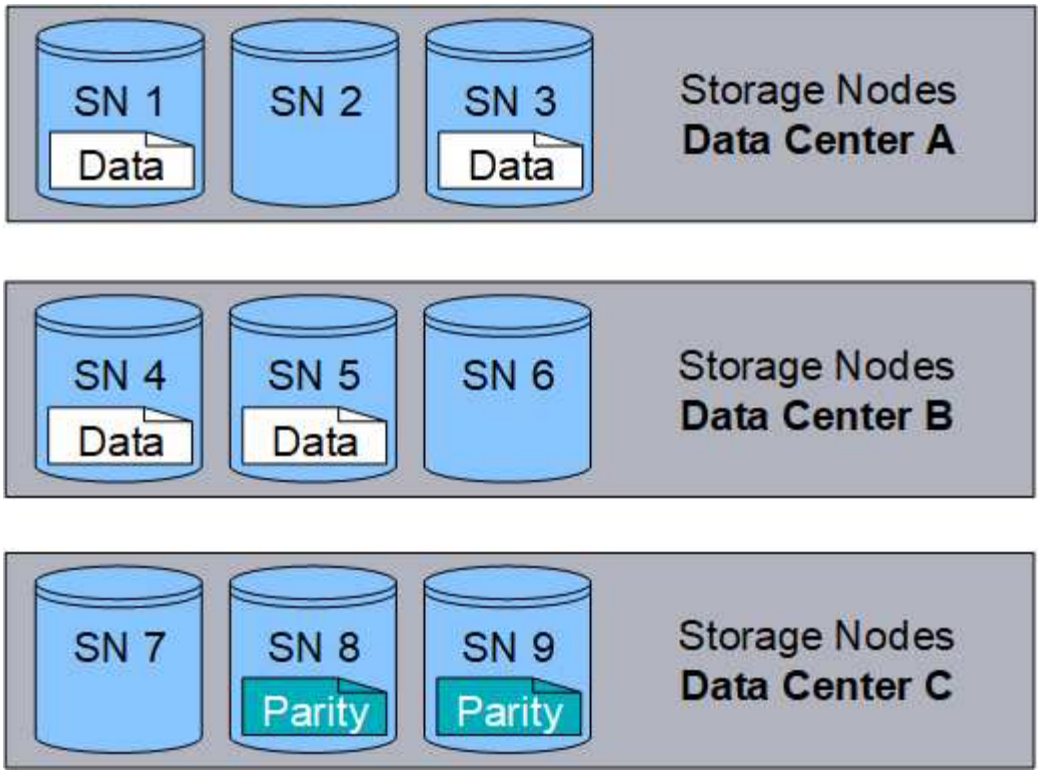
O que é codificação de apagamento?

A codificação de apagamento é um dos dois métodos que o StorageGRID usa para armazenar dados de objeto (a replicação é o outro método). Quando os objetos correspondem a uma regra ILM que usa codificação de apagamento, esses objetos são cortados em fragmentos de dados, fragmentos de paridade adicionais são computados e cada fragmento é armazenado em um nó de armazenamento diferente.

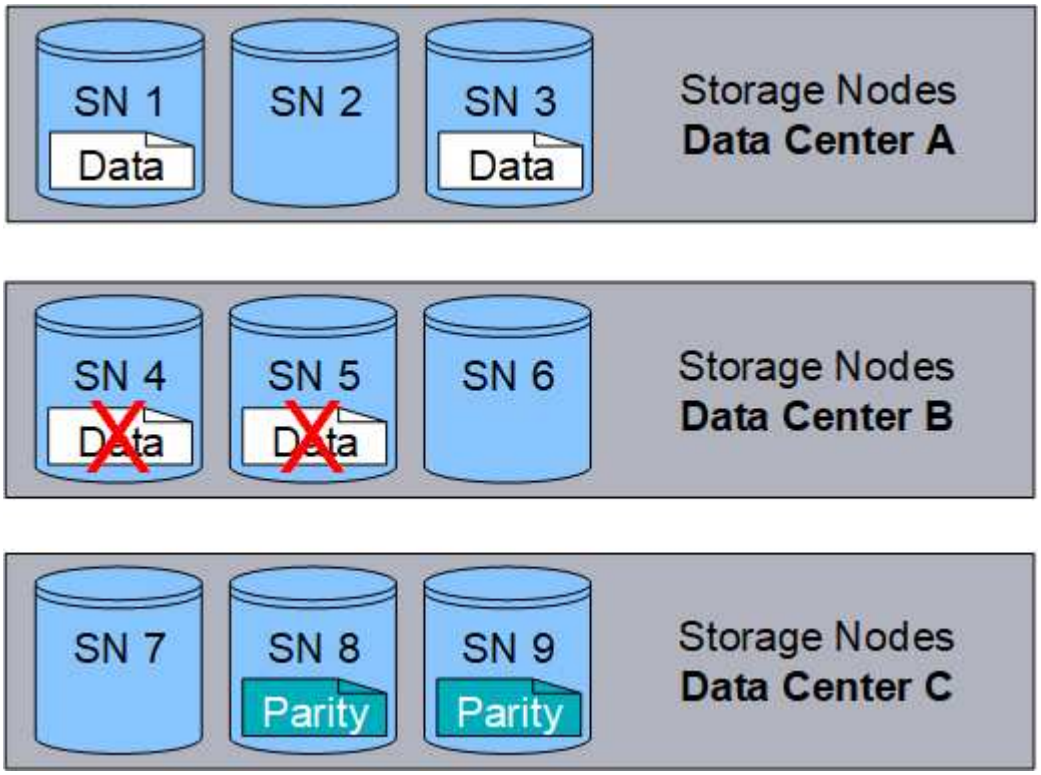
Quando um objeto é acessado, ele é remontado usando os fragmentos armazenados. Se um dado ou um fragmento de paridade ficar corrompido ou perdido, o algoritmo de codificação de apagamento pode recriar esse fragmento usando um subconjunto dos dados restantes e fragmentos de paridade.

À medida que você cria regras de ILM, o StorageGRID cria perfis de codificação de apagamento que suportam essas regras. É possível exibir uma lista de perfis de codificação de apagamento, "renomeie um perfil de codificação de apagamento", ou "Desative um perfil de codificação de apagamento se ele não for usado atualmente em nenhuma regra ILM".

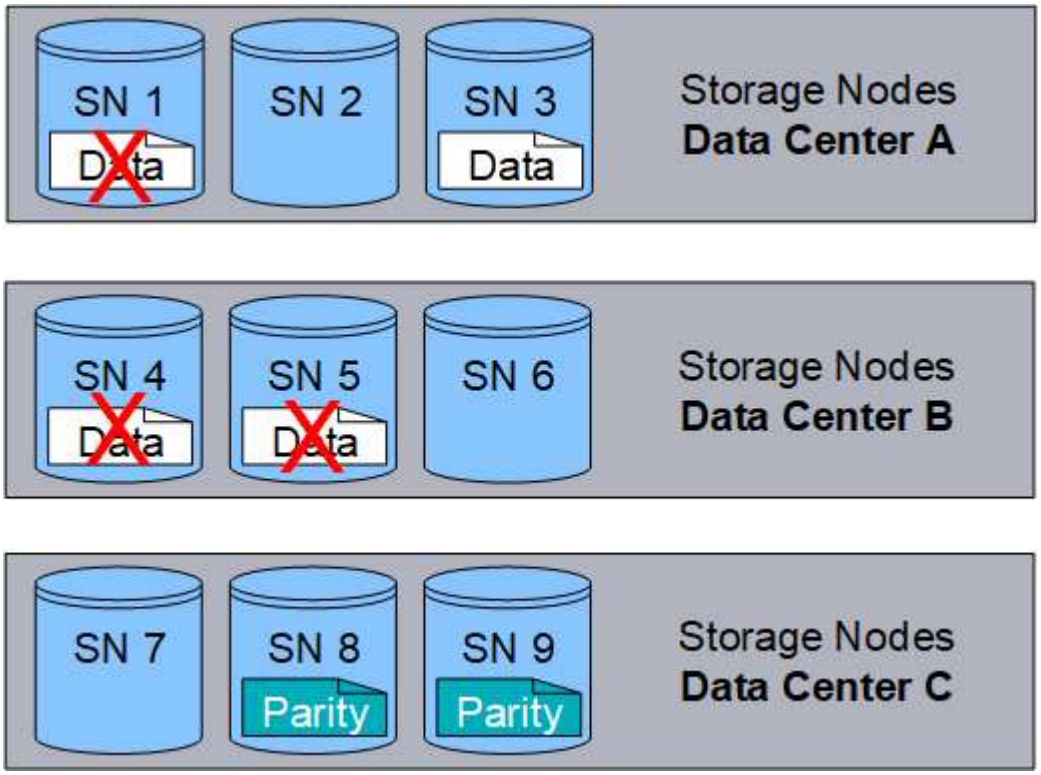
O exemplo a seguir ilustra o uso de um algoritmo de codificação de apagamento nos dados de um objeto. Neste exemplo, a regra ILM usa um esquema de codificação de apagamento 4-2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados do objeto. Cada um dos seis fragmentos é armazenado em um nó diferente em três locais de data center para fornecer proteção de dados para falhas de nós ou perda de local.



O esquema de codificação de apagamento 4-2 pode ser configurado de várias maneiras. Por exemplo, você pode configurar um pool de storage de um único local que contenha seis nós de storage. Para "proteção contra perda de local", você pode usar um pool de storage que contém três locais com três nós de storage em cada local. Um objeto pode ser recuperado desde que quaisquer quatro dos seis fragmentos (dados ou paridade) permaneçam disponíveis. Até dois fragmentos podem ser perdidos sem perda dos dados do objeto. Se um site inteiro for perdido, o objeto ainda pode ser recuperado ou reparado, desde que todos os outros fragmentos permaneçam acessíveis.



Se mais de dois nós de storage forem perdidos, o objeto não poderá ser recuperado.



Informações relacionadas

- "O que é replicação"
- "O que é um pool de armazenamento"
- "O que são esquemas de codificação de apagamento"
- "Renomeie um perfil de codificação de apagamento"
- "Desativar um perfil de codificação de apagamento"

O que são esquemas de codificação de apagamento?

Os esquemas de codificação de apagamento controlam quantos fragmentos de dados e quantos fragmentos de paridade são criados para cada objeto.

Ao criar ou editar uma regra ILM, você seleciona um esquema de codificação de apagamento disponível. O StorageGRID cria automaticamente esquemas de codificação de apagamento com base em quantos nós e sites de storage compõem o pool de storage que você planeja usar.

Proteção de dados

O sistema StorageGRID usa o algoritmo de codificação de apagamento de Reed-Solomon. O algoritmo corta um objeto em `k` fragmentos de dados e calcula `m` fragmentos de paridade.

```
`k + m = n`Os fragmentos são espalhados pelos `n` nós de storage para
fornecer proteção de dados da seguinte forma:
```

- Para recuperar ou reparar um objeto, `k` fragmentos são necessários.

- Um objeto pode sustentar até `m` fragmentos perdidos ou corrompidos. Quanto maior o valor de `m`, maior a tolerância à falha.

A melhor proteção de dados é fornecida pelo esquema de codificação de apagamento com a maior tolerância a falhas de volume ou nó em um pool de storage.

Sobrecarga de storage

A sobrecarga de armazenamento de um esquema de codificação de apagamento é calculada dividindo o número de fragmentos de paridade (`m`) pelo número de fragmentos de (`k`dados). Você pode usar a sobrecarga de storage para calcular quanto espaço em disco cada objeto com codificação de apagamento requer:

```
disk space = object size + (object size * storage overhead)
```

Por exemplo, se você armazenar um objeto de 10 MB usando o esquema 4-2 (que tem 50% de sobrecarga de armazenamento), o objeto consome 15 MB de armazenamento em grade. Se você armazenar o mesmo objeto de 10 MB usando o esquema 6-2 (que tem 33% de sobrecarga de armazenamento), o objeto consome aproximadamente 13,3 MB.

Selecione o esquema de codificação de apagamento com o menor valor total `k+m` que atenda às suas necessidades. Esquemas de codificação de apagamento com um número menor de fragmentos são mais eficientes computacionalmente porque:

- Menos fragmentos são criados e distribuídos (ou recuperados) por objeto
- Eles mostram melhor desempenho porque o tamanho do fragmento é maior
- Eles podem exigir que menos nós sejam adicionados em um "expansão quando mais armazenamento é necessário"

Diretrizes para pools de armazenamento

Ao selecionar o pool de armazenamento a ser usado para uma regra que criará uma cópia codificada por apagamento, use as seguintes diretrizes para pools de armazenamento:

- O pool de storage deve incluir três ou mais locais, ou exatamente um local.

  > Não é possível usar a codificação de apagamento se o pool de armazenamento incluir dois sites.

  - Esquemas de codificação de apagamento para pools de storage que contêm três ou mais locais
  - Esquemas de codificação de apagamento para pools de storage de um local
- Não use um pool de armazenamento que inclua o site todos os sites.
- O pool de storage deve incluir pelo menos *k+m* `+1` nós de storage que podem armazenar dados de objetos.

  > Os nós de storage podem ser configurados durante a instalação para conter apenas metadados de objetos e não dados de objetos. Para obter mais informações, "Tipos de nós de storage"consulte .

  O número mínimo de nós de storage necessário é `k+m`. No entanto, ter pelo menos um nó de armazenamento adicional pode ajudar a evitar falhas de ingestão ou backlogs de ILM se um nó de

armazenamento necessário estiver temporariamente indisponível.

Esquemas de codificação de apagamento para pools de storage que contêm três ou mais locais

A tabela a seguir descreve os esquemas de codificação de apagamento atualmente compatíveis com o StorageGRID para pools de storage que incluem três ou mais locais. Todos esses esquemas fornecem proteção contra perda de sites. Um site pode ser perdido, e o objeto ainda estará acessível.

Para esquemas de codificação de apagamento que fornecem proteção contra perda de local, o número recomendado de nós de storage no pool de storage excede `k+m +1` porque cada local requer um mínimo de três nós de storage.

Esquema de codificação de apagamento (*k*)	Número mínimo de locais implantados	Número recomendado de nós de storage em cada local	Número total recomendado de nós de storage	Proteção contra perda de site?	Sobrecarga de storage
4-2	3	3	9	Sim	50%
6-2	4	3	12	Sim	33%
8-2	5	3	15	Sim	25%
6-+3	3	4	12	Sim	50%
9-+3	4	4	16	Sim	33%
2-+1	3	3	9	Sim	50%
4-+1	5	3	15	Sim	25%
6-+1	7	3	21	Sim	17%
7-+5	3	5	15	Sim	71%

> O StorageGRID requer um mínimo de três nós de storage por local. Para usar o esquema 7-5, cada local requer um mínimo de quatro nós de storage. Recomenda-se o uso de cinco nós de storage por local.

Ao selecionar um esquema de codificação de apagamento que forneça proteção do site, equilibre a importância relativa dos seguintes fatores:

- **Número de fragmentos**: Desempenho e flexibilidade de expansão são geralmente melhores quando o número total de fragmentos é menor.
- **Tolerância a falhas**: A tolerância a falhas é aumentada por ter mais segmentos de paridade (ou seja, `m` quando tem um valor mais alto).
- **Tráfego de rede**: Ao recuperar de falhas, usar um esquema com mais fragmentos (ou seja, um total maior para `k+m`) cria mais tráfego de rede.

- * Sobrecarga de armazenamento*: Esquemas com maior sobrecarga requerem mais espaço de armazenamento por objeto.

Por exemplo, ao decidir entre um esquema 4-2 e um esquema 6-3 (que ambos têm uma sobrecarga de armazenamento de 50%), selecione o esquema 6-3 se for necessária uma tolerância de falha adicional. Selecione o esquema 4-2 se os recursos de rede forem restritos. Se todos os outros fatores forem iguais, selecione 4-2 porque ele tem um número total menor de fragmentos.

Se você não tiver certeza de qual esquema usar, selecione 4 3 ou 2 ou 6 ou entre em Contato com o suporte técnico.

Esquemas de codificação de apagamento para pools de storage de um local

Um pool de storage de um local dá suporte a todos os esquemas de codificação de apagamento definidos para três ou mais locais, desde que o local tenha nós de storage suficientes.

O número mínimo de nós de storage necessário é `k+m`, mas é recomendável usar um pool de storage com `k+m +1` nós de storage. Por exemplo, o esquema de codificação de apagamento 2 mais de 1 requer um pool de storage com no mínimo três nós de storage, mas quatro nós de storage são recomendados.

Esquema de codificação de apagamento (*k*)	Número mínimo de nós de storage	Número recomendado de nós de storage	Sobrecarga de storage
4-2	6	7	50%
6-2	8	9	33%
8-2	10	11	25%
6-+3	9	10	50%
9-+3	12	13	33%
2-+1	3	4	50%
4-+1	5	6	25%
6-+1	7	8	17%
7-+5	12	13	71%

Vantagens, desvantagens e requisitos para codificação de apagamento

Antes de decidir se deve usar a replicação ou a codificação de apagamento para proteger os dados do objeto contra perda, você deve entender as vantagens, desvantagens e os requisitos para codificação de apagamento.

Vantagens da codificação de apagamento

Em comparação com a replicação, a codificação de apagamento oferece maior confiabilidade, disponibilidade e eficiência de storage.

- **Confiabilidade**: A confiabilidade é medida em termos de tolerância a falhas - ou seja, o número de falhas simultâneas que podem ser sustentadas sem perda de dados. Com a replicação, várias cópias idênticas são armazenadas em nós diferentes e em locais diferentes. Com a codificação de apagamento, um objeto é codificado em dados e fragmentos de paridade e distribuído em muitos nós e sites. Essa dispersão fornece proteção contra falha de local e nó. Em comparação com a replicação, a codificação de apagamento oferece maior confiabilidade a custos de storage comparáveis.
- **Disponibilidade**: A disponibilidade pode ser definida como a capacidade de recuperar objetos se os nós de armazenamento falharem ou ficarem inacessíveis. Em comparação com a replicação, a codificação de apagamento oferece maior disponibilidade a custos de storage comparáveis.
- **Eficiência de storage**: Para níveis semelhantes de disponibilidade e confiabilidade, os objetos protegidos por meio da codificação de apagamento consomem menos espaço em disco do que os mesmos objetos se protegidos por meio da replicação. Por exemplo, um objeto de 10 MB replicado para dois locais consome 20 MB de espaço em disco (duas cópias), enquanto um objeto codificado por apagamento em três locais com um esquema de codificação de apagamento 6-3 consome apenas 15 MB de espaço em disco.

> ⓘ O espaço em disco para objetos codificados por apagamento é calculado como o tamanho do objeto, além da sobrecarga de storage. A porcentagem de sobrecarga de storage é o número de fragmentos de paridade divididos pelo número de fragmentos de dados.

Desvantagens da codificação de apagamento

Quando comparada à replicação, a codificação de apagamento tem as seguintes desvantagens:

- Recomenda-se um número maior de nós e sites de storage, dependendo do esquema de codificação de apagamento. Em contraste, se você replicar dados de objeto, precisará de apenas um nó de storage para cada cópia. "Esquemas de codificação de apagamento para pools de storage que contêm três ou mais locais"Consulte e "Esquemas de codificação de apagamento para pools de storage de um local".
- Aumento do custo e complexidade das expansões de armazenamento. Para expandir uma implantação que usa replicação, você adiciona capacidade de storage em todos os locais onde são feitas cópias de objetos. Para expandir uma implantação que usa codificação de apagamento, você deve considerar tanto o esquema de codificação de apagamento em uso quanto o número total de nós de storage existentes. Por exemplo, se você esperar até que os nós existentes estejam 100% cheios, será necessário adicionar pelo menos `k+m` nós de storage. No entanto, se você expandir quando os nós existentes estiverem 70% cheios, poderá adicionar dois nós por local e ainda maximizar a capacidade de storage utilizável. Para obter mais informações, "Adicionar capacidade de storage para objetos codificados por apagamento"consulte .
- Há maiores latências de recuperação quando você usa codificação de apagamento em sites distribuídos geograficamente. Os fragmentos de objeto para um objeto que é codificado por apagamento e distribuído entre locais remotos levam mais tempo para recuperar conexões WAN do que um objeto que é replicado e disponível localmente (o mesmo local ao qual o cliente se coneta).
- Quando você usa codificação de apagamento em sites distribuídos geograficamente, há maior uso de tráfego de rede WAN para recuperações e reparos, especialmente para objetos recuperados com frequência ou para reparos de objetos em conexões de rede WAN.
- Quando você usa codificação de apagamento em todos os sites, a taxa de transferência máxima de objetos diminui drasticamente à medida que a latência de rede entre sites aumenta. Esta diminuição deve-

se à diminuição correspondente da taxa de transferência da rede TCP, que afeta a rapidez com que o sistema StorageGRID pode armazenar e recuperar fragmentos de objeto.

- Maior uso de recursos de computação.

Quando usar codificação de apagamento

A codificação de apagamento é mais adequada para os seguintes requisitos:

- Objetos com mais de 1 MB de tamanho.

> A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.

- Armazenamento a longo prazo ou a frio para conteúdo pouco recuperado.
- Alta disponibilidade e confiabilidade de dados.
- Proteção contra falhas completas no local e no nó.
- Eficiência de storage.
- Implantações de um único local que exigem proteção de dados eficiente com apenas uma cópia codificada de apagamento em vez de várias cópias replicadas.
- Implantações de vários locais em que a latência entre locais é inferior a 100 ms.

Como a retenção de objetos é determinada

O StorageGRID fornece opções para administradores de grade e usuários individuais de locatários especificarem por quanto tempo armazenar objetos. Em geral, todas as instruções de retenção fornecidas por um usuário locatário têm precedência sobre as instruções de retenção fornecidas pelo administrador da grade.

Como os usuários do locatário controlam a retenção de objetos

Os usuários do locatário podem usar esses métodos para controlar por quanto tempo seus objetos são armazenados no StorageGRID:

- Se a configuração global S3 Object Lock estiver ativada para a grade, os usuários do locatário S3 poderão criar buckets com o S3 Object Lock ativado e, em seguida, selecionar um **período de retenção padrão** para cada bucket.
- Se a configuração global S3 Object Lock estiver ativada para a grade, os usuários do locatário S3 poderão criar buckets com o S3 Object Lock ativado e, em seguida, usar a API REST S3 para especificar as configurações de retenção de data e retenção legal para cada versão de objeto adicionada a esse bucket.
  - Uma versão de objeto que está sob uma retenção legal não pode ser excluída por nenhum método.
  - Antes que a data de retenção de uma versão de objeto seja alcançada, essa versão não pode ser excluída por nenhum método.
  - Objetos em buckets com o S3 Object Lock ativado são retidos pelo ILM "Forever". No entanto, após a data de retenção ser alcançada, uma versão de objeto pode ser excluída por uma solicitação de cliente ou pela expiração do ciclo de vida do bucket. "Gerencie objetos com o S3 Object Lock"Consulte .
- S3 os usuários de locatários podem adicionar uma configuração de ciclo de vida aos buckets que

especifica uma ação de expiração. Se existir um ciclo de vida de bucket, o StorageGRID armazena um objeto até que a data ou o número de dias especificados na ação de expiração sejam atendidos, a menos que o cliente exclua o objeto primeiro. "Crie a configuração do ciclo de vida do S3"Consulte .

- Um cliente S3 pode emitir uma solicitação de exclusão de objeto. O StorageGRID sempre prioriza solicitações de exclusão de clientes ao longo do ciclo de vida do bucket S3 ou ILM ao determinar se deseja excluir ou reter um objeto.

Como os administradores de grade controlam a retenção de objetos

Os administradores de grade podem usar esses métodos para controlar a retenção de objetos:

- Defina um período de retenção máximo de bloqueio de objetos S3D para cada locatário. Em seguida, os usuários do locatário podem definir um período de retenção padrão para cada um de seus buckets. O período máximo de retenção também é aplicado em quaisquer objetos recém-ingeridos para esse bucket (data de retenção do objeto até a data).
- Crie instruções de posicionamento ILM para controlar quanto tempo objetos são armazenados. Quando os objetos são correspondidos por uma regra ILM, o StorageGRID armazena esses objetos até que o último período de tempo na regra ILM tenha decorrido. Os objetos são mantidos indefinidamente se "para sempre" for especificado para as instruções de colocação.
- Independentemente de quem controla por quanto tempo os objetos são retidos, as configurações do ILM controlam quais tipos de cópias de objetos (replicadas ou codificadas para apagamento) são armazenadas e onde as cópias estão localizadas (nós de storage ou pools de storage em nuvem).

Como o ciclo de vida do bucket do S3 e o ILM interagem

Quando um ciclo de vida do bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política do ILM para objetos que correspondem ao filtro do ciclo de vida. Como resultado, um objeto pode ser retido na grade mesmo depois que quaisquer instruções ILM para colocar o objeto tenham expirado.

Exemplos para retenção de objetos

Para entender melhor as interações entre o bloqueio de objetos S3, as configurações do ciclo de vida do bucket, as solicitações de exclusão do cliente e o ILM, considere os exemplos a seguir.

Exemplo 1: O ciclo de vida do bucket S3 mantém objetos mais longos do que o ILM

ILM

Armazenar duas cópias por 1 ano (365 dias)

Ciclo de vida do balde

Expira objetos em 2 anos (730 dias)

Resultado

O StorageGRID armazena o objeto por 730 dias. O StorageGRID usa as configurações do ciclo de vida do bucket para determinar se deseja excluir ou reter um objeto.

> ⓘ Se o ciclo de vida do bucket especificar que os objetos devem ser mantidos por mais tempo do que o especificado pelo ILM, o StorageGRID continuará a usar as instruções de colocação do ILM ao determinar o número e o tipo de cópias a armazenar. Neste exemplo, duas cópias do objeto continuarão sendo armazenadas no StorageGRID de dias 366 a 730.

Exemplo 2: O ciclo de vida do bucket S3 expira objetos antes do ILM

ILM

Armazenar duas cópias por 2 anos (730 dias)

Ciclo de vida do balde

Expira objetos em 1 ano (365 dias)

Resultado

O StorageGRID exclui ambas as cópias do objeto após o dia 365.

Exemplo 3: A exclusão do cliente substitui o ciclo de vida do bucket e o ILM

ILM

Armazenar duas cópias em nós de storage "para sempre"

Ciclo de vida do balde

Expira objetos em 2 anos (730 dias)

Solicitação de exclusão do cliente

Emitido no dia 400

Resultado

O StorageGRID exclui ambas as cópias do objeto no dia 400 em resposta à solicitação de exclusão do cliente.

Exemplo 4: S3 Object Lock substitui a solicitação de exclusão do cliente

S3 bloqueio de objetos

Reter-até-data para uma versão de objeto é 2026-03-31. Uma retenção legal não está em vigor.

Regra ILM compatível

Armazenar duas cópias em nós de storage "para sempre"

Solicitação de exclusão do cliente

Emitido em 2024-03-31

Resultado

O StorageGRID não excluirá a versão do objeto porque a data de retenção ainda está a 2 anos de distância.

Como os objetos são excluídos

O StorageGRID pode excluir objetos em resposta direta a uma solicitação de cliente ou automaticamente como resultado da expiração de um ciclo de vida de bucket do S3 ou dos requisitos da política do ILM. Entender as diferentes maneiras pelas quais os objetos podem ser excluídos e como o StorageGRID lida com solicitações de exclusão pode ajudar você a gerenciar objetos com mais eficiência.

O StorageGRID pode usar um dos dois métodos para excluir objetos:

- Exclusão síncrona: Quando o StorageGRID recebe uma solicitação de exclusão de cliente, todas as cópias de objeto são removidas imediatamente. O cliente é informado de que a exclusão foi bem-sucedida após as cópias terem sido removidas.
- Os objetos são enfileirados para exclusão: Quando o StorageGRID recebe uma solicitação de exclusão, o objeto é enfileirado para exclusão e o cliente é informado imediatamente de que a exclusão foi bem-sucedida. Cópias de objeto são removidas posteriormente pelo processamento ILM em segundo plano.

Ao excluir objetos, o StorageGRID usa o método que otimiza o desempenho de exclusão, minimiza possíveis backlogs de exclusão e libera espaço mais rapidamente.

A tabela resume quando o StorageGRID usa cada método.

Método de execução da exclusão	Quando utilizado
Os objetos estão na fila para exclusão	Quando **qualquer** das seguintes condições for verdadeira: • A exclusão automática de objetos foi acionada por um dos seguintes eventos: ◦ A data de expiração ou o número de dias na configuração do ciclo de vida de um bucket do S3 é atingida. ◦ O último período de tempo especificado em uma regra ILM decorre. **Observação:** objetos em um bucket que tenha o bloqueio de objeto S3 ativado não podem ser excluídos se estiverem sob uma retenção legal ou se uma data de retenção até tiver sido especificada, mas ainda não cumprida. • Um cliente S3 solicita a exclusão e uma ou mais destas condições é verdadeira: ◦ As cópias não podem ser excluídas dentro de 30 segundos porque, por exemplo, um local de objeto está temporariamente indisponível. ◦ As filas de exclusão em segundo plano estão ociosas.
Os objetos são removidos imediatamente (exclusão síncrona)	Quando um cliente S3 faz uma solicitação de exclusão e **todas** das seguintes condições são atendidas: • Todas as cópias podem ser removidas dentro de 30 segundos. • As filas de exclusão em segundo plano contêm objetos a serem processados.

Quando os clientes S3 fazem solicitações de exclusão, o StorageGRID começa adicionando objetos à fila de exclusão. Em seguida, ele alterna para executar a exclusão síncrona. Certificar-se de que a fila de exclusão em segundo plano tem objetos para processar permite que o StorageGRID processe exclusões de forma mais eficiente, especialmente para clientes de baixa simultaneidade, ao mesmo tempo que ajuda a impedir que o cliente exclua backlogs.

Tempo necessário para excluir objetos

A forma como o StorageGRID exclui objetos pode afetar o desempenho do sistema:

- Quando o StorageGRID executa a exclusão síncrona, pode levar StorageGRID até 30 segundos para retornar um resultado ao cliente. Isso significa que a exclusão pode parecer estar acontecendo mais lentamente, mesmo que as cópias estejam sendo removidas mais rapidamente do que quando o

StorageGRID coloca objetos em fila para exclusão.

- Se você estiver monitorando de perto o desempenho de exclusão durante uma exclusão em massa, você pode notar que a taxa de exclusão parece ser lenta após um certo número de objetos ter sido excluído. Essa alteração ocorre quando o StorageGRID muda de enfileirar objetos para exclusão para a execução da exclusão síncrona. A aparente redução na taxa de exclusão não significa que as cópias de objetos estejam sendo removidas mais lentamente. Pelo contrário, indica que, em média, o espaço está agora a ser libertado mais rapidamente.

Se você estiver excluindo grandes números de objetos e sua prioridade for liberar espaço rapidamente, considere usar uma solicitação de cliente para excluir objetos em vez de excluí-los usando ILM ou outros métodos. Em geral, o espaço é liberado mais rapidamente quando a exclusão é realizada pelos clientes porque o StorageGRID pode usar a exclusão síncrona.

A quantidade de tempo necessário para liberar espaço depois que um objeto é excluído depende de vários fatores:

- Se as cópias de objetos são removidas de forma síncrona ou estão em fila para serem removidas posteriormente (para solicitações de exclusão de clientes).
- Outros fatores, como o número de objetos na grade ou a disponibilidade de recursos da grade quando as cópias de objetos são enfileiradas para remoção (para exclusões de clientes e outros métodos).

Como objetos com versão S3 são excluídos

Quando o controle de versão está habilitado para um bucket do S3, o StorageGRID segue o comportamento do Amazon S3 ao responder a solicitações de exclusão, sejam elas provenientes de um cliente S3, a expiração de um ciclo de vida de bucket do S3 ou os requisitos da política do ILM.

Quando os objetos são versionados, as solicitações de exclusão de objetos não excluem a versão atual do objeto e não libertam espaço. Em vez disso, uma solicitação de exclusão de objeto cria um marcador de exclusão de byte zero como a versão atual do objeto, o que torna a versão anterior do objeto "não atual". Um marcador de exclusão de objeto torna-se um marcador de exclusão de objeto expirado quando é a versão atual e não há versões não atuais.

Mesmo que o objeto não tenha sido removido, o StorageGRID se comporta como se a versão atual do objeto não estivesse mais disponível. Solicitações para esse objeto retornam 404 NotFound. No entanto, como os dados de objetos não atuais não foram removidos, as solicitações que especificam uma versão não atual do objeto podem ser bem-sucedidas.

Para liberar espaço ao excluir objetos com controle de versão ou remover marcadores de exclusão, use um dos seguintes procedimentos:

- **Solicitação de cliente S3**: Especifique o ID da versão do objeto na solicitação DE EXCLUSÃO de objeto S3 (`DELETE /object?versionId=ID`). Tenha em mente que essa solicitação só remove cópias de objetos para a versão especificada (as outras versões ainda estão ocupando espaço).
- **Ciclo de vida do bucket**: Use a `NoncurrentVersionExpiration` ação na configuração do ciclo de vida do bucket. Quando o número de dias não-correntes especificado é atendido, o StorageGRID remove permanentemente todas as cópias de versões de objetos não-atuais. Essas versões de objeto não podem ser recuperadas.

  A `NewerNoncurrentVersions` ação na configuração do ciclo de vida do bucket especifica o número de versões não atuais retidas em um bucket S3 com versão. Se houver mais versões não atuais do que `NewerNoncurrentVersions` o especificado, o StorageGRID removerá as versões mais antigas quando o valor não-atual tiver decorrido. O `NewerNoncurrentVersions` limite substitui as regras de ciclo de vida fornecidas pelo ILM, o que significa que um objeto não atual com uma versão dentro do

`NewerNoncurrentVersions` limite é retido se o ILM solicitar sua exclusão.

Para remover marcadores de exclusão de objetos expirados, use a `Expiration` ação com uma das seguintes tags: `ExpiredObjectDeleteMarker` `Days` , Ou `Date`.

- **ILM**: "Clonar uma política ativa" E adicione duas regras ILM à nova política:
  - Primeira regra: Use "tempo não atual" como tempo de referência para corresponder às versões não atuais do objeto. No "Etapa 1 (Digite detalhes) do assistente criar uma regra ILM", selecione **Sim** para a pergunta: "Aplicar esta regra apenas a versões de objetos mais antigas (em buckets do S3 com controle de versão ativado)?"
  - Segunda regra: Use **tempo de ingestão** para corresponder à versão atual. A regra "hora não atual" deve aparecer na política acima da regra **tempo de ingestão**.

    Para remover marcadores de exclusão de objetos expirados, use uma regra **tempo de ingestão** para corresponder aos marcadores de exclusão atuais. Os marcadores de exclusão só são removidos quando um **período de tempo** de **dias** passou e o criador de exclusão atual expirou (não há versões não atuais).
- **Excluir objetos no bucket**: Use o gerenciador de locatários para "eliminar todas as versões de objetos", incluindo excluir marcadores, de um bucket.

Quando um objeto versionado é excluído, o StorageGRID cria um marcador de exclusão de byte zero como a versão atual do objeto. Todos os objetos e marcadores de exclusão devem ser removidos antes que um bucket versionado possa ser excluído.

- Excluir marcadores criados no StorageGRID 11,7 ou anterior só pode ser removido por meio de solicitações de cliente S3, eles não são removidos pelo ILM, regras de ciclo de vida do bucket ou Excluir objetos em operações de bucket.
- Excluir marcadores de um bucket criado no StorageGRID 11,8 ou posterior pode ser removido pelo ILM, regras de ciclo de vida do bucket, Excluir objetos em operações de bucket ou uma exclusão explícita do cliente S3.

Informações relacionadas

- "USE A API REST DO S3"
- "Exemplo 4: Regras ILM e política para objetos com versão S3"

Criar e atribuir notas de armazenamento

Os graus de armazenamento identificam o tipo de armazenamento usado por um nó de armazenamento. Você pode criar classes de storage se quiser que as regras do ILM coloquem determinados objetos em determinados nós de storage.

Antes de começar

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

Sobre esta tarefa

Quando você instala o StorageGRID pela primeira vez, o nível de armazenamento **padrão** é atribuído automaticamente a cada nó de armazenamento no sistema. Conforme necessário, você pode, opcionalmente, definir categorias de storage personalizadas e atribuí-las a diferentes nós de storage.

O uso de classes de armazenamento personalizadas permite criar pools de armazenamento ILM que contêm apenas um tipo específico de nó de armazenamento. Por exemplo, você pode querer que certos objetos sejam armazenados em seus nós de storage mais rápidos, como dispositivos de storage all-flash StorageGRID.

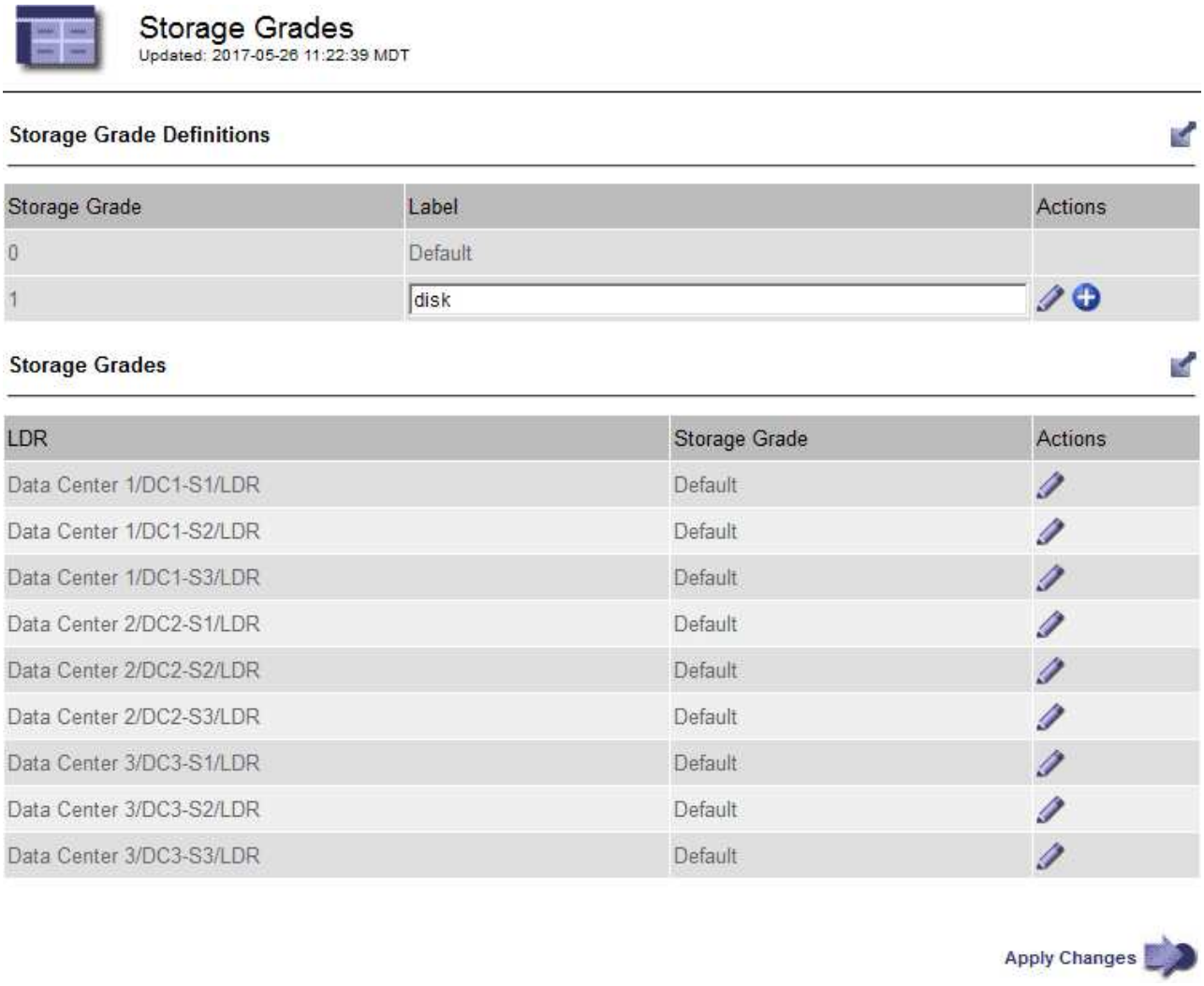
> Os nós de storage podem ser configurados durante a instalação para conter apenas metadados de objetos e não dados de objetos. Os nós de storage somente de metadados não podem ser atribuídos a um nível de storage. Para obter mais informações, "Tipos de nós de storage"consulte .

Se o grau de armazenamento não for um problema (por exemplo, todos os nós de armazenamento são idênticos), você pode ignorar este procedimento e usar a seleção **inclui todas as classes de armazenamento** para o grau de armazenamento quando "crie pools de armazenamento"você . O uso dessa seleção garante que o pool de armazenamento incluirá todos os nós de armazenamento no local, independentemente de seu nível de armazenamento.

> Não crie mais notas de armazenamento do que o necessário. Por exemplo, não crie um nível de armazenamento para cada nó de armazenamento. Em vez disso, atribua cada nível de storage a dois ou mais nós. Os graus de armazenamento atribuídos a apenas um nó podem causar backlogs de ILM se esse nó ficar indisponível.

Passos

1. Selecione **ILM** > **classes de armazenamento**.
2. Definir graus de armazenamento personalizados:
   a. Para cada grau de armazenamento personalizado que você deseja adicionar, selecione **Inserir** para adicionar uma linha.
   b. Introduza uma etiqueta descritiva.



c. Selecione **aplicar alterações**.

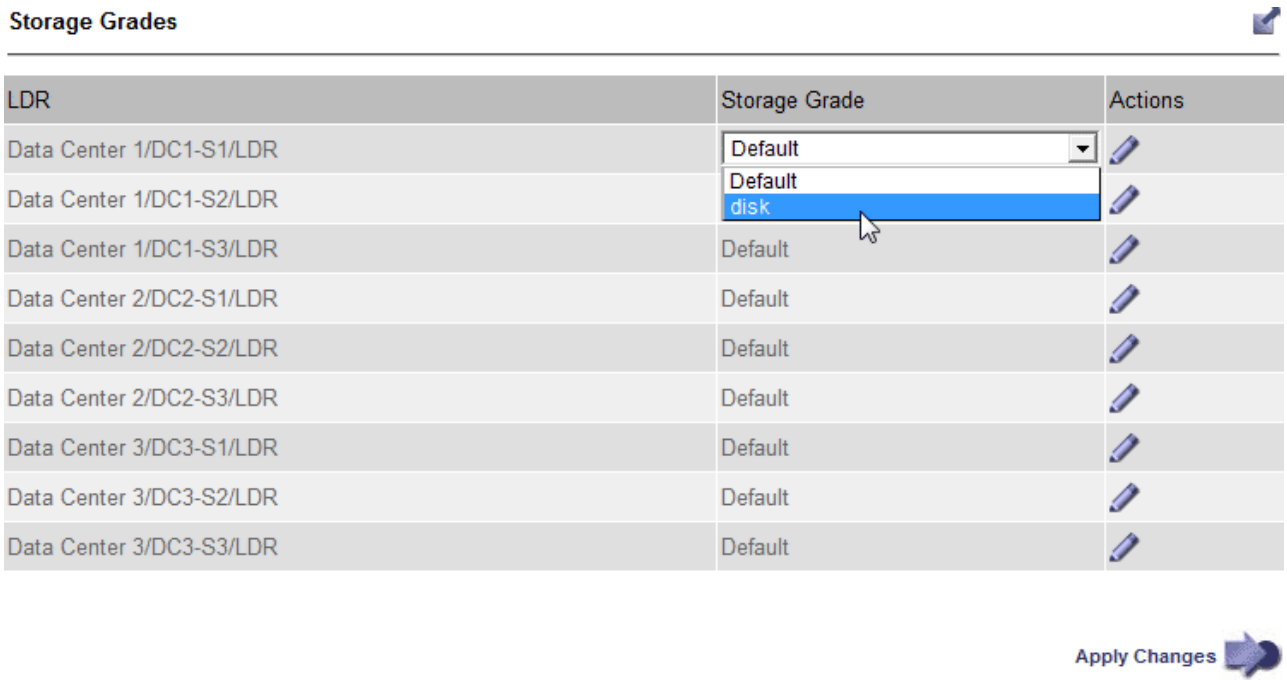
d. Opcionalmente, se você precisar modificar um rótulo salvo, selecione **Editar** e selecione **aplicar alterações**.

Não é possível excluir graus de armazenamento.

3. Atribuir novos graus de storage aos nós de storage:

a. Localize o nó de armazenamento na lista LDR e selecione o ícone **Editar**.

b. Selecione o grau de armazenamento adequado na lista.



Atribua um nível de storage a um determinado nó de storage somente uma vez. Um nó de armazenamento recuperado de falha mantém o grau de armazenamento atribuído anteriormente. Não altere esta atribuição depois de a política ILM estar ativada. Se a atribuição for alterada, os dados serão armazenados com base no novo nível de armazenamento.

a. Selecione **aplicar alterações**.

Use pools de armazenamento

O que é um pool de storage?

Um pool de storage é um agrupamento lógico de nós de storage.

Quando você instala o StorageGRID, um pool de storage por site é criado automaticamente. Você pode configurar pools de storage adicionais conforme necessário para seus requisitos de storage.

Os nós de storage podem ser configurados durante a instalação para conter dados de objetos e metadados de objetos, ou apenas metadados de objetos. Os nós de storage somente de metadados não podem ser usados em pools de storage. Para obter mais informações, "Tipos de nós de storage"consulte .

Os pools de armazenamento têm dois atributos:

- **Storage grade**: Para nós de storage, o desempenho relativo do armazenamento de backup.
- **Site**: O centro de dados onde os objetos serão armazenados.

Os pools de armazenamento são usados em regras ILM para determinar onde os dados do objeto são armazenados e o tipo de armazenamento usado. Ao configurar regras de ILM para replicação, você seleciona um ou mais pools de armazenamento.

Diretrizes para a criação de pools de armazenamento

Configure e use pools de storage para se proteger contra a perda de dados, distribuindo dados em vários locais. As cópias replicadas e as cópias codificadas por apagamento exigem configurações de pool de storage diferentes.

"Exemplos de ativação da proteção contra perda de sites usando replicação e codificação de apagamento"Consulte .

Diretrizes para todos os pools de armazenamento

- Mantenha as configurações do pool de storage o mais simples possível. Não crie mais pools de armazenamento do que o necessário.
- Crie pools de storage com tantos nós quanto possível. Cada pool de storage deve conter dois ou mais nós. Um pool de storage com nós insuficientes pode causar backlogs de ILM se um nó ficar indisponível.
- Evite criar ou usar pools de storage que se sobrepõem (contêm um ou mais dos mesmos nós). Se os pools de armazenamento se sobrepuserem, mais de uma cópia dos dados de objeto poderá ser salva no mesmo nó.
- Em geral, não use o pool de storage todos os nós de storage (StorageGRID 11,6 e anterior) ou o site todos os sites. Esses itens são atualizados automaticamente para incluir novos sites adicionados em uma expansão, o que pode não ser o comportamento desejado.

Diretrizes para pools de storage usados para cópias replicadas

- Para proteção contra perda de local usando "replicação"o , especifique um ou mais pools de armazenamento específicos do local no "Instruções de colocação para cada regra ILM".

  Um pool de storage é criado automaticamente para cada local durante a instalação do StorageGRID.

  O uso de um pool de storage para cada local garante que as cópias de objetos replicadas sejam colocadas exatamente onde você espera (por exemplo, uma cópia de cada objeto em cada local para proteção contra perda de local).

- Se você adicionar um site em uma expansão, crie um novo pool de armazenamento que contenha apenas o novo site. Em seguida"Atualizar regras ILM", para controlar quais objetos são armazenados no novo site.
- Se o número de cópias for menor que o número de pools de storage, o sistema as distribuirá para equilibrar a utilização de disco entre os pools.
- Se os pools de storage se sobreporem (contiverem os mesmos nós de storage), todas as cópias do objeto poderão ser salvas em apenas um local. Você deve garantir que os pools de storage selecionados não contenham os mesmos nós de storage.

Diretrizes para pools de storage usados para cópias codificadas por apagamento

- Para proteção contra perda de local usando "codificação de apagamento"o , crie pools de armazenamento que consistem em pelo menos três locais. Se um pool de armazenamento incluir apenas dois sites, você não poderá usar esse pool de armazenamento para codificação de apagamento. Não há esquemas de codificação de apagamento disponíveis para um pool de storage que tenha dois locais.
- O número de nós de storage e sites contidos no pool de storage determina quais "esquemas de codificação de apagamento"estão disponíveis.
- Se possível, um pool de storage deve incluir mais do que o número mínimo de nós de storage necessário para o esquema de codificação de apagamento selecionado. Por exemplo, se você usar um 3 esquema

de codificação de apagamento de mais de 6 anos, precisará ter pelo menos nove nós de storage. No entanto, é recomendável ter pelo menos um nó de armazenamento adicional por local.

- Distribua os nós de storage entre locais da forma mais uniforme possível. Por exemplo, para dar suporte a um 3 esquema de codificação de apagamento de mais de 6 horas por dia, configure um pool de storage que inclua pelo menos três nós de storage em três locais.
- Se você tiver altos requisitos de taxa de transferência, usar um pool de armazenamento que inclua vários locais não é recomendado se a latência de rede entre locais for maior que 100 ms. À medida que a latência aumenta, a taxa na qual o StorageGRID pode criar, colocar e recuperar fragmentos de objetos diminui drasticamente devido à diminuição da taxa de transferência da rede TCP.

  A diminuição na taxa de transferência afeta as taxas máximas alcançáveis de ingestão e recuperação de objetos (quando balanceado ou rigoroso são selecionados como o comportamento de ingestão) ou pode levar a backlogs de fila ILM (quando Dual Commit é selecionado como o comportamento de ingestão). "Comportamento de ingestão de regra de ILM"Consulte .

> Se a grade incluir apenas um local, você será impedido de usar o pool de storage todos os nós de storage (StorageGRID 11,6 e anterior) ou o site todos os sites em um perfil de codificação de apagamento. Esse comportamento impede que o perfil se torne inválido se um segundo site for adicionado.

Ativar a proteção contra perda de local

Se a implantação do StorageGRID incluir mais de um local, você poderá usar a replicação e a codificação de apagamento com pools de storage configurados adequadamente para habilitar a proteção contra perda de site.

A replicação e a codificação de apagamento exigem configurações diferentes de pool de storage:

- Para usar a replicação para proteção contra perda de site, use os pools de storage específicos do local que são criados automaticamente durante a instalação do StorageGRID. Em seguida, crie regras ILM com "instruções de colocação" que especificam vários pools de armazenamento de modo que uma cópia de cada objeto seja colocada em cada local.
- Para usar a codificação de apagamento para proteção contra perda de site"crie pools de armazenamento que consistem em vários locais", . Em seguida, crie regras ILM que usam um pool de armazenamento que consiste em vários sites e qualquer esquema de codificação de apagamento disponível.

> Ao configurar a implantação do StorageGRID para proteção contra perda de site, você também deve levar em conta os efeitos do "opções de ingestão" e "consistência"do .

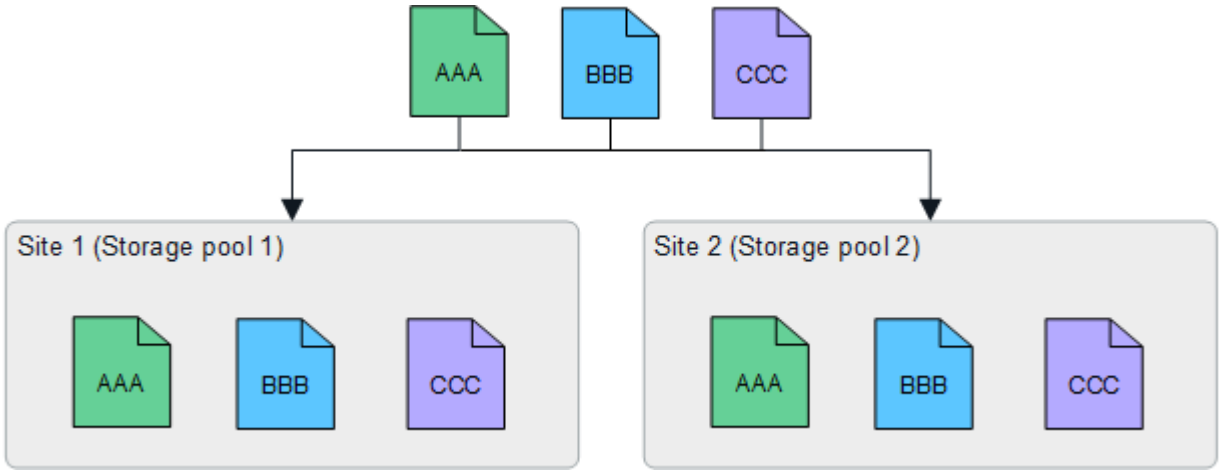
Exemplo de replicação

Por padrão, um pool de armazenamento é criado para cada local durante a instalação do StorageGRID. Ter pools de storage que consistem em apenas um local permite configurar regras de ILM que usam replicação para proteção contra perda de site. Neste exemplo:

- O pool de armazenamento 1 contém o local 1
- O pool de armazenamento 2 contém o local 2
- A regra ILM contém dois posicionamentos:
  - Armazene objetos replicando cópia 1 no local 1

◦ Armazene objetos replicando cópia 1 no local 2

Colocações de regra ILM:



Se um site for perdido, cópias dos objetos estarão disponíveis no outro site.

Exemplo de codificação de apagamento

Ter pools de storage compostos por mais de um local por pool de storage permite configurar regras de ILM que usam codificação de apagamento para proteção contra perda de site. Neste exemplo:

- O pool de armazenamento 1 contém os locais 1 a 3
- A regra ILM contém um posicionamento: Armazenar objetos por codificação de apagamento usando um esquema EC 4-2 no pool de armazenamento 1, que contém três locais

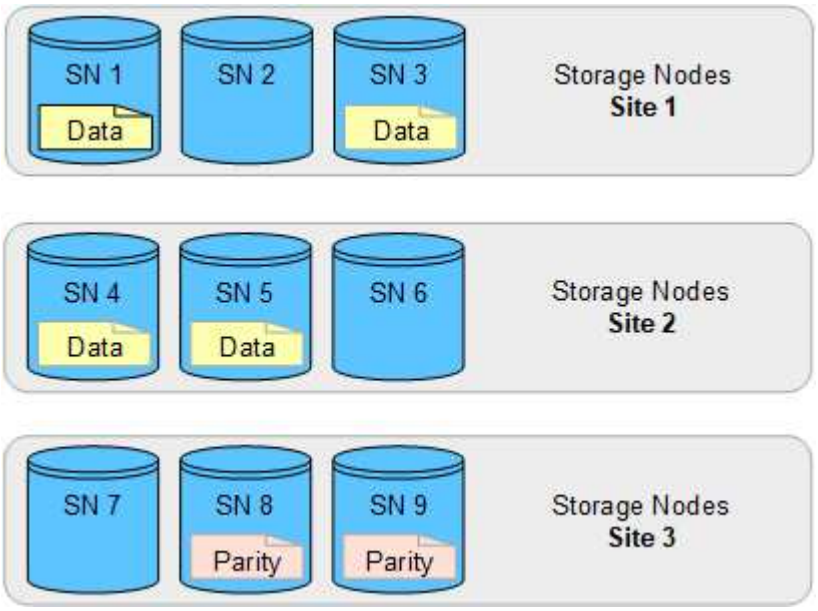
Colocações de regra ILM:

Neste exemplo:

- A regra ILM usa um esquema de codificação de apagamento 4-2.
- Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados do objeto.
- Cada um dos seis fragmentos é armazenado em um nó diferente em três locais de data center para fornecer proteção de dados para falhas de nós ou perda de local.

> A codificação de apagamento é permitida em pools de armazenamento contendo qualquer número de sites *exceto* dois sites.

Regra ILM usando o esquema de codificação de apagamento 4-2:



Se um site for perdido, os dados ainda podem ser recuperados:

Crie um pool de armazenamento

Você cria pools de storage para determinar onde o sistema StorageGRID armazena dados de objetos e o tipo de storage usado. Cada pool de storage inclui um ou mais locais e um ou mais tipos de storage.

> Quando você instala o StorageGRID 11,9 em uma nova grade, os pools de storage são criados automaticamente para cada local. No entanto, se você instalou inicialmente o StorageGRID 11,6 ou anterior, os pools de armazenamento não serão criados automaticamente para cada site.

Se você quiser criar pools de armazenamento em nuvem para armazenar dados de objetos fora do sistema StorageGRID, consulte "Informações sobre como usar Cloud Storage Pools".

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você revisou as diretrizes para a criação de pools de armazenamento.

Sobre esta tarefa

Os pools de storage determinam onde os dados do objeto são armazenados. O número de pools de storage de que você precisa depende do número de locais na grade e dos tipos de cópias que você deseja: Replicados ou codificados para apagamento.

- Para replicação e codificação de apagamento de um único local, crie um pool de storage para cada local. Por exemplo, se você quiser armazenar cópias de objetos replicadas em três locais, crie três pools de storage.
- Para codificação de apagamento em três ou mais locais, crie um pool de storage que inclua uma entrada

para cada local. Por exemplo, se você quiser apagar objetos de código em três locais, crie um pool de storage.

> Não inclua o site todos os sites em um pool de armazenamento que será usado em um perfil de codificação de apagamento. Em vez disso, adicione uma entrada separada ao pool de storage para cada local que armazenará dados codificados por apagamento. este passoConsulte para obter um exemplo.

- Se você tiver mais de um nível de armazenamento, não crie um pool de armazenamento que inclua diferentes graus de armazenamento em um único local. Consulte "Diretrizes para a criação de pools de armazenamento".

Passos

1. Selecione **ILM** > **Storage Pools**.

   A guia pools de armazenamento lista todos os pools de armazenamento definidos.

   > Para novas instalações do StorageGRID 11,6 ou anterior, o pool de storage de todos os nós de storage é atualizado automaticamente sempre que você adiciona novos locais de data center. Não use esse pool nas regras do ILM.

2. Para criar um novo pool de armazenamento, selecione **criar**.
3. Insira um nome exclusivo para o pool de armazenamento. Use um nome que será fácil de identificar quando você configurar perfis de codificação de apagamento e regras ILM.
4. Na lista suspensa **Site**, selecione um site para esse pool de armazenamento.

   Quando você seleciona um site, o número de nós de storage na tabela é atualizado automaticamente.

   Em geral, não use o site todos os sites em nenhum pool de armazenamento. As regras de ILM que usam um pool de armazenamento de todos os sites colocam objetos em qualquer site disponível, proporcionando menos controle sobre o posicionamento de objetos. Além disso, um pool de storage All Sites usa os nós de storage em um novo local imediatamente, o que pode não ser o comportamento esperado.

5. Na lista suspensa **Storage grade**, selecione o tipo de armazenamento que será usado se uma regra ILM usar esse pool de armazenamento.

   O nível de storage, *inclui todos os tipos de storage*, inclui todos os nós de storage no local selecionado. Se você criou graus de storage adicionais para os nós de storage na grade, eles serão listados na lista suspensa.

6. se você quiser usar o pool de armazenamento em um perfil de codificação de apagamento de vários sites, selecione **Add More Nodes** para adicionar uma entrada para cada site ao pool de armazenamento.

   > Você será avisado se você adicionar mais de uma entrada com diferentes graus de armazenamento para um site.

   Para remover uma entrada, selecione o ícone de exclusão ✕.

7. Quando estiver satisfeito com suas seleções, selecione **Salvar**.

   O novo pool de armazenamento é adicionado à lista.

Veja os detalhes do pool de armazenamento

Você pode visualizar os detalhes de um pool de storage para determinar onde o pool de storage é usado e ver quais nós e categorias de storage estão incluídos.

Antes de começar

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

Passos

1. Selecione **ILM** > **Storage Pools**.

   A tabela Storage Pools inclui as seguintes informações para cada pool de storage que inclui nós de storage:

   - **Nome**: O nome de exibição exclusivo do pool de armazenamento.
   - **Contagem de nós**: O número de nós no pool de storage.
   - **Uso do armazenamento**: A porcentagem do espaço utilizável total que foi usado para dados de objeto neste nó. Esse valor não inclui metadados de objetos.
   - **Capacidade total**: O tamanho do pool de armazenamento, que é igual à quantidade total de espaço utilizável para dados de objetos para todos os nós no pool de armazenamento.
   - **Uso de ILM**: Como o pool de armazenamento está sendo usado atualmente. Um pool de storage pode não ser usado ou pode ser usado em uma ou mais regras do ILM, perfis de codificação de apagamento ou ambos.

2. Para exibir detalhes de um pool de armazenamento específico, selecione seu nome.

   A página de detalhes do pool de armazenamento é exibida.

3. Exiba a guia **nós** para saber mais sobre os nós de armazenamento incluídos no pool de armazenamento.

   A tabela inclui as seguintes informações para cada nó:

   - Nome do nó
   - Nome do local
   - Grau de armazenamento
   - Uso do storage: A porcentagem do espaço utilizável total para dados de objetos que foram usados para o nó de storage.

   > ⓘ O mesmo valor de uso de armazenamento (%) também é mostrado no gráfico armazenamento usado - dados de objetos para cada nó de armazenamento (selecione **NÓS** > ***Storage Node*** > **Storage**).

4. Visualize a guia **uso de ILM** para determinar se o pool de armazenamento está sendo usado atualmente em quaisquer regras de ILM ou perfis de codificação de apagamento.
5. Opcionalmente, vá para a página **regras ILM** para saber mais e gerenciar quaisquer regras que usem o pool de armazenamento.

   Consulte "Instruções para trabalhar com regras ILM".

Editar pool de armazenamento

Você pode editar um pool de armazenamento para alterar seu nome ou atualizar sites e classes de armazenamento.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você revisou o "diretrizes para a criação de pools de armazenamento".
- Se você planeja editar um pool de armazenamento que é usado por uma regra na política ILM ativa, você considerou como suas alterações afetarão o posicionamento dos dados do objeto.

Sobre esta tarefa

Se você estiver adicionando um novo local ou nível de storage a um pool de storage usado na política de ILM ativa, saiba que os nós de storage no novo local ou nível de storage não serão usados automaticamente. Para forçar o StorageGRID a usar um novo local ou nível de armazenamento, você deve ativar uma nova política de ILM depois de salvar o pool de armazenamento editado.

Passos

1. Selecione **ILM** > **Storage Pools**.
2. Marque a caixa de seleção do pool de armazenamento que deseja editar.

   Não é possível editar o pool de storage de todos os nós de storage (StorageGRID 11,6 e anterior).

3. Selecione **Editar**.
4. Conforme necessário, altere o nome do pool de armazenamento.
5. Conforme necessário, selecione outros locais e categorias de armazenamento.

   Você é impedido de alterar o local ou o nível de armazenamento se o pool de armazenamento for usado em um perfil de codificação de apagamento e a alteração fizer com que o esquema de codificação de apagamento se torne inválido. Por exemplo, se um pool de armazenamento usado em um perfil de codificação de apagamento incluir atualmente um grau de armazenamento com apenas um local, você será impedido de usar um grau de armazenamento com dois sites porque a alteração tornaria o esquema de codificação de apagamento inválido.

   > Adicionar ou remover sites de um pool de armazenamento existente não moverá nenhum dado codificado de apagamento existente. Se você quiser mover os dados existentes do site, você deve criar um novo pool de armazenamento e perfil EC para recodificar os dados.

6. Selecione **Guardar**.

Depois de terminar

Se você adicionou um novo local ou nível de armazenamento a um pool de armazenamento usado na política ILM ativa, ative uma nova política ILM para forçar o StorageGRID a usar o novo local ou nível de armazenamento. Por exemplo, clone sua política ILM existente e, em seguida, ative o clone. "Trabalhe com regras ILM e políticas ILM"Consulte .

Remova um pool de armazenamento

Você pode remover um pool de armazenamento que não está sendo usado.

Antes de começar

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

Passos

1. Selecione **ILM** > **Storage Pools**.
2. Observe a coluna de uso do ILM na tabela para determinar se você pode remover o pool de armazenamento.

   Não é possível remover um pool de armazenamento se ele estiver sendo usado em uma regra ILM ou em um perfil de codificação de apagamento. Conforme necessário, selecione ***storage pool name*** > **ILM usage** para determinar onde o pool de armazenamento é usado.

3. Se o pool de armazenamento que você deseja remover não estiver sendo usado, marque a caixa de seleção.
4. Selecione **Remover**.
5. Selecione **OK**.

Use Cloud Storage Pools

O que é um Cloud Storage Pool?

Um pool de armazenamento em nuvem permite que você use o ILM para mover dados de objetos para fora do seu sistema StorageGRID. Por exemplo, você pode migrar objetos acessados com pouca frequência para storage de nuvem de baixo custo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou a categoria Acesso de arquivamento no storage de Blobs do Microsoft Azure. Ou, talvez você queira manter um backup na nuvem de objetos do StorageGRID para aprimorar a recuperação de desastres.

Do ponto de vista do ILM, um Cloud Storage Pool é semelhante a um pool de storage. Para armazenar objetos em qualquer local, selecione o pool ao criar as instruções de posicionamento para uma regra ILM. No entanto, embora os pools de storage consistam em nós de storage no sistema StorageGRID, um pool de storage de nuvem consiste em um bucket externo (S3 TB) ou contêiner (storage Blob do Azure).

A tabela compara pools de armazenamento com pools de armazenamento em nuvem e mostra as semelhanças e diferenças de alto nível.

	Pool de storage	**Cloud Storage Pool**
Como é criado?	Usando a opção **ILM** > **Storage Pools** no Gerenciador de Grade.	Usando a opção **ILM** > **Storage Pools** > **Cloud Storage Pools** no Grid Manager. Você deve configurar o bucket externo ou o contêiner antes de criar o pool de storage de nuvem.

	Pool de storage	Cloud Storage Pool
Quantas piscinas você pode criar?	Ilimitado.	Até 10 TB.
Onde os objetos são armazenados?	Em um ou mais nós de storage no StorageGRID.	Em um bucket do Amazon S3, o contêiner de storage do Blob do Azure ou o Google Cloud externo ao sistema StorageGRID. Se o Cloud Storage Pool for um bucket do Amazon S3: • Opcionalmente, é possível configurar um ciclo de vida do bucket para migrar objetos para storage de baixo custo e longo prazo, como Amazon S3 Glacier ou S3 Glacier Deep Archive. O sistema de armazenamento externo deve suportar a classe de armazenamento Glacier e a API S3 RestoreObject. • Você pode criar pools de armazenamento na nuvem para uso com os Serviços comerciais da AWS (C2S), que oferecem suporte à região secreta da AWS. Se o pool de storage de nuvem for um contêiner de storage de Blob do Azure, o StorageGRID fará o transição do objeto para a categoria Archive. **Observação:** em geral, não configure o gerenciamento do ciclo de vida de armazenamento do Blob do Azure para o contêiner usado em um pool de storage do Cloud Storage. As operações de RestoreObject em objetos no Cloud Storage Pool podem ser afetadas pelo ciclo de vida configurado.
O que controla o posicionamento do objeto?	Uma regra ILM nas políticas ILM ativas.	Uma regra ILM nas políticas ILM ativas.
Que método de proteção de dados é usado?	Replicação ou codificação de apagamento.	Replicação.
Quantas cópias de cada objeto são permitidas?	Vários.	Uma cópia no pool de storage de nuvem e, opcionalmente, uma ou mais cópias no StorageGRID. **Observação:** você não pode armazenar um objeto em mais de um pool de armazenamento em nuvem a qualquer momento.

	Pool de storage	Cloud Storage Pool
Quais são as vantagens?	Os objetos são rapidamente acessíveis a qualquer momento.	Armazenamento de baixo custo. **Nota**: Os dados do FabricPool não podem ser dispostos em camadas nos pools de armazenamento em nuvem.

Ciclo de vida de um objeto Cloud Storage Pool

Antes de implementar Cloud Storage Pools, revise o ciclo de vida dos objetos armazenados em cada tipo de Cloud Storage Pool.

S3: Ciclo de vida de um objeto Cloud Storage Pool

As etapas descrevem os estágios do ciclo de vida de um objeto que é armazenado em um pool de armazenamento em nuvem S3.

> "Glacier" refere-se à classe de armazenamento Glacier e à classe de armazenamento Glacier Deep Archive, com uma exceção: A classe de armazenamento Glacier Deep Archive não suporta o nível de restauração Expedited. Apenas a recuperação em massa ou padrão é suportada.

> O Google Cloud Platform (GCP) oferece suporte à recuperação de objetos de armazenamento de longo prazo sem exigir uma operação PÓS-restauração.

1. **Objeto armazenado no StorageGRID**

   Para iniciar o ciclo de vida, um aplicativo cliente armazena um objeto no StorageGRID.

2. **Objeto movido para o pool de armazenamento em nuvem S3**
   - Quando o objeto é correspondido por uma regra ILM que usa um pool de armazenamento em nuvem S3 como local de colocação, o StorageGRID move o objeto para o bucket externo S3 especificado pelo pool de armazenamento em nuvem.
   - Quando o objeto for movido para o pool de armazenamento em nuvem S3, o aplicativo cliente poderá recuperá-lo usando uma solicitação GetObject S3 do StorageGRID, a menos que o objeto tenha sido transferido para o armazenamento Glacier.
3. **Objeto transicionado para Glacier (estado não recuperável)**
   - Opcionalmente, o objeto pode ser transferido para o armazenamento Glacier. Por exemplo, o bucket externo do S3 pode usar a configuração do ciclo de vida para fazer a transição de um objeto para o armazenamento do Glacier imediatamente ou após algum número de dias.

     > Se você quiser fazer a transição de objetos, crie uma configuração de ciclo de vida para o bucket externo do S3 e use uma solução de armazenamento que implemente a classe de armazenamento Glacier e ofereça suporte à API S3 RestoreObject.

   - Durante a transição, o aplicativo cliente pode usar uma solicitação de S3 HeadObject para monitorar o status do objeto.
4. * Objeto restaurado a partir do armazenamento Glacier*

Se um objeto tiver sido transferido para o armazenamento Glacier, o aplicativo cliente poderá emitir uma solicitação de S3 RestoreObject para restaurar uma cópia recuperável para o pool de armazenamento em nuvem S3. A solicitação especifica quantos dias a cópia deve estar disponível no Cloud Storage Pool e no nível de acesso a dados a ser usado para a operação de restauração (Expedited, Standard ou Bulk). Quando a data de expiração da cópia recuperável é atingida, a cópia é automaticamente devolvida a um estado não recuperável.

> Se uma ou mais cópias do objeto também existirem em nós de storage no StorageGRID, não será necessário restaurar o objeto do Glacier emitindo uma solicitação de RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

5. **Objeto recuperado**

   Uma vez que um objeto foi restaurado, o aplicativo cliente pode emitir uma solicitação GetObject para recuperar o objeto restaurado.

Azure: Ciclo de vida de um objeto Cloud Storage Pool

As etapas descrevem os estágios do ciclo de vida de um objeto que é armazenado em um pool de armazenamento em nuvem do Azure.

1. **Objeto armazenado no StorageGRID**

   Para iniciar o ciclo de vida, um aplicativo cliente armazena um objeto no StorageGRID.

2. **Objeto movido para o Azure Cloud Storage Pool**

   Quando o objeto é correspondido por uma regra de ILM que usa um pool de storage do Azure Cloud como local de posicionamento, o StorageGRID move o objeto para o contêiner de storage externo de Blob especificado pelo pool de storage do Cloud.

3. **Objeto transicionado para o nível de Arquivo (estado não recuperável)**

   Imediatamente após a migração do objeto para o pool de storage de nuvem do Azure, o StorageGRID faz a transição automática do objeto para a categoria de arquivamento de storage de Blob do Azure.

4. **Objeto restaurado a partir do nível de Arquivo**

   Se um objeto tiver sido transferido para o nível Archive, o aplicativo cliente poderá emitir uma solicitação de S3 RestoreObject para restaurar uma cópia recuperável para o pool de armazenamento em nuvem do Azure.

   Quando o StorageGRID recebe o RestoreObject, ele faz a transição temporária do objeto para a camada de recuperação de storage do Blob do Azure. Assim que a data de expiração na solicitação de RestoreObject for atingida, o StorageGRID faz a transição do objeto de volta para o nível de arquivamento.

   > Se uma ou mais cópias do objeto também existirem em nós de storage no StorageGRID, não será necessário restaurar o objeto do nível de acesso de arquivamento emitindo uma solicitação de RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

5. **Objeto recuperado**

Depois que um objeto for restaurado para o Azure Cloud Storage Pool, o aplicativo cliente poderá emitir uma solicitação GetObject para recuperar o objeto restaurado.

Informações relacionadas

"USE A API REST DO S3"

Quando usar Cloud Storage Pools

Com o Cloud Storage Pools, é possível fazer backup ou categorizar dados em um local externo. Além disso, você pode fazer backup ou categorizar dados em mais de uma nuvem.

Faça backup dos dados do StorageGRID em um local externo

Você pode usar um pool de armazenamento em nuvem para fazer backup de objetos do StorageGRID para um local externo.

Se as cópias no StorageGRID estiverem inacessíveis, os dados de objeto no pool de armazenamento em nuvem podem ser usados para atender solicitações de clientes. No entanto, talvez seja necessário emitir a solicitação S3 RestoreObject para acessar a cópia de objeto de backup no pool de armazenamento em nuvem.

Os dados de objeto em um pool de storage de nuvem também podem ser usados para recuperar dados perdidos do StorageGRID devido a uma falha de volume de storage ou nó de storage. Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID restaurará temporariamente o objeto e criará uma nova cópia no nó de armazenamento recuperado.

Para implementar uma solução de backup:

1. Crie um único pool de storage de nuvem.
2. Configurar uma regra de ILM que armazene simultaneamente cópias de objetos em nós de storage (como cópias replicadas ou codificadas por apagamento) e uma única cópia de objeto no Cloud Storage Pool.
3. Adicione a regra à sua política ILM. Em seguida, simule e ative a política.

Categorize os dados do StorageGRID para o local externo

Você pode usar um pool de armazenamento em nuvem para armazenar objetos fora do sistema StorageGRID. Por exemplo, suponha que você tenha um grande número de objetos que você precisa reter, mas você espera acessar esses objetos raramente, se nunca. Você pode usar um pool de storage de nuvem para categorizar os objetos em storage de baixo custo e liberar espaço no StorageGRID.

Para implementar uma solução de disposição em camadas:

1. Crie um único pool de storage de nuvem.
2. Configure uma regra de ILM que mova objetos raramente usados de nós de storage para o Cloud Storage Pool.
3. Adicione a regra à sua política ILM. Em seguida, simule e ative a política.

Manter vários pontos de extremidade de nuvem

Você pode configurar vários pontos de extremidade do Cloud Storage Pool se quiser categorizar ou fazer backup de dados de objetos em mais de uma nuvem. Os filtros nas regras do ILM permitem especificar quais

objetos são armazenados em cada pool de armazenamento em nuvem. Por exemplo, você pode querer armazenar objetos de alguns locatários ou buckets no Amazon S3 Glacier e objetos de outros locatários ou buckets no storage Blob do Azure. Ou, talvez você queira mover dados entre o Amazon S3 Glacier e o storage Azure Blob.

> Ao usar vários pontos de extremidade do Cloud Storage Pool, lembre-se de que um objeto pode ser armazenado em apenas um pool de armazenamento em nuvem de cada vez.

Para implementar vários pontos de extremidade de nuvem:

1. Crie até 10 pools de armazenamento em nuvem.
2. Configure as regras do ILM para armazenar os dados de objeto apropriados no momento apropriado em cada pool de armazenamento em nuvem. Por exemplo, armazene objetos do bucket A no Cloud Storage Pool A e armazene objetos do bucket B no Cloud Storage Pool B. ou armazene objetos no Cloud Storage Pool A por algum tempo e, em seguida, mova-os para o Cloud Storage Pool B.
3. Adicione as regras à sua política ILM. Em seguida, simule e ative a política.

Considerações para pools de storage em nuvem

Se você planeja usar um pool de armazenamento em nuvem para mover objetos para fora do sistema StorageGRID, leia as considerações sobre como configurar e usar pools de armazenamento em nuvem.

Considerações gerais

- Em geral, o storage de arquivamento em nuvem, como o armazenamento Amazon S3 Glacier ou Azure Blob, é um local econômico para armazenar dados de objetos. No entanto, os custos para recuperar dados do armazenamento de arquivamento em nuvem são relativamente altos. Para alcançar o menor custo geral, você deve considerar quando e com que frequência acessará os objetos no Cloud Storage Pool. O uso de um Cloud Storage Pool é recomendado apenas para conteúdo que você espera acessar com pouca frequência.
- O uso de pools de armazenamento em nuvem com FabricPool não é suportado devido à latência adicional para recuperar um objeto do destino de pool de armazenamento em nuvem.
- Os objetos com bloqueio de objeto S3 ativado não podem ser colocados em pools de armazenamento em nuvem.
- Se o bucket S3 de destino para um pool de armazenamento em nuvem tiver o bloqueio de objeto S3 ativado, a tentativa de configurar a replicação de bucket (PutBucketReplication) falhará com um erro AccessDenied.
- As seguintes combinações de plataforma, autenticação e protocolo com o bloqueio de objetos S3 não são compatíveis com Cloud Storage Pools:
  - **Plataformas**: Google Cloud Platform e Azure
  - **Tipos de autenticação**: Funções do IAM em qualquer lugar e acesso anônimo
  - **Protocolo**: HTTP

Considerações para as portas usadas para pools de armazenamento em nuvem

Para garantir que as regras do ILM possam mover objetos de e para o pool de armazenamento em nuvem especificado, você deve configurar a rede ou redes que contêm os nós de armazenamento do sistema. Você deve garantir que as seguintes portas possam se comunicar com o Cloud Storage Pool.

Por padrão, os pools de armazenamento em nuvem usam as seguintes portas:

- **80**: Para URIs de endpoint que começam com http
- **443**: Para URIs de endpoint que começam com https

Você pode especificar uma porta diferente ao criar ou editar um pool de armazenamento em nuvem.

Se você usar um servidor proxy não transparente, também deverá "configurar um proxy de armazenamento"permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet.

Considerações sobre custos

O acesso ao storage na nuvem usando um pool de armazenamento em nuvem requer conetividade de rede com a nuvem. Você deve considerar o custo da infraestrutura de rede que usará para acessar a nuvem e provisioná-la adequadamente, com base na quantidade de dados que espera mover entre o StorageGRID e a nuvem usando o pool de armazenamento em nuvem.

Quando o StorageGRID se coneta ao endpoint externo do pool de armazenamento em nuvem, ele emite várias solicitações para monitorar a conetividade e garantir que ele possa executar as operações necessárias. Embora alguns custos adicionais sejam associados a essas solicitações, o custo do monitoramento de um pool de armazenamento em nuvem deve ser apenas uma pequena fração do custo geral de armazenamento de objetos no S3 ou Azure.

Custos mais significativos podem ser incorridos se você precisar mover objetos de um endpoint externo do pool de armazenamento em nuvem de volta para o StorageGRID. Os objetos podem ser movidos de volta para o StorageGRID em qualquer um destes casos:

- A única cópia do objeto está em um pool de storage de nuvem e você decide armazenar o objeto no StorageGRID. Nesse caso, você reconfigura suas regras e políticas de ILM. Quando a avaliação do ILM ocorre, o StorageGRID emite várias solicitações para recuperar o objeto do pool de armazenamento em nuvem. Em seguida, o StorageGRID cria o número especificado de cópias replicadas ou codificadas para apagamento localmente. Depois que o objeto é movido de volta para o StorageGRID, a cópia no pool de armazenamento em nuvem é excluída.
- Os objetos são perdidos devido à falha do nó de storage. Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID restaurará temporariamente o objeto e criará uma nova cópia no nó de armazenamento recuperado.

> ⓘ Quando os objetos são movidos de volta para o StorageGRID de um pool de armazenamento em nuvem, o StorageGRID emite várias solicitações para o ponto de extremidade do pool de armazenamento em nuvem para cada objeto. Antes de mover um grande número de objetos, entre em Contato com o suporte técnico para obter ajuda na estimativa do prazo e dos custos associados.

S3: Permissões necessárias para o bucket do Cloud Storage Pool

As políticas para o bucket externo do S3 usadas em um pool de armazenamento em nuvem devem conceder permissão StorageGRID para mover um objeto para o bucket, obter o status de um objeto, restaurar um objeto do armazenamento do Glacier quando necessário e muito mais. Idealmente, o StorageGRID deve ter acesso de controle total ao bucket (`s3:*`); no entanto, se isso não for possível, a política de bucket deve conceder as seguintes permissões do S3 ao StorageGRID:

- `s3:AbortMultipartUpload`

- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Considerações sobre o ciclo de vida do balde externo

O movimento de objetos entre o StorageGRID e o bucket externo do S3 especificado no pool de storage de nuvem é controlado pelas regras do ILM e pelas políticas ativas do ILM no StorageGRID. Em contraste, a transição de objetos do bucket externo S3 especificado no pool de armazenamento em nuvem para o Amazon S3 Glacier ou o S3 Glacier Deep Archive (ou para uma solução de armazenamento que implemente a classe de armazenamento Glacier) é controlada pela configuração do ciclo de vida desse bucket.

Se você quiser fazer a transição de objetos do Cloud Storage Pool, crie a configuração de ciclo de vida apropriada no bucket externo do S3 e use uma solução de armazenamento que implemente a classe de armazenamento Glacier e ofereça suporte à API S3 RestoreObject.

Por exemplo, suponha que você queira que todos os objetos movidos do StorageGRID para o pool de armazenamento em nuvem sejam transferidos imediatamente para o armazenamento do Amazon S3 Glacier. Você criaria uma configuração de ciclo de vida no bucket externo do S3 que especifica uma única ação (**transition**) da seguinte forma:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Essa regra faria a transição de todos os objetos de bucket para o Amazon S3 Glacier no dia em que foram criados (ou seja, no dia em que foram movidos do StorageGRID para o pool de storage de nuvem).

> Ao configurar o ciclo de vida do bucket externo, nunca use as ações **Expiration** para definir quando os objetos expiram. As ações de expiração fazem com que o sistema de armazenamento externo exclua objetos expirados. Se você tentar acessar um objeto expirado do StorageGRID, o objeto excluído não será encontrado.

Se você quiser fazer a transição de objetos no Cloud Storage Pool para o S3 Glacier Deep Archive (em vez de para o Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` no ciclo de vida do bucket. No entanto, esteja ciente de que você não pode usar o `Expedited` nível para restaurar objetos do S3 Glacier Deep Archive.

Azure: Considerações para o nível de acesso

Ao configurar uma conta de armazenamento do Azure, você pode definir o nível de acesso padrão como Hot or Cool. Ao criar uma conta de storage para uso com um Cloud Storage Pool, você deve usar o Hot Tier como o nível padrão. Mesmo que o StorageGRID defina imediatamente o nível para Arquivo quando ele move objetos para o pool de armazenamento em nuvem, usar uma configuração padrão do Hot garante que você não será cobrada uma taxa de exclusão antecipada para objetos removidos do nível Cool antes do mínimo de 30 dias.

Azure: Gerenciamento de ciclo de vida não suportado

Não use o gerenciamento do ciclo de vida do storage Azure Blob para o contêiner usado com um Cloud Storage Pool. As operações do ciclo de vida podem interferir nas operações do Cloud Storage Pool.

Informações relacionadas

"Crie um pool de storage em nuvem"

Compare os pools do Cloud Storage e a replicação do CloudMirror

À medida que você começa a usar o Cloud Storage Pools, pode ser útil entender as semelhanças e diferenças entre o Cloud Storage Pools e o serviço de replicação do StorageGRID CloudMirror.

	Cloud Storage Pool	Serviço de replicação do CloudMirror
Qual é o objetivo principal?	Atua como um destino de arquivo. A cópia de objeto no Cloud Storage Pool pode ser a única cópia do objeto ou pode ser uma cópia adicional. Ou seja, em vez de manter duas cópias no local, você pode manter uma cópia no StorageGRID e enviar uma cópia para o pool de storage de nuvem.	Permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket externo do S3 (destino). Cria uma cópia independente de um objeto em uma infraestrutura S3 independente.
Como é configurado?	Definido da mesma forma que os pools de armazenamento, usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Pode ser selecionado como o local de colocação em uma regra ILM. Enquanto um pool de storage consiste em um grupo de nós de storage, um pool de armazenamento em nuvem é definido usando um endpoint remoto S3 ou Azure (endereço IP, credenciais etc.).	Um usuário de locatário "Configura a replicação do CloudMirror"definindo um endpoint do CloudMirror (endereço IP, credenciais, etc.) usando o Gerenciador do locatário ou a API do S3. Depois que o endpoint do CloudMirror for configurado, qualquer bucket de propriedade dessa conta de locatário poderá ser configurado para apontar para o endpoint do CloudMirror.
Quem é responsável por montá-lo?	Normalmente, um administrador de grade	Normalmente, um usuário locatário

	Cloud Storage Pool	Serviço de replicação do CloudMirror
Qual é o destino?	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3) • Camada de arquivamento de Blob do Azure • Google Cloud Platform (GCP)	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3) • Google Cloud Platform (GCP)
O que faz com que os objetos sejam movidos para o destino?	Uma ou mais regras ILM nas políticas ILM ativas. As regras do ILM definem quais objetos o StorageGRID move para o pool de armazenamento em nuvem e quando os objetos são movidos.	O ato de inserir um novo objeto em um bucket de origem que foi configurado com um endpoint do CloudMirror. Os objetos que existiam no bucket de origem antes do bucket ser configurado com o endpoint do CloudMirror não são replicados, a menos que sejam modificados.
Como os objetos são recuperados?	Os aplicativos devem fazer solicitações ao StorageGRID para recuperar objetos que foram movidos para um pool de armazenamento em nuvem. Se a única cópia de um objeto tiver sido transferida para armazenamento de arquivo, o StorageGRID gerencia o processo de restauração do objeto para que ele possa ser recuperado.	Como a cópia espelhada no intervalo de destino é uma cópia independente, os aplicativos podem recuperar o objeto fazendo solicitações para o StorageGRID ou para o destino S3. Por exemplo, suponha que você use a replicação do CloudMirror para espelhar objetos em uma organização parceira. O parceiro pode usar seus próprios aplicativos para ler ou atualizar objetos diretamente do destino S3. Não é necessário utilizar o StorageGRID.
Você pode ler diretamente do destino?	Não. Os objetos movidos para um pool de storage de nuvem são gerenciados pelo StorageGRID. As solicitações de leitura devem ser direcionadas ao StorageGRID (e o StorageGRID será responsável pela recuperação do pool de armazenamento em nuvem).	Sim, porque a cópia espelhada é uma cópia independente.
O que acontece se um objeto for excluído da origem?	O objeto também é excluído do Cloud Storage Pool.	A ação de exclusão não é replicada. Um objeto excluído não existe mais no bucket do StorageGRID, mas continua a existir no bucket de destino. Da mesma forma, os objetos no intervalo de destino podem ser excluídos sem afetar a origem.

	Cloud Storage Pool	Serviço de replicação do CloudMirror
Como você acessa objetos após um desastre (sistema StorageGRID não operacional)?	Os nós de StorageGRID com falha devem ser recuperados. Durante esse processo, cópias de objetos replicados podem ser restauradas usando as cópias no Cloud Storage Pool.	As cópias de objeto no destino do CloudMirror são independentes do StorageGRID, portanto, podem ser acessadas diretamente antes que os nós do StorageGRID sejam recuperados.

Crie um pool de storage em nuvem

Um Cloud Storage Pool especifica um único bucket externo do Amazon S3 ou outro fornecedor compatível com o S3 ou um contêiner de storage Azure Blob.

Ao criar um pool de storage de nuvem, especifique o nome e o local do bucket ou do contêiner externo que o StorageGRID usará para armazenar objetos, o tipo de fornecedor de nuvem (storage Amazon S3/GCP ou Azure Blob) e as informações que o StorageGRID precisa para acessar o bucket ou o contêiner externo.

O StorageGRID valida o pool de armazenamento em nuvem assim que você o salva, portanto, você deve garantir que o bucket ou o contentor especificado no pool de armazenamento em nuvem existe e está acessível.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "permissões de acesso necessárias".
- Você revisou o "Considerações para pools de storage em nuvem".
- O bucket externo ou o contentor referenciado pelo Cloud Storage Pool já existe e você tem o informações sobre endpoint de serviço.
- Para acessar o balde ou recipiente, você tem o informações de conta para o tipo de autenticação que você vai escolher.

Passos

1. Selecione **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Selecione **criar** e insira as seguintes informações:

Campo	Descrição
Nome do Cloud Storage Pool	Um nome que descreve brevemente o Cloud Storage Pool e sua finalidade. Use um nome que será fácil de identificar quando você configurar regras ILM.
Tipo de fornecedor	Qual provedor de nuvem você usará para este pool de armazenamento em nuvem: • **Amazon S3/GCP**: Selecione essa opção para um Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou outro provedor compatível com S3. • **Armazenamento de Blobs do Azure**

Campo	Descrição
Balde ou recipiente	O nome do bucket externo do S3 ou do recipiente do Azure. Não é possível alterar esse valor depois que o pool de armazenamento em nuvem for salvo.

3. com base na seleção do tipo de provedor, insira as informações do endpoint do serviço.

Amazon S3/GCP

a. Para o protocolo, selecione HTTPS ou HTTP.

> Não use conexões HTTP para dados confidenciais.

b. Introduza o nome do anfitrião. Exemplo:

`s3-aws-region.amazonaws.com`

c. Selecione o estilo de URL:

Opção	Descrição
Detecção automática	Tente detetar automaticamente qual estilo de URL usar, com base nas informações fornecidas. Por exemplo, se você especificar um endereço IP, o StorageGRID usará um URL estilo caminho. Selecione esta opção somente se você não souber qual estilo específico usar.
Virtual-hospedado-estilo	Use um URL de estilo virtual hospedado para acessar o bucket. URLs de estilo virtual hospedadas incluem o nome do intervalo como parte do nome de domínio. Exemplo: `https://bucket-name.s3.company.com/key-name`
Estilo de caminho	Use um URL de estilo de caminho para acessar o bucket. URLs de estilo de caminho incluem o nome do intervalo no final Exemplo: `https://s3.company.com/bucket-name/key-name` **Nota:** a opção URL estilo caminho não é recomendada e será obsoleta em uma versão futura do StorageGRID.

d. Opcionalmente, insira o número da porta ou use a porta padrão: 443 para HTTPS ou 80 para HTTP.

Storage Blob do Azure

a. Usando um dos formatos a seguir, insira o URI para o endpoint de serviço.

- `https://host:port`
- `http://host:port`

Exemplo: `https://myaccount.blob.core.windows.net:443`

Se você não especificar uma porta, por padrão, a porta 443 será usada para HTTPS e a porta 80 será usada para HTTP.

4. Selecione **Continue**. Em seguida, selecione o tipo de autenticação e insira as informações necessárias para o endpoint do Cloud Storage Pool:

Chave de acesso

Para Amazon S3/GCP ou outro provedor compatível com S3

a. **ID da chave de acesso**: Insira o ID da chave de acesso para a conta que possui o bucket externo.
b. **Chave de acesso secreta**: Insira a chave de acesso secreta.

Funções do IAM em qualquer lugar

Para o AWS IAM Roles Anywhere Service

O StorageGRID usa o Serviço de token de segurança (STS) da AWS para gerar dinamicamente um token de curta duração para acessar recursos da AWS.

a. **Região do AWS IAM Role Anywhere**: Selecione a região para o Cloud Storage Pool. Por exemplo, `us-east-1`.
b. **URNA âncora de confiança**: Insira a URNA da âncora de confiança que valida solicitações de credenciais STS de curta duração. Pode ser uma CA raiz ou intermediária.
c. **URN de perfil**: Insira a URN do perfil de funções do IAM em qualquer lugar que lista as funções que são assumíveis para qualquer pessoa confiável.
d. **Role URN**: Insira a URNA do papel do IAM que é assumível para qualquer pessoa confiável.
e. **Duração da sessão**: Insira a duração das credenciais de segurança temporárias e da sessão de função. Introduza pelo menos 15 minutos e não mais de 12 horas.
f. **Certificado de CA do servidor** (opcional): Um ou mais certificados de CA confiáveis, em formato PEM, para verificar as funções do IAM em qualquer servidor. Se omitido, o servidor não será verificado.
g. **Certificado de entidade final**: A chave pública, em formato PEM, do certificado X509 assinado pela âncora fiduciária. As funções do AWS IAM em qualquer lugar usam essa chave para emitir um token STS.
h. **Chave privada da entidade final**: A chave privada para o certificado da entidade final.

CAP (portal de acesso C2S)

Para serviços comerciais de nuvem (C2S) S3 Service

a. **URL de credenciais temporárias**: Insira o URL completo que o StorageGRID usará para obter credenciais temporárias do SERVIDOR CAP, incluindo todos os parâmetros de API necessários e opcionais atribuídos à sua conta C2S.
b. **Certificado CA do servidor**: Selecione **Procurar** e carregue o certificado CA que o StorageGRID usará para verificar o servidor CAP. O certificado deve ser codificado em PEM e emitido por uma autoridade de certificação governamental (CA) apropriada.
c. **Certificado do cliente**: Selecione **Procurar** e carregue o certificado que o StorageGRID usará para se identificar no servidor CAP. O certificado de cliente deve ser codificado em PEM, emitido por uma autoridade de certificação governamental (CA) adequada e ter acesso à sua conta C2S.
d. **Chave privada do cliente**: Selecione **Procurar** e carregue a chave privada codificada pelo PEM para o certificado do cliente.
e. Se a chave privada do cliente estiver encriptada, introduza a frase-passe para desencriptar a chave privada do cliente. Caso contrário, deixe o campo **Client private key passphrase** em branco.

Se o certificado de cliente for encriptado, utilize o formato tradicional para a encriptação. O formato criptografado PKCS nº 8 não é suportado.

Storage Blob do Azure

Para armazenamento de Blobs do Azure, somente chave compartilhada

a. **Nome da conta**: Insira o nome da conta de armazenamento que possui o contentor externo
b. **Chave de conta**: Insira a chave secreta da conta de armazenamento

Você pode usar o portal do Azure para encontrar esses valores.

Anônimo

Nenhuma informação adicional é necessária.

5. Selecione **continuar**. Em seguida, escolha o tipo de verificação de servidor que você deseja usar:

Opção	Descrição
Use certificados de CA raiz no SO nó de armazenamento	Use os certificados Grid CA instalados no sistema operacional para proteger conexões.
Use certificado CA personalizado	Use um certificado de CA personalizado. Selecione **Procurar** e carregue o certificado codificado em PEM.
Não verifique o certificado	Selecionar esta opção significa que as ligações TLS ao Cloud Storage Pool não são seguras.

6. Selecione **Guardar**.

   Quando você salva um pool de storage de nuvem, o StorageGRID faz o seguinte:

   - Valida que o bucket ou o contentor e o endpoint de serviço existem e que eles podem ser alcançados usando as credenciais que você especificou.
   - Grava um arquivo de marcador no bucket ou no contêiner para identificá-lo como um pool de armazenamento em nuvem. Nunca remova esse arquivo, que é `x-ntap-sgws-cloud-pool-uuid` chamado .

     Se a validação do Cloud Storage Pool falhar, você receberá uma mensagem de erro que explica por que a validação falhou. Por exemplo, um erro pode ser relatado se houver um erro de certificado ou se o bucket ou contentor especificado ainda não existir.

7. Se ocorrer um erro, consulte o "Instruções para solução de problemas de Cloud Storage Pools", resolva quaisquer problemas e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Veja os detalhes do Cloud Storage Pool

Você pode exibir os detalhes de um pool de storage de nuvem para determinar onde ele é usado e ver quais nós e categorias de storage estão incluídos.

Antes de começar

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

Passos

1. Selecione **ILM** > **Storage Pools** > **Cloud Storage Pools**.

   A tabela Cloud Storage Pools inclui as seguintes informações para cada pool de storage de nuvem que inclui nós de storage:

   - **Nome**: O nome de exibição exclusivo da piscina.
   - * URI*: O identificador de recurso uniforme do pool de armazenamento em nuvem.
   - **Tipo de provedor**: Qual provedor de nuvem é usado para este pool de armazenamento em nuvem.
   - **Container**: O nome do bucket usado para o Cloud Storage Pool.
   - **Uso de ILM**: Como o pool está sendo usado atualmente. Um pool de storage em nuvem pode não ser usado ou pode ser usado em uma ou mais regras de ILM, perfis de codificação de apagamento ou ambos.
   - **Último erro**: O último erro detetado durante uma verificação de integridade deste Cloud Storage Pool.

2. Para exibir detalhes de um pool de armazenamento em nuvem específico, selecione seu nome.

   A página de detalhes do pool é exibida.

3. Exiba a guia **Autenticação** para saber mais sobre o tipo de autenticação deste pool de armazenamento em nuvem e editar os detalhes de autenticação.
4. Veja a guia **Verificação do servidor** para saber mais sobre detalhes de verificação, editar verificação, baixar um novo certificado ou copiar o PEM do certificado.
5. Exiba a guia **uso de ILM** para determinar se o Cloud Storage Pool está sendo usado atualmente em quaisquer regras de ILM ou perfis de codificação de apagamento.
6. Opcionalmente, vá para a página **regras ILM** para "saiba mais e gerencie quaisquer regras"usar o Cloud Storage Pool.

Edite um pool de armazenamento em nuvem

Você pode editar um pool de armazenamento em nuvem para alterar seu nome, ponto de extremidade de serviço ou outros detalhes; no entanto, não é possível alterar o bucket do S3 ou o contentor do Azure para um pool de armazenamento em nuvem.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você revisou o "Considerações para pools de storage em nuvem".

Passos

1. Selecione **ILM** > **Storage Pools** > **Cloud Storage Pools**.

   A tabela Cloud Storage Pools lista os pools de armazenamento em nuvem existentes.

2. Marque a caixa de seleção do pool de armazenamento em nuvem que deseja editar e selecione **ações** > **Editar**.

Como alternativa, selecione o nome do pool de armazenamento em nuvem e, em seguida, selecione **Editar**.

3. Conforme necessário, altere o nome do Cloud Storage Pool, o ponto de extremidade do serviço, as credenciais de autenticação ou o método de verificação de certificado.

   > Não é possível alterar o tipo de provedor, o bucket do S3 ou o contentor do Azure para um pool de armazenamento em nuvem.

   Se você carregou anteriormente um certificado de servidor ou cliente, poderá expandir o acordeão **Detalhes do certificado** para rever o certificado que está atualmente em uso.

4. Selecione **Guardar**.

   Quando você salva um pool de armazenamento em nuvem, o StorageGRID valida que o bucket ou o contentor e o endpoint de serviço existem e que eles podem ser alcançados usando as credenciais especificadas.

   Se a validação do Cloud Storage Pool falhar, uma mensagem de erro será exibida. Por exemplo, um erro pode ser relatado se houver um erro de certificado.

   Consulte as instruções do "Solução de problemas de Cloud Storage Pools", resolva o problema e tente salvar o pool de armazenamento em nuvem novamente.

Remova um pool de armazenamento em nuvem

Você pode remover um Cloud Storage Pool se ele não for usado em uma regra ILM e não contiver dados de objeto.

Antes de começar

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

Se necessário, use o ILM para mover dados de objeto

Se o pool de armazenamento em nuvem que você deseja remover contiver dados de objeto, use o ILM para mover os dados para um local diferente. Por exemplo, você pode mover os dados para nós de storage na grade ou para um pool de storage de nuvem diferente.

Passos

1. Selecione **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Veja a coluna de uso do ILM na tabela para determinar se você pode remover o pool de armazenamento em nuvem.

   Não é possível remover um Cloud Storage Pool se ele estiver sendo usado em uma regra ILM ou em um perfil de codificação de apagamento.

3. Se o Cloud Storage Pool estiver sendo usado, selecione ***cloud storage pool name*** > **ILM usage**.
4. "Clonar cada regra de ILM" Que atualmente coloca objetos no pool de armazenamento em nuvem que você deseja remover.
5. Determine onde você deseja mover os objetos existentes gerenciados por cada regra clonada.

Você pode usar um ou mais pools de storage ou outro pool de storage de nuvem.

6. Edite cada uma das regras que clonou.

   Para a Etapa 2 do assistente criar regra ILM, selecione o novo local no campo **Copies at**.

7. "Crie uma nova política ILM" e substituir cada uma das regras antigas por uma regra clonada.
8. Ative a nova política.
9. Aguarde que o ILM remova objetos do pool de armazenamento em nuvem e os coloque no novo local.

Excluir Cloud Storage Pool

Quando o pool de armazenamento em nuvem está vazio e não é usado em nenhuma regra ILM, você pode excluí-lo.

Antes de começar

- Você removeu quaisquer regras ILM que possam ter usado o pool.
- Você confirmou que o bucket do S3 ou o contentor do Azure não contém nenhum objeto.

  Um erro ocorre se você tentar remover um pool de armazenamento em nuvem se ele contém objetos. "Solucionar problemas em Cloud Storage Pools"Consulte .

> Quando você cria um pool de storage de nuvem, o StorageGRID grava um arquivo de marcador no bucket ou no contentor para identificá-lo como um pool de storage de nuvem. Não remova esse arquivo, que é `x-ntap-sgws-cloud-pool-uuid` chamado .

Passos

1. Selecione **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Se a coluna de uso do ILM indicar que o Cloud Storage Pool não está sendo usado, marque a caixa de seleção.
3. Selecione **ações** > **Remover**.
4. Selecione **OK**.

Solucionar problemas em Cloud Storage Pools

Use estas etapas de solução de problemas para ajudar a resolver erros que você pode encontrar ao criar, editar ou excluir um pool de armazenamento em nuvem.

Determine se ocorreu um erro

O StorageGRID executa uma verificação de integridade simples em cada pool de armazenamento em nuvem lendo o objeto conhecido `x-ntap-sgws-cloud-pool-uuid` para garantir que o pool de armazenamento em nuvem possa ser acessado e esteja funcionando corretamente. Quando o StorageGRID encontra um erro no endpoint, ele executa uma verificação de integridade a cada minuto a partir de cada nó de storage. Quando o erro é resolvido, as verificações de integridade param. Se uma verificação de integridade detetar um problema, uma mensagem será exibida na coluna último erro da tabela Cloud Storage Pools na página Storage Pools.

A tabela mostra o erro mais recente detetado para cada pool de armazenamento em nuvem e indica há quanto tempo o erro ocorreu.

Além disso, um alerta de **erro de conetividade do Cloud Storage Pool** é acionado se a verificação de integridade detetar que um ou mais novos erros do Cloud Storage Pool ocorreram nos últimos 5 minutos. Se você receber uma notificação por e-mail para esse alerta, vá para a página pools de armazenamento (selecione **ILM** > **pools de armazenamento**), revise as mensagens de erro na coluna último erro e consulte as diretrizes de solução de problemas abaixo.

Verifique se um erro foi resolvido

Depois de resolver quaisquer problemas subjacentes, você pode determinar se o erro foi resolvido. Na página Cloud Storage Pool, selecione o ponto final e selecione **Limpar erro**. Uma mensagem de confirmação indica que o StorageGRID apagou o erro do pool de armazenamento em nuvem.

Se o problema subjacente tiver sido resolvido, a mensagem de erro já não é apresentada. No entanto, se o problema subjacente não foi corrigido (ou se um erro diferente for encontrado), a mensagem de erro será mostrada na coluna último erro dentro de alguns minutos.

Erro: Falha na verificação de integridade. Erro do endpoint

Você pode encontrar esse erro ao ativar o bloqueio de objetos S3 com retenção padrão para o bucket do Amazon S3 depois de começar a usar esse bucket em um pool de armazenamento em nuvem. Esse erro ocorre quando a operação PUT não tem um cabeçalho HTTP com um valor de checksum de payload, como `Content-MD5`. Esse valor de cabeçalho é exigido pela AWS para COLOCAR operações em buckets com o S3 Object Lock ativado.

Para corrigir esse problema, siga as etapas em "Edite um pool de armazenamento em nuvem" sem fazer alterações. Essa ação aciona a validação da configuração do Cloud Storage Pool que deteta e atualiza automaticamente o sinalizador S3 Object Lock em uma configuração de endpoint do Cloud Storage Pool.

Erro: Este pool de armazenamento em nuvem contém conteúdo inesperado

Você pode encontrar esse erro ao tentar criar, editar ou excluir um pool de armazenamento em nuvem. Esse erro ocorre se o intervalo ou contentor incluir o `x-ntap-sgws-cloud-pool-uuid` arquivo marcador, mas esse arquivo não tiver o campo metadados com o UUID esperado.

Normalmente, você só verá esse erro se estiver criando um novo pool de armazenamento em nuvem e outra instância do StorageGRID já estiver usando o mesmo pool de armazenamento em nuvem.

Tente estas etapas para corrigir o problema:

- Verifique se ninguém na sua organização também está usando este pool de armazenamento em nuvem.
- Exclua todos os objetos existentes dentro do intervalo de destino, incluindo o `x-ntap-sgws-cloud-pool-uuid` arquivo, e tente configurar o pool de armazenamento do Cloud novamente.

Erro: Não foi possível criar ou atualizar o Cloud Storage Pool. Erro do endpoint

Pode encontrar este erro nas seguintes circunstâncias:

- Quando você tenta criar ou editar um pool de armazenamento em nuvem.
- Quando você seleciona uma combinação de plataforma, autenticação ou protocolo sem suporte com o bloqueio de objetos S3 durante a configuração de um novo pool de armazenamento em nuvem. "Considerações para pools de storage em nuvem"Consulte .

Esse erro indica que um problema de conetividade ou configuração está impedindo a gravação do StorageGRID no pool de armazenamento em nuvem.

Para corrigir o problema, revise a mensagem de erro do endpoint.

- Se a mensagem de erro contiver `Get *url*: EOF`, verifique se o endpoint de serviço usado para o Cloud Storage Pool não usa HTTP para um contentor ou bucket que requer HTTPS.
- Se a mensagem de erro contiver `Get *url*: net/http: request canceled while waiting for connection`, verifique se a configuração de rede permite que os nós de armazenamento acessem o endpoint de serviço usado para o pool de armazenamento em nuvem.
- Se o erro se dever a uma plataforma, autenticação ou protocolo não suportados, altere para uma configuração suportada com o bloqueio de objetos S3 e tente salvar o novo pool de armazenamento em nuvem novamente.
- Para todas as outras mensagens de erro de endpoint, tente uma ou mais das seguintes opções:
  - Crie um recipiente ou bucket externo com o mesmo nome que você inseriu para o Cloud Storage Pool e tente salvar o novo Cloud Storage Pool novamente.
  - Corrija o nome do recipiente ou do bucket especificado para o pool de armazenamento em nuvem e tente salvar o novo pool de armazenamento em nuvem novamente.

Erro: Falha ao analisar o certificado CA

Você pode encontrar esse erro ao tentar criar ou editar um pool de armazenamento em nuvem. O erro ocorre se o StorageGRID não puder analisar o certificado digitado ao configurar o pool de armazenamento em nuvem.

Para corrigir o problema, verifique se há problemas no certificado da CA fornecido.

Erro: Um pool de armazenamento em nuvem com esta ID não foi encontrado

Você pode encontrar esse erro ao tentar editar ou excluir um pool de armazenamento em nuvem. Esse erro ocorre se o endpoint retornar uma resposta 404, o que pode significar uma das seguintes opções:

- As credenciais usadas para o Cloud Storage Pool não têm permissão de leitura para o bucket.
- O intervalo usado para o pool de armazenamento em nuvem não inclui o `x-ntap-sgws-cloud-pool-uuid` arquivo de marcador.

Tente um ou mais destes passos para corrigir o problema:

- Verifique se o usuário associado à chave de acesso configurada tem as permissões necessárias.
- Edite o Cloud Storage Pool com credenciais que tenham as permissões necessárias.
- Se as permissões estiverem corretas, entre em Contato com o suporte.

Erro: Não foi possível verificar o conteúdo do pool de armazenamento em nuvem. Erro do endpoint

Você pode encontrar esse erro ao tentar excluir um pool de armazenamento em nuvem. Esse erro indica que algum tipo de problema de conetividade ou configuração está impedindo o StorageGRID de ler o conteúdo do bucket do pool de armazenamento em nuvem.

Para corrigir o problema, revise a mensagem de erro do endpoint.

Erro: Os objetos já foram colocados neste intervalo

Você pode encontrar esse erro ao tentar excluir um pool de armazenamento em nuvem. Não é possível excluir um Cloud Storage Pool se ele contiver dados que foram movidos pelo ILM, dados que estavam no bucket

antes de configurar o Cloud Storage Pool ou dados que foram colocados no bucket por outra fonte após a criação do Cloud Storage Pool.

Tente um ou mais destes passos para corrigir o problema:

- Siga as instruções para mover objetos de volta para o StorageGRID em "ciclo de vida de um objeto de pool de armazenamento em nuvem".
- Se você tiver certeza de que os objetos restantes não foram colocados no Cloud Storage Pool pelo ILM, exclua manualmente os objetos do bucket.

> Nunca exclua manualmente objetos de um pool de armazenamento em nuvem que possam ter sido colocados lá pelo ILM. Se você tentar acessar um objeto excluído manualmente do StorageGRID, o objeto excluído não será encontrado.

Erro: O proxy encontrou um erro externo ao tentar alcançar o pool de armazenamento em nuvem

Você pode encontrar esse erro se tiver configurado um proxy de armazenamento não transparente entre nós de armazenamento e o endpoint S3 externo usado para o Cloud Storage Pool. Esse erro ocorre se o servidor proxy externo não conseguir alcançar o ponto de extremidade do Cloud Storage Pool. Por exemplo, o servidor DNS pode não conseguir resolver o nome do host ou pode haver um problema de rede externo.

Tente um ou mais destes passos para corrigir o problema:

- Verifique as configurações do pool de armazenamento em nuvem (**ILM** > **pools de armazenamento**).
- Verifique a configuração de rede do servidor proxy de armazenamento.

Erro: O certificado X,509 está fora do período de validade

Você pode encontrar esse erro ao tentar excluir um pool de armazenamento em nuvem. Esse erro ocorre quando a autenticação requer um certificado X,509 para garantir que o pool de armazenamento externo correto seja validado e o pool externo esteja vazio antes que a configuração do pool de armazenamento em nuvem seja excluída.

Tente estas etapas para corrigir o problema:

- Atualize o certificado configurado para autenticação para o Cloud Storage Pool.
- Certifique-se de que qualquer alerta de expiração de certificado neste Cloud Storage Pool esteja resolvido.

Informações relacionadas

"Ciclo de vida de um objeto Cloud Storage Pool"

Gerenciar perfis de codificação de apagamento

Você pode exibir os detalhes de um perfil de codificação de apagamento e renomear um perfil, se necessário. Você pode desativar um perfil de codificação de apagamento se ele não for usado atualmente em nenhuma regra ILM.

Antes de começar

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

Ver detalhes do perfil de codificação de apagamento

Você pode visualizar os detalhes de um perfil de codificação de apagamento para determinar seu status, o esquema de codificação de apagamento usado e outras informações.

Passos

1. Selecione **CONFIGURATION** > **System** > **Erasure coding**.
2. Selecione o perfil. É apresentada a página de detalhes do perfil.
3. Opcionalmente, exiba a guia regras ILM para obter uma lista de regras ILM que usam o perfil e as políticas ILM que usam essas regras.
4. Como opção, exiba a guia nós de storage para obter detalhes sobre cada nó de storage no pool de storage do perfil, como o local onde ele está localizado e o uso do storage.

Renomeie um perfil de codificação de apagamento

Você pode querer renomear um perfil de codificação de apagamento para torná-lo mais óbvio o que o perfil faz.

Passos

1. Selecione **CONFIGURATION** > **System** > **Erasure coding**.
2. Selecione o perfil que deseja renomear.
3. Selecione **Renomear**.
4. Insira um nome exclusivo para o perfil de codificação de apagamento.

   O nome do perfil de codificação de apagamento é anexado ao nome do pool de armazenamento na instrução de colocação de uma regra ILM.

   > Os nomes de perfis de codificação de apagamento devem ser exclusivos. Um erro de validação ocorre se você usar o nome de um perfil existente, mesmo que esse perfil tenha sido desativado.

5. Selecione **Guardar**.

Desativar um perfil de codificação de apagamento

Você pode desativar um perfil de codificação de apagamento se você não planeja mais usá-lo e se o perfil não for usado atualmente em nenhuma regra ILM.

> Confirme se não estão em curso operações de reparo de dados codificados por apagamento ou procedimentos de desativação. Uma mensagem de erro será retornada se você tentar desativar um perfil de codificação de apagamento enquanto qualquer uma dessas operações estiver em andamento.

Sobre esta tarefa

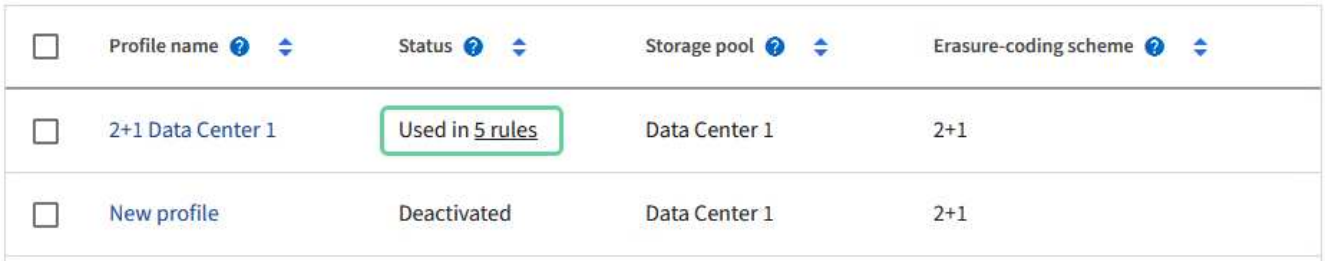
O StorageGRID impede que você desative um perfil de codificação de apagamento se uma das seguintes opções for verdadeira:

- O perfil de codificação de apagamento é usado atualmente em uma regra ILM.
- O perfil de codificação de apagamento não é mais usado em nenhuma regra ILM, mas os dados de objetos e fragmentos de paridade para o perfil ainda existem.

Passos

1. Selecione **CONFIGURATION** > **System** > **Erasure coding**.
2. Na guia Ativo, revise a coluna **Status** para confirmar que o perfil de codificação de apagamento que você deseja desativar não é usado em nenhuma regra ILM.

   Você não pode desativar um perfil de codificação de apagamento se ele for usado em qualquer regra ILM. No exemplo, o perfil 2 mais 1 Data Center 1 é usado em pelo menos uma regra ILM.



3. Se o perfil for usado em uma regra ILM, siga estas etapas:
   a. Selecione **ILM** > **regras**.
   b. Selecione cada regra e revise o diagrama de retenção para determinar se a regra usa o perfil de codificação de apagamento que você deseja desativar.
   c. Se a regra ILM usar o perfil de codificação de apagamento que você deseja desativar, determine se a regra é usada em qualquer política ILM.
   d. Conclua as etapas adicionais na tabela, com base em onde o perfil de codificação de apagamento é usado.

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Nunca usado em nenhuma regra ILM	Não são necessários passos adicionais. Continue com este procedimento.	*Nenhum*
Em uma regra ILM que nunca foi usada em nenhuma política ILM	i. Edite ou exclua todas as regras ILM afetadas. Se você editar a regra, remova todos os canais que usam o perfil de codificação de apagamento. ii. Continue com este procedimento.	"Trabalhe com regras ILM e políticas ILM"

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra ILM que está atualmente em uma política ILM ativa	i. Clonar a política. ii. Remova a regra ILM que usa o perfil de codificação de apagamento. iii. Adicione uma ou mais novas regras ILM para garantir que os objetos estejam protegidos. iv. Salve, simule e ative a nova política. v. Aguarde que a nova política seja aplicada e que os objetos existentes sejam movidos para novos locais com base nas novas regras adicionadas. **Observação:** dependendo do número de objetos e do tamanho do seu sistema StorageGRID, pode levar semanas ou até meses para que as operações do ILM movam os objetos para novos locais, com base nas novas regras do ILM. Embora você possa tentar desativar um perfil de codificação de apagamento com segurança enquanto ele ainda estiver associado a dados, a operação de desativação falhará. Uma mensagem de erro irá informá-lo se o perfil ainda não está pronto para ser desativado. vi. Edite ou exclua a regra que você removeu da política. Se você editar a regra, remova todos os canais que usam o perfil de codificação de apagamento. vii. Continue com este procedimento.	"Crie uma política ILM" "Trabalhe com regras ILM e políticas ILM"
Em uma regra ILM que está atualmente em uma política ILM	i. Edite a política. ii. Remova a regra ILM que usa o perfil de codificação de apagamento. iii. Adicione uma ou mais novas regras ILM para garantir que todos os objetos estejam protegidos. iv. Salve a política. v. Edite ou exclua a regra que você removeu da política. Se você editar a regra, remova todos os canais que usam o perfil de codificação de apagamento. vi. Continue com este procedimento.	"Crie uma política ILM" "Trabalhe com regras ILM e políticas ILM"

e. Atualize a página Perfis de codificação de apagamento para garantir que o perfil não seja usado em uma regra ILM.

4. Se o perfil não for usado em uma regra ILM, selecione o botão de opção e selecione **Deactivate**. A caixa de diálogo Desativar perfil de codificação de apagamento é exibida.

> Você pode selecionar vários perfis para desativar ao mesmo tempo, desde que cada perfil não seja usado em nenhuma regra.

5. Se tiver a certeza de que pretende desativar o perfil, selecione **Desativar**.

Resultados

- Se o StorageGRID for capaz de desativar o perfil de codificação de apagamento, seu status será desativado. Você não pode mais selecionar este perfil para qualquer regra ILM. Não é possível reativar um perfil desativado.
- Se o StorageGRID não conseguir desativar o perfil, é apresentada uma mensagem de erro. Por exemplo, uma mensagem de erro será exibida se os dados do objeto ainda estiverem associados a esse perfil. Talvez seja necessário esperar várias semanas antes de tentar novamente o processo de desativação.

Configurar regiões (opcional e apenas S3)

As regras do ILM podem filtrar objetos com base nas regiões em que os buckets do S3 são criados, permitindo armazenar objetos de diferentes regiões em diferentes locais de armazenamento.

Se você quiser usar uma região de bucket do S3 como filtro em uma regra, primeiro crie as regiões que podem ser usadas pelos buckets do sistema.

> Não é possível alterar a região de um bucket após o bucket ter sido criado.

Antes de começar

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

Sobre esta tarefa

Ao criar um bucket do S3, você pode especificar que o bucket seja criado em uma região específica. A especificação de uma região permite que o bucket esteja geograficamente próximo de seus usuários, o que pode ajudar a otimizar a latência, minimizar custos e atender aos requisitos regulatórios.

Ao criar uma regra ILM, você pode querer usar a região associada a um bucket do S3 como um filtro avançado. Por exemplo, você pode criar uma regra que se aplique apenas a objetos em buckets do S3 criados na `us-west-2` região. Em seguida, é possível especificar que as cópias desses objetos serão colocadas em nós de storage em um local de data center nessa região para otimizar a latência.

Ao configurar regiões, siga estas diretrizes:

- Por padrão, todos os buckets são considerados como pertencentes à `us-east-1` região.
- Você deve criar as regiões usando o Gerenciador de Grade antes de especificar uma região não padrão ao criar buckets usando o Gerenciador de locatário ou a API de gerenciamento de locatário ou com o elemento de solicitação de LocationConstraint para solicitações de API de bucket do S3 PUT. Um erro ocorre se uma solicitação COLOCAR balde usar uma região que não foi definida no StorageGRID.
- Você deve usar o nome exato da região ao criar o bucket do S3. Os nomes de região são sensíveis a maiúsculas e minúsculas. Os carateres válidos são números, letras e hífens.

A UE não é considerada um apelido para a ue-oeste-1. Se você quiser usar a região da UE ou da ue-oeste-1, você deve usar o nome exato.

- Não é possível excluir ou modificar uma região se ela for usada em uma regra atribuída a qualquer política (ativa ou inativa).
- Se você usar uma região inválida como filtro avançado em uma regra ILM, não será possível adicionar essa regra a uma política.

  Uma região inválida pode resultar se você usar uma região como um filtro avançado em uma regra ILM, mas excluir essa região posteriormente, ou se você usar a API de Gerenciamento de Grade para criar uma regra e especificar uma região que você não definiu.

- Se você excluir uma região depois de usá-la para criar um bucket do S3, será necessário adicionar novamente a região se quiser usar o filtro avançado restrição de localização para encontrar objetos nesse bucket.

Passos

1. Selecione **ILM** > **Regiões**.

   É apresentada a página Regiões, com as regiões atualmente definidas listadas. **Região 1** mostra a região padrão `us-east-1` , que não pode ser modificada ou removida.

2. Para adicionar uma região:
   a. Selecione **Adicionar outra região**.
   b. Insira o nome de uma região que você deseja usar ao criar buckets do S3.

      Você deve usar esse nome exato da região como o elemento de solicitação LocationConstraint ao criar o bucket S3 correspondente.

3. Para remover uma região não utilizada, selecione o ícone de exclusão ✕.

   Uma mensagem de erro será exibida se você tentar remover uma região atualmente usada em qualquer política (ativa ou inativa).

4. Quando terminar de fazer alterações, selecione **Guardar**.

   Agora você pode selecionar essas regiões na seção filtros avançados na etapa 1 do assistente criar regra ILM. "Use filtros avançados nas regras do ILM"Consulte .

Criar regra ILM

Use regras ILM para gerenciar objetos

Para gerenciar objetos, você cria um conjunto de regras de gerenciamento do ciclo de vida das informações (ILM) e as organiza em uma política ILM.

Cada objeto ingerido no sistema é avaliado em relação à política ativa. Quando uma regra na política corresponde aos metadados de um objeto, as instruções na regra determinam quais ações o StorageGRID executa para copiar e armazenar esse objeto.

Os metadados de objetos não são gerenciados pelas regras do ILM. Em vez disso, os metadados de objetos são armazenados em um banco de dados Cassandra no que é conhecido como armazenamento de metadados. Três cópias dos metadados de objetos são mantidas automaticamente em cada local para proteger os dados da perda.

Elementos de uma regra ILM

Uma regra ILM tem três elementos:

- **Critérios de filtragem**: Os filtros básicos e avançados de uma regra definem a que objetos a regra se aplica. Se um objeto corresponder a todos os filtros, o StorageGRID aplicará a regra e criará as cópias de objeto especificadas nas instruções de colocação da regra.
- **Instruções de colocação**: As instruções de colocação de uma regra definem o número, o tipo e a localização das cópias de objetos. Cada regra pode incluir uma sequência de instruções de posicionamento para alterar o número, o tipo e a localização das cópias de objetos ao longo do tempo. Quando o período de tempo para um posicionamento expira, as instruções na próxima colocação são aplicadas automaticamente pela próxima avaliação ILM.
- **Comportamento de ingestão**: O comportamento de ingestão de uma regra permite que você escolha como os objetos filtrados pela regra são protegidos à medida que são ingeridos (quando um cliente S3 salva um objeto na grade).

Filtragem de regras ILM

Quando você cria uma regra ILM, você especifica filtros para identificar quais objetos a regra se aplica.

No caso mais simples, uma regra pode não usar nenhum filtro. Qualquer regra que não use filtros se aplica a todos os objetos, portanto, deve ser a última regra (padrão) em uma política ILM. A regra padrão fornece instruções de armazenamento para objetos que não correspondem aos filtros em outra regra.

- Os filtros básicos permitem que você aplique regras diferentes a grupos grandes e distintos de objetos. Esses filtros permitem que você aplique uma regra a contas de locatário específicas, buckets específicos do S3 ou ambos.

  Os filtros básicos oferecem uma maneira simples de aplicar regras diferentes a um grande número de objetos. Por exemplo, os Registros financeiros da sua empresa podem precisar ser armazenados para atender aos requisitos regulatórios, enquanto os dados do departamento de marketing podem precisar ser armazenados para facilitar as operações diárias. Depois de criar contas de inquilino separadas para cada departamento ou depois de segregar dados dos diferentes departamentos em intervalos separados do S3, você pode facilmente criar uma regra que se aplica a todos os Registros financeiros e uma segunda regra que se aplica a todos os dados de marketing.

- Filtros avançados oferecem controle granular. Você pode criar filtros para selecionar objetos com base nas seguintes propriedades do objeto:
  - Tempo de ingestão
  - Último tempo de acesso
  - Todo ou parte do nome do objeto (chave)
  - Restrição de localização (apenas S3)
  - Tamanho do objeto
  - Metadados do usuário
  - Etiqueta de objeto (apenas S3)

Você pode filtrar objetos em critérios muito específicos. Por exemplo, os objetos armazenados pelo departamento de imagiologia de um hospital podem ser utilizados frequentemente quando têm menos de 30 dias de idade e pouco depois, enquanto os objetos que contêm informações sobre a visita do paciente podem precisar de ser copiados para o departamento de faturação na sede da rede de saúde. Você pode criar filtros que identificam cada tipo de objeto com base no nome, tamanho, tags de objeto S3D ou qualquer outro critério relevante e, em seguida, criar regras separadas para armazenar cada conjunto de objetos adequadamente.

Você pode combinar filtros conforme necessário em uma única regra. Por exemplo, o departamento de marketing pode querer armazenar arquivos de imagem grandes de forma diferente dos Registros de seus fornecedores, enquanto o departamento de recursos humanos pode precisar armazenar Registros de pessoal em uma geografia específica e informações de políticas centralmente. Nesse caso, você pode criar regras que filtram por conta de locatário para segregar os Registros de cada departamento, enquanto usa filtros em cada regra para identificar o tipo específico de objetos aos quais a regra se aplica.

Instruções de colocação de regra ILM

As instruções de posicionamento determinam onde, quando e como os dados do objeto são armazenados. Uma regra ILM pode incluir uma ou mais instruções de colocação. Cada instrução de colocação aplica-se a um único período de tempo.

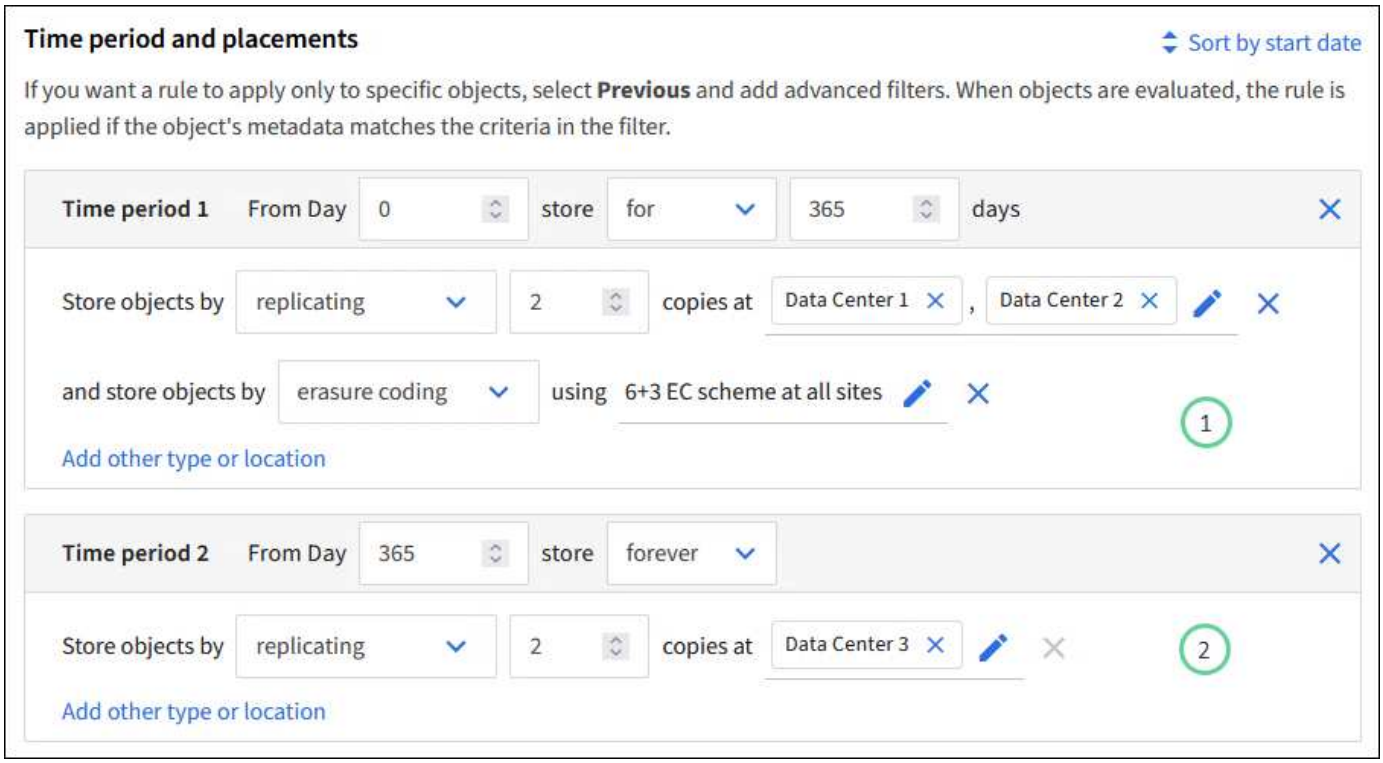
Ao criar instruções de colocação:

- Você começa especificando o tempo de referência, que determina quando as instruções de colocação começam. O tempo de referência pode ser quando um objeto é ingerido, quando um objeto é acessado, quando um objeto versionado se torna não atual ou um tempo definido pelo usuário.
- Em seguida, você especifica quando o posicionamento será aplicado, em relação ao tempo de referência. Por exemplo, uma colocação pode começar no dia 0 e continuar por 365 dias, em relação a quando o objeto foi ingerido.
- Por fim, você especifica o tipo de cópias (replicação ou codificação de apagamento) e o local onde as cópias são armazenadas. Por exemplo, você pode querer armazenar duas cópias replicadas em dois sites diferentes.

Cada regra pode definir vários posicionamentos para um único período de tempo e diferentes posicionamentos para diferentes períodos de tempo.

- Para colocar objetos em vários locais durante um único período de tempo, selecione **Adicionar outro tipo ou local** para adicionar mais de uma linha para esse período de tempo.
- Para colocar objetos em locais diferentes em períodos de tempo diferentes, selecione **Adicionar outro período de tempo** para adicionar o próximo período de tempo. Em seguida, especifique uma ou mais linhas dentro do período de tempo.

O exemplo mostra duas instruções de posicionamento na página Definir posicionamentos do assistente criar regra ILM.



A primeira instrução de colocação (1) tem duas linhas para o primeiro ano:

- A primeira linha cria duas cópias de objeto replicadas em dois locais de data center.
- A segunda linha cria uma cópia codificada por apagamento de mais de 6 3 usando todos os sites de data center.

A segunda instrução de colocação (2) cria duas cópias após um ano e mantém essas cópias para sempre.

Quando você define o conjunto de instruções de colocação para uma regra, você deve garantir que pelo menos uma instrução de colocação comece no dia 0, que não haja lacunas entre os períodos de tempo definidos e que a instrução de colocação final continue para sempre ou até que você não precise mais nenhuma cópia de objeto.

À medida que cada período de tempo na regra expira, as instruções de colocação de conteúdo para o próximo período de tempo são aplicadas. Novas cópias de objetos são criadas e todas as cópias desnecessárias são excluídas.

Comportamento de ingestão de regra de ILM

O comportamento de ingestão controla se as cópias de objeto são imediatamente colocadas de acordo com as instruções na regra, ou se cópias provisórias são feitas e as instruções de posicionamento são aplicadas posteriormente. Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Balanced**: O StorageGRID tenta fazer todas as cópias especificadas na regra ILM no ingest; se isso não for possível, cópias provisórias são feitas e o sucesso é retornado ao cliente. As cópias especificadas na regra ILM são feitas quando possível.
- **Strict**: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido ao cliente.
- * Commit duplo*: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao

cliente. Cópias especificadas na regra ILM são feitas quando possível.

Informações relacionadas

- "Opções de ingestão"
- "Vantagens, desvantagens e limitações das opções de ingestão"
- "Como a consistência e as regras de ILM interagem para afetar a proteção de dados"

Exemplo de regra ILM

Como exemplo, uma regra ILM pode especificar o seguinte:

- Aplicar apenas aos objetos pertencentes ao Locatário A..
- Faça duas cópias replicadas desses objetos e armazene cada cópia em um local diferente.
- Guarde as duas cópias "para sempre", o que significa que o StorageGRID não as eliminará automaticamente. Em vez disso, o StorageGRID manterá esses objetos até que sejam excluídos por uma solicitação de exclusão de cliente ou pela expiração de um ciclo de vida de bucket.
- Use a opção equilibrada para comportamento de ingestão: A instrução de colocação de dois locais é aplicada assim que o locatário A salva um objeto no StorageGRID, a menos que não seja possível fazer imediatamente ambas as cópias necessárias.

  Por exemplo, se o local 2 estiver inacessível quando o locatário A salva um objeto, o StorageGRID fará duas cópias provisórias nos nós de storage no local 1. Assim que o Site 2 estiver disponível, a StorageGRID fará a cópia necessária nesse site.

Informações relacionadas

- "O que é um pool de armazenamento"
- "O que é um Cloud Storage Pool"

Acesse o assistente criar uma regra ILM

As regras do ILM permitem gerenciar o posicionamento dos dados do objeto ao longo do tempo. Para criar uma regra ILM, use o assistente criar uma regra ILM.

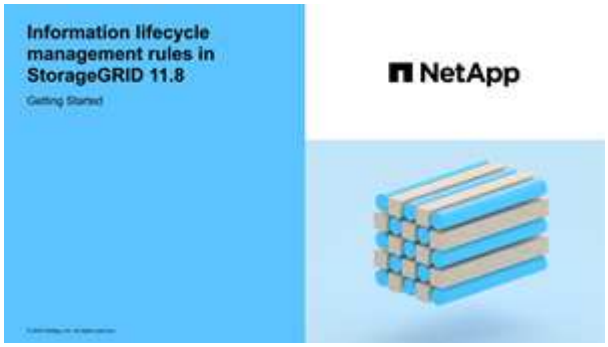
> Se você quiser criar a regra ILM padrão para uma política, siga o "Instruções para criar uma regra ILM padrão" em vez disso.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Se você quiser especificar a que contas de locatário esta regra se aplica, você tem o "Permissão de contas de inquilino"ID da conta ou sabe o ID de cada conta.
- Se você quiser que a regra filtre objetos nos metadados da última hora de acesso, as atualizações da última hora de acesso devem ser habilitadas pelo bucket do S3.
- Você configurou todos os pools de armazenamento em nuvem que planeja usar. "Crie Cloud Storage Pool"Consulte .
- Você está familiarizado com o "opções de ingestão".
- Se você precisar criar uma regra compatível para usar com o bloqueio de objetos S3, você estará

familiarizado com o "Requisitos para o bloqueio de objetos S3".

- Opcionalmente, você assistiu o vídeo: "Vídeo: Visão geral das regras do ILM".



Sobre esta tarefa

Ao criar regras ILM:

- Considere a topologia do sistema StorageGRID e as configurações de storage.
- Considere quais tipos de cópias de objetos você deseja fazer (replicadas ou codificadas para apagamento) e o número de cópias de cada objeto que são necessárias.
- Determine quais tipos de metadados de objetos são usados nos aplicativos que se conetam ao sistema StorageGRID. As regras do ILM filtram objetos com base em seus metadados.
- Considere onde você quer que cópias de objeto sejam colocadas ao longo do tempo.
- Decida qual opção de ingestão usar (Balanced, strict ou Dual Commit).

Passos

1. Selecione **ILM** > **regras**.
2. Selecione **criar**. "Passo 1 (introduzir detalhes)" Do assistente criar uma regra ILM é exibido.

Passo 1 de 3: Insira os detalhes

A etapa **Inserir detalhes** do assistente criar uma regra ILM permite inserir um nome e uma descrição para a regra e definir filtros para a regra.

Inserir uma descrição e definir filtros para a regra são opcionais.

Sobre esta tarefa

Ao avaliar um objeto em relação a um "Regra ILM", o StorageGRID compara os metadados do objeto com os filtros da regra. Se os metadados do objeto corresponderem a todos os filtros, o StorageGRID usará a regra para colocar o objeto. Você pode criar uma regra para aplicar a todos os objetos ou especificar filtros básicos, como uma ou mais contas de locatário ou nomes de bucket, ou filtros avançados, como o tamanho do objeto ou metadados do usuário.

Passos

1. Digite um nome exclusivo para a regra no campo **Nome**.
2. Opcionalmente, insira uma breve descrição para a regra no campo **Description**.

   Você deve descrever o propósito ou função da regra para que você possa reconhecer a regra mais tarde.

3. Opcionalmente, selecione uma ou mais contas de inquilino S3 às quais esta regra se aplica. Se esta regra

se aplicar a todos os inquilinos, deixe este campo em branco.

Se você não tiver a permissão de acesso root ou a permissão Contas do locatário, não será possível selecionar locatários na lista. Em vez disso, insira o ID do locatário ou insira vários IDs como uma cadeia delimitada por vírgulas.

4. Opcionalmente, especifique os buckets do S3 aos quais esta regra se aplica.

   Se **aplica a todos os buckets** estiver selecionado (padrão), a regra se aplica a todos os buckets do S3.

5. Para locatários S3, selecione opcionalmente **Yes** para aplicar a regra apenas a versões de objetos mais antigas em buckets do S3 que tenham o controle de versão habilitado.

   Se selecionar **Sim**, a opção "hora não atual" será selecionada automaticamente para o tempo de referência em "Etapa 2 do assistente criar uma regra ILM".

   > O tempo não atual aplica-se apenas a objetos S3D em buckets habilitados para versionamento. "Operações em buckets, PutBucketControle de versão"Consulte e "Gerencie objetos com o S3 Object Lock".

   Você pode usar essa opção para reduzir o impactos de armazenamento de objetos com controle de versão filtrando versões de objetos não atuais. "Exemplo 4: Regras ILM e política para objetos com versão S3"Consulte .

6. Opcionalmente, selecione **Adicionar um filtro avançado** para especificar filtros adicionais.

   Se você não configurar a filtragem avançada, a regra se aplica a todos os objetos que correspondem aos filtros básicos. Para obter mais informações sobre filtragem avançada, Use filtros avançados nas regras do ILMconsulte e Especifique vários tipos e valores de metadados.

7. Selecione **continuar**. "Passo 2 (definir posicionamentos)" Do assistente criar uma regra ILM é exibido.

Use filtros avançados nas regras do ILM

A filtragem avançada permite criar regras ILM que se aplicam somente a objetos específicos com base em seus metadados. Ao configurar a filtragem avançada para uma regra, você seleciona o tipo de metadados que deseja corresponder, seleciona um operador e especifica um valor de metadados. Quando os objetos são avaliados, a regra ILM é aplicada somente aos objetos que têm metadados correspondentes ao filtro avançado.

A tabela mostra os tipos de metadados que você pode especificar em filtros avançados, os operadores que você pode usar para cada tipo de metadados e os valores de metadados esperados.

Tipo de metadados	Operadores suportados	Valor dos metadados
Tempo de ingestão	• is • não é • é antes • está ligado ou antes • é depois • está ligado ou depois	Hora e data em que o objeto foi ingerido. **Observação:** para evitar problemas de recursos ao ativar uma nova política ILM, você pode usar o filtro avançado de tempo de ingestão em qualquer regra que possa alterar a localização de grandes números de objetos existentes. Defina o tempo de ingestão para ser maior ou igual ao tempo aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.
Chave	• igual a • não é igual • contém • não contém • começa com • não começa com • termina com • não termina com	Toda ou parte de uma chave de objeto S3 única. Por exemplo, você pode querer combinar objetos que terminam com `.txt` ou começam `test-object/` com .
Último tempo de acesso	• is • não é • é antes • está ligado ou antes • é depois • está ligado ou depois	Hora e data em que o objeto foi recuperado pela última vez (lido ou visualizado). **Observação:** se você planeja "use o último tempo de acesso"como um filtro avançado, as atualizações do último tempo de acesso devem estar ativadas para o bucket do S3.
Restrição de localização (apenas S3)	• igual a • não é igual	A região onde foi criado um bucket S3. Utilize **ILM** > **Regiões** para definir as regiões que são apresentadas. **Nota:** Um valor de US-East-1 irá corresponder objetos em buckets criados na região US-East-1, bem como objetos em buckets que não têm nenhuma região especificada. "Configurar regiões (opcional e apenas S3)"Consulte .

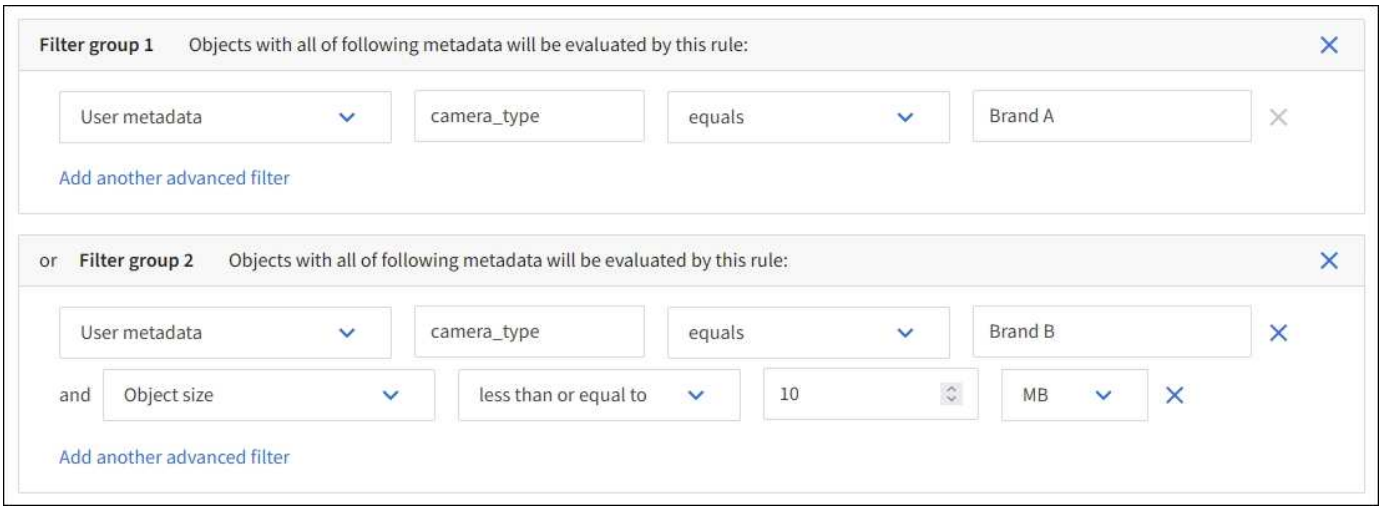
Tipo de metadados	Operadores suportados	Valor dos metadados
Tamanho do objeto	• igual a • não é igual • menos de • inferior ou igual a • superior a. • maior ou igual a	O tamanho do objeto. A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.
Metadados do usuário	• contém • termina com • igual a • existe • começa com • não contém • não termina com • não é igual • não existe • não começa com	Par chave-valor, onde **Nome dos metadados do usuário** é a chave e **valor dos metadados** é o valor. Por exemplo, para filtrar objetos que têm metadados de usuário do `color=blue`, especifique `color` para **Nome de metadados de usuário**, `equals` para o operador e `blue` para **valor de metadados**. **Observação:** os nomes de metadados do usuário não são sensíveis a maiúsculas e minúsculas; os valores de metadados do usuário são sensíveis a maiúsculas e minúsculas.
Etiqueta de objeto (apenas S3)	• contém • termina com • igual a • existe • começa com • não contém • não termina com • não é igual • não existe • não começa com	Par chave-valor, onde **Nome da tag objeto** é a chave e **valor da tag objeto** é o valor. Por exemplo, para filtrar objetos que têm uma tag de objeto de `Image=True`, especifique `Image` para **Nome da tag de objeto**, `equals` para o operador e `True` para **valor da tag de objeto**. **Nota:** nomes de marcas de objetos e valores de tags de objetos são sensíveis a maiúsculas e minúsculas. Você deve inserir esses itens exatamente como eles foram definidos para o objeto.

Especifique vários tipos e valores de metadados

Ao definir filtragem avançada, você pode especificar vários tipos de metadados e vários valores de metadados. Por exemplo, se você quiser que uma regra corresponda a objetos entre 10 MB e 100 MB de tamanho, você selecionaria o tipo de metadados **tamanho do objeto** e especificaria dois valores de metadados.

- O primeiro valor de metadados especifica objetos maiores ou iguais a 10 MB.
- O segundo valor de metadados especifica objetos menores ou iguais a 100 MB.

O uso de várias entradas permite que você tenha controle preciso sobre quais objetos são correspondidos. No exemplo a seguir, a regra se aplica a objetos que têm marca A ou marca B como o valor dos metadados do usuário camera_type. No entanto, a regra só se aplica aos objetos da marca B menores que 10 MB.



Passo 2 de 3: Definir posicionamentos

A etapa **Definir posicionamentos** do assistente criar regra ILM permite definir as instruções de posicionamento que determinam quanto tempo os objetos são armazenados, o tipo de cópias (replicadas ou codificadas por apagamento), o local de armazenamento e o número de cópias.

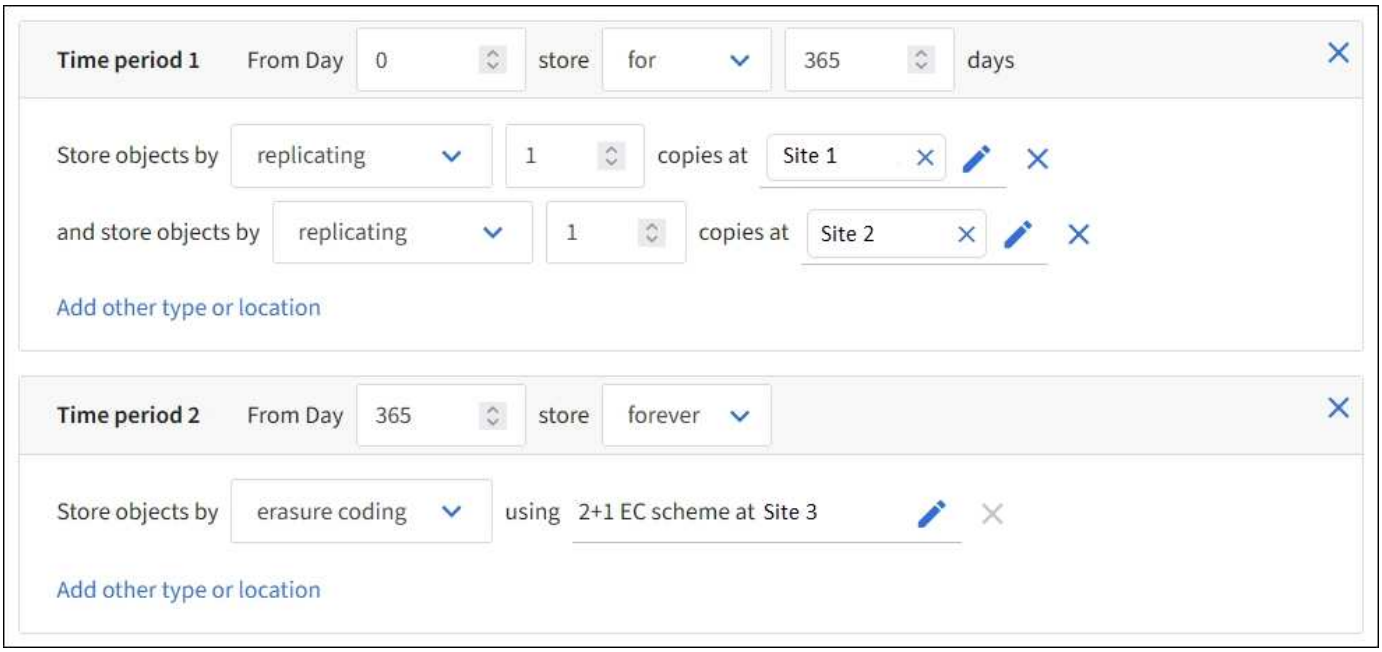
> As capturas de tela mostradas são exemplos. Seus resultados podem variar dependendo da versão do StorageGRID.

Sobre esta tarefa

Uma regra ILM pode incluir uma ou mais instruções de colocação. Cada instrução de colocação aplica-se a um único período de tempo. Quando você usa mais de uma instrução, os períodos de tempo devem ser contíguos, e pelo menos uma instrução deve começar no dia 0. As instruções podem continuar para sempre ou até que você não precise mais nenhuma cópia de objeto.

Cada instrução de colocação pode ter várias linhas se você quiser criar diferentes tipos de cópias ou usar locais diferentes durante esse período de tempo.

Neste exemplo, a regra ILM armazena uma cópia replicada no local 1 e uma cópia replicada no local 2 para o primeiro ano. Após um ano, uma cópia codificada por apagamento de 2 mais de 1 é feita e salva em apenas um local.



Passos

1. Para **tempo de referência**, selecione o tipo de tempo a ser utilizado para calcular a hora de início de uma instrução de colocação.

Opção	Descrição
Tempo de ingestão	O tempo em que o objeto foi ingerido.
Último tempo de acesso	A hora em que o objeto foi recuperado pela última vez (lido ou visualizado). Para usar essa opção, as atualizações do último tempo de acesso devem estar ativadas para o bucket do S3. "Use o último tempo de acesso nas regras do ILM"Consulte a .
Tempo de criação definido pelo utilizador	Um tempo especificado nos metadados definidos pelo usuário.
Hora não atual	"Hora não atual" é selecionado automaticamente se você selecionou **Sim** para a pergunta, "aplicar esta regra apenas a versões de objetos mais antigas (em buckets do S3 com controle de versão ativado)?" em "Etapa 1 do assistente criar uma regra ILM".

   Se você quiser criar uma regra *compliant*, selecione **tempo de ingestão**. "Gerencie objetos com o S3 Object Lock"Consulte a .

2. Na seção **período de tempo e colocações**, insira uma hora de início e uma duração para o primeiro período de tempo.

   Por exemplo, você pode querer especificar onde armazenar objetos para o primeiro ano (*from day 0 store for 365 Days*). Pelo menos uma instrução deve começar no dia 0.

3. Se você quiser criar cópias replicadas:

a. Na lista suspensa **Store Objects by**, selecione **replicing**.

b. Selecione o número de cópias que deseja fazer.

   Um aviso será exibido se você alterar o número de cópias para 1. Uma regra de ILM que cria apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. "Por que você não deve usar replicação de cópia única"Consulte a .

   Para evitar o risco, faça um ou mais dos seguintes procedimentos:

   - Aumente o número de cópias para o período de tempo.
   - Adicione cópias a outros pools de storage ou a um pool de storage de nuvem.
   - Selecione **codificação de apagamento** em vez de **replicação**.

     Você pode ignorar esse aviso com segurança se essa regra já criar várias cópias para todos os períodos de tempo.

c. No campo **Copies at**, selecione os pools de armazenamento que deseja adicionar.

   Se você especificar apenas um pool de armazenamento, esteja ciente de que o StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer nó de armazenamento. Se a grade incluir três nós de storage e você selecionar 4 como o número de cópias, apenas três cópias serão feitas& no. 8212;uma cópia para cada nó de storage.

   O alerta **ILM Placement Unachievable** é acionado para indicar que a regra ILM não pôde ser completamente aplicada.

   Se você especificar mais de um pool de armazenamento, tenha em mente estas regras:

   - O número de cópias não pode ser maior do que o número de pools de armazenamento.
   - Se o número de cópias for igual ao número de pools de storage, uma cópia do objeto será armazenada em cada pool de storage.
   - Se o número de cópias for menor que o número de pools de storage, uma cópia será armazenada no local de ingestão e, em seguida, o sistema distribui as cópias restantes para manter o uso do disco entre os pools balanceado, garantindo que nenhum local receba mais de uma cópia de um objeto.
   - Se os pools de storage se sobreporem (contiverem os mesmos nós de storage), todas as cópias do objeto poderão ser salvas em apenas um local. Por esse motivo, não especifique o pool de storage de todos os nós de storage (StorageGRID 11,6 e anterior) e outro pool de storage.

4. Se você quiser criar uma cópia codificada por apagamento:

   a. Na lista suspensa **armazenar objetos por**, selecione **codificação de apagamento**.

      > A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.

   b. Se você não adicionou um filtro de tamanho de objeto para um valor maior que 200 KB, selecione **anterior** para retornar à Etapa 1. Em seguida, selecione **Adicionar um filtro avançado** e defina um filtro **tamanho do objeto** para qualquer valor maior que 200 KB.

   c. Selecione o pool de armazenamento que deseja adicionar e o esquema de codificação de

apagamento que deseja usar.

O local de storage para uma cópia codificada de apagamento inclui o nome do esquema de codificação de apagamento, seguido do nome do pool de storage.

Os esquemas de codificação de apagamento disponíveis são limitados pelo número de nós de storage no pool de storage selecionado. Um `Recommended` crachá aparece ao lado dos esquemas que fornecem o "melhor proteção ou menor sobrecarga de storage".

5. Opcionalmente:
   a. Selecione **Adicionar outro tipo ou local** para criar cópias adicionais em locais diferentes.
   b. Selecione **Adicionar outro período de tempo** para adicionar diferentes períodos de tempo.

> As exclusões de objetos ocorrem com base nas seguintes configurações:
>
> - Os objetos são automaticamente excluídos no final do período de tempo final, a menos que outro período de tempo termine com **Forever**.
> - Dependendo "definições do período de retenção do balde e do inquilino"do , os objetos podem não ser excluídos mesmo que o período de retenção ILM termine.

6. Se você quiser armazenar objetos em um pool de armazenamento em nuvem:
   a. Na lista suspensa **Store Objects by**, selecione **replicing**.
   b. Selecione o campo **Copies at** e, em seguida, selecione um pool de armazenamento em nuvem.

   Ao usar Cloud Storage Pools, tenha em mente estas regras:

   - Você não pode selecionar mais de um pool de armazenamento em nuvem em uma única instrução de colocação. Da mesma forma, você não pode selecionar um pool de armazenamento em nuvem e um pool de armazenamento na mesma instrução de colocação.
   - Você pode armazenar apenas uma cópia de um objeto em qualquer pool de armazenamento em nuvem. Uma mensagem de erro será exibida se você definir **Copies** como 2 ou mais.
   - Você não pode armazenar mais de uma cópia de objeto em qualquer pool de armazenamento em nuvem ao mesmo tempo. Uma mensagem de erro será exibida se vários posicionamentos que usam um pool de armazenamento em nuvem tiverem datas sobrepostas ou se várias linhas no mesmo posicionamento usarem um pool de armazenamento em nuvem.
   - Você pode armazenar um objeto em um pool de storage de nuvem ao mesmo tempo em que o objeto está sendo armazenado como cópias replicadas ou codificadas por apagamento no StorageGRID. No entanto, você deve incluir mais de uma linha na instrução de colocação para o período de tempo, para que você possa especificar o número e os tipos de cópias para cada local.

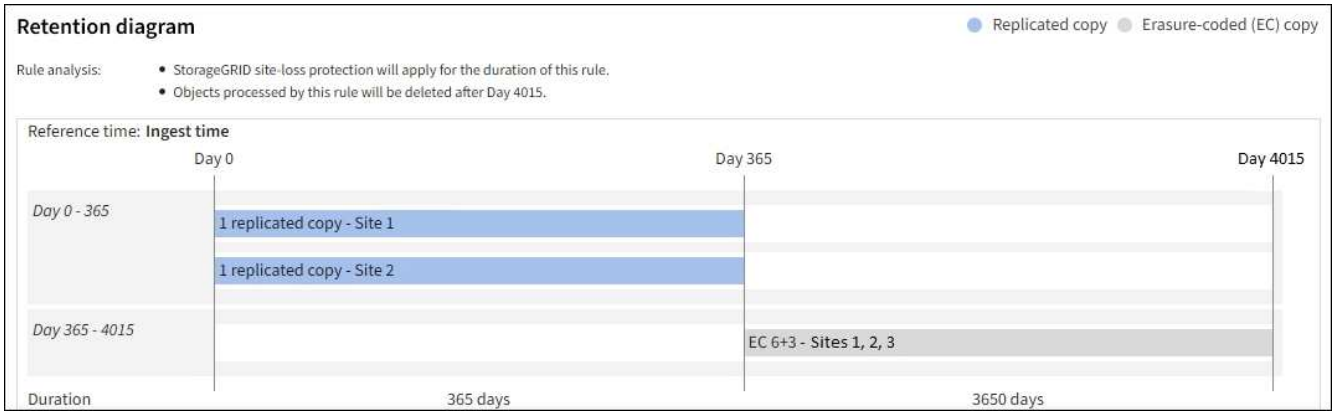
7. No diagrama de retenção, confirme as instruções de colocação.

   Neste exemplo, a regra ILM armazena uma cópia replicada no local 1 e uma cópia replicada no local 2 para o primeiro ano. Depois de um ano e por mais 10 anos, uma cópia codificada por apagamento 6-3 será salva em três sites. Após 11 anos no total, os objetos serão excluídos do StorageGRID.

   A seção análise de regras do diagrama de retenção afirma:

   - A proteção contra perda de site da StorageGRID será aplicada durante a duração desta regra.
   - Os objetos processados por esta regra serão excluídos após o dia 4015.

Consulte "Ativar a proteção contra perda de local."



8. Selecione **continuar**. "Etapa 3 (Selecionar comportamento de ingestão)" Do assistente criar uma regra ILM é exibido.

Use o último tempo de acesso nas regras do ILM

Você pode usar a hora do último acesso como hora de referência em uma regra ILM. Por exemplo, você pode querer deixar objetos que foram visualizados nos últimos três meses em nós de storage local, enquanto move objetos que não foram vistos recentemente para um local externo. Você também pode usar o último tempo de acesso como um filtro avançado se quiser que uma regra ILM se aplique apenas a objetos que foram acessados pela última vez em uma data específica.

Sobre esta tarefa

Antes de usar o último tempo de acesso em uma regra ILM, revise as seguintes considerações:

- Ao usar a hora do último acesso como hora de referência, esteja ciente de que alterar a hora do último acesso de um objeto não aciona uma avaliação ILM imediata. Em vez disso, os posicionamentos do objeto são avaliados e o objeto é movido conforme necessário quando ILM em segundo plano avalia o objeto. Isso pode levar duas semanas ou mais depois que o objeto é acessado.

  Leve essa latência em consideração ao criar regras de ILM com base no último tempo de acesso e evite colocações que usam períodos de tempo curtos (menos de um mês).

- Ao usar o último tempo de acesso como um filtro avançado ou como uma hora de referência, você deve habilitar as atualizações da última hora de acesso para buckets do S3. Pode utilizar a "Gerente do locatário" ou a "API de gerenciamento do locatário".

  As atualizações da última hora de acesso são desativadas por padrão para buckets do S3.

  Esteja ciente de que ativar as atualizações do último tempo de acesso pode reduzir o desempenho, especialmente em sistemas com objetos pequenos. O impactos no desempenho ocorre porque o StorageGRID deve atualizar os objetos com novos timestamps sempre que os objetos são recuperados.

A tabela a seguir resume se o último tempo de acesso é atualizado para todos os objetos no intervalo para diferentes tipos de solicitações.

Tipo de solicitação	Se a última hora de acesso é atualizada quando as atualizações da última hora de acesso são desativadas	Se a última hora de acesso é atualizada quando as atualizações da última hora de acesso estão ativadas
Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados	Não	Sim
Solicitação para atualizar os metadados de um objeto	Sim	Sim
Solicitação para copiar um objeto de um bucket para outro	• Não, para a cópia de origem • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino
Pedido para concluir um carregamento multipart	Sim, para o objeto montado	Sim, para o objeto montado

Passo 3 de 3: Selecione comportamento de ingestão

A etapa **Selecionar comportamento de ingestão** do assistente criar regra ILM permite escolher como os objetos filtrados por essa regra são protegidos à medida que são ingeridos.

Sobre esta tarefa

O StorageGRID pode fazer cópias provisórias e enfileirar os objetos para avaliação do ILM mais tarde, ou pode fazer cópias para cumprir as instruções de colocação da regra imediatamente.

Passos

1. Selecione a "comportamento de ingestão" para utilizar.

   Para obter mais informações, "Vantagens, desvantagens e limitações das opções de ingestão"consulte .

   > Você não pode usar a opção equilibrada ou rigorosa se a regra usar um desses posicionamentos:
   >
   > - Um pool de armazenamento em nuvem no dia 0
   > - Um pool de armazenamento em nuvem quando a regra usa um tempo de criação definido pelo usuário como um tempo de referência
   >
   > "Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"Consulte .

2. Selecione **criar**.

   A regra ILM é criada. A regra não se torna ativa até que seja adicionada a uma "Política de ILM" e essa política seja ativada.

   Para exibir os detalhes da regra, selecione o nome da regra na página regras do ILM.

Crie uma regra ILM padrão

Antes de criar uma política de ILM, você deve criar uma regra padrão para colocar objetos não correspondidos por outra regra na política. A regra padrão não pode usar nenhum filtro. Ele deve se aplicar a todos os locatários, todos os buckets e todas as versões de objetos.

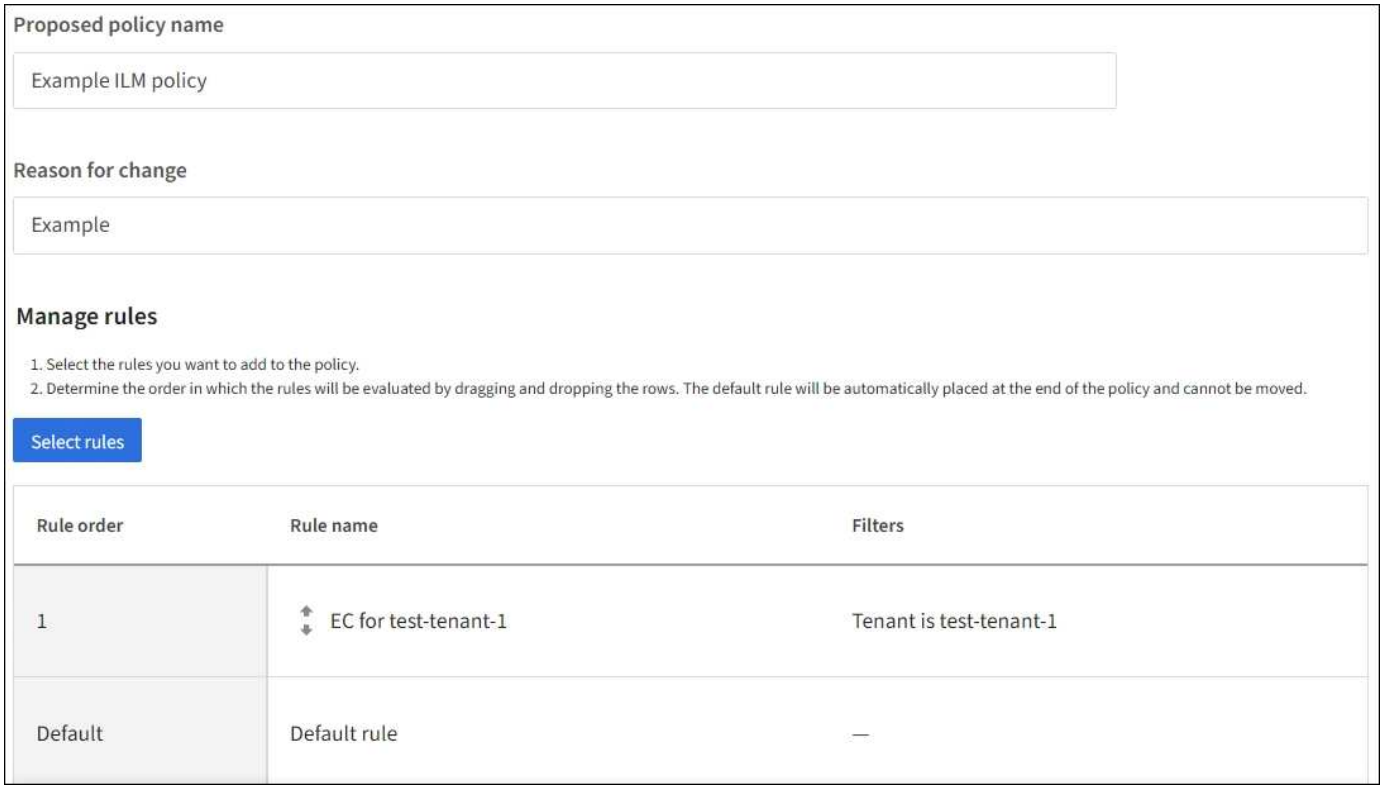
Antes de começar

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

Sobre esta tarefa

A regra padrão é a última regra a ser avaliada em uma política ILM, portanto, ela não pode usar nenhum filtro. As instruções de posicionamento para a regra padrão são aplicadas a quaisquer objetos que não sejam correspondidos por outra regra na política.

Neste exemplo de política, a primeira regra se aplica apenas a objetos pertencentes ao test-tenant-1. A regra padrão, que é a última, aplica-se a objetos pertencentes a todas as outras contas de inquilino.



Ao criar a regra padrão, lembre-se destes requisitos:

- A regra padrão será automaticamente colocada como a última regra quando você a adicionar a uma política.
- A regra padrão não pode usar nenhum filtro básico ou avançado.
- A regra padrão deve ser aplicada a todas as versões de objetos.
- A regra padrão deve criar cópias replicadas.

Não use uma regra que crie cópias codificadas por apagamento como regra padrão para uma política. As regras de codificação de apagamento devem usar um filtro avançado para evitar que objetos menores sejam codificados por apagamento.

- Em geral, a regra padrão deve manter objetos para sempre.
- Se você estiver usando (ou planeja habilitar) a configuração global S3 Object Lock, a regra padrão deve ser compatível.

Passos

1. Selecione **ILM** > **regras**.
2. Selecione **criar**.

   O passo 1 (Inserir detalhes) do assistente criar regra ILM é exibido.

3. Digite um nome exclusivo para a regra no campo **Nome da regra**.
4. Opcionalmente, insira uma breve descrição para a regra no campo **Description**.
5. Deixe o campo **Contas do locatário** em branco.

   A regra padrão deve ser aplicada a todas as contas de locatário.

6. Deixe a seleção suspensa Nome do balde como **aplicável a todos os baldes**.

   A regra padrão deve ser aplicada a todos os buckets do S3.

7. Mantenha a resposta padrão, **não**, para a pergunta: "Aplicar esta regra apenas a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?"
8. Não adicione filtros avançados.

   A regra padrão não pode especificar nenhum filtro.

9. Selecione **seguinte**.

   É apresentado o passo 2 (Definir posicionamentos).

10. Para tempo de referência, selecione qualquer opção.

    Se você manteve a resposta padrão, **não**, para a pergunta, "aplicar esta regra apenas a versões de objetos mais antigas?" A hora não atual não será incluída na lista suspensa. A regra padrão deve aplicar todas as versões de objeto.

11. Especifique as instruções de colocação para a regra padrão.
    - A regra padrão deve manter objetos para sempre. Um aviso aparece quando você ativa uma nova política se a regra padrão não retiver objetos para sempre. Você deve confirmar que este é o comportamento que você espera.
    - A regra padrão deve criar cópias replicadas.

    Não use uma regra que crie cópias codificadas por apagamento como regra padrão para uma política. As regras de codificação de apagamento devem incluir o filtro avançado **Object Size (MB) maior que 200 KB** para evitar que objetos menores sejam codificados por apagamento.

- Se você estiver usando (ou pretende ativar) a configuração global S3 Object Lock, a regra padrão deve ser compatível:
  - Ele precisa criar pelo menos duas cópias de objeto replicadas ou uma cópia codificada por apagamento.
  - Essas cópias devem existir nos nós de storage durante toda a duração de cada linha nas instruções de posicionamento.
  - As cópias de objetos não podem ser salvas em um pool de armazenamento em nuvem.
  - Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando o tempo de ingestão como o tempo de referência.
  - Pelo menos uma linha das instruções de colocação deve ser "para sempre".

12. Veja o diagrama de retenção para confirmar as instruções de colocação.
13. Selecione **continuar**.

    A etapa 3 (Selecionar comportamento de ingestão) é exibida.

14. Selecione a opção de ingestão a utilizar e selecione **criar**.

Gerenciar políticas de ILM

Use políticas ILM

Uma política de gerenciamento de ciclo de vida das informações (ILM) é um conjunto ordenado de regras ILM que determina como o sistema StorageGRID gerencia os dados de objetos ao longo do tempo.

> Uma política de ILM que foi configurada incorretamente pode resultar em perda de dados irrecuperável. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM e simule a política ILM. Confirme sempre que a política de ILM funcionará como pretendido.

Política ILM padrão

Quando você instala o StorageGRID e adiciona sites, uma política ILM padrão é criada automaticamente, da seguinte forma:

- Se a grade contiver um local, a política padrão conterá uma regra padrão que replica duas cópias de cada objeto nesse local.
- Se a grade contiver mais de um local, a regra padrão replicará uma cópia de cada objeto em cada local.

Se a política padrão não atender aos requisitos de storage, você poderá criar suas próprias regras e políticas. "Crie uma regra ILM"Consulte e "Crie uma política ILM".

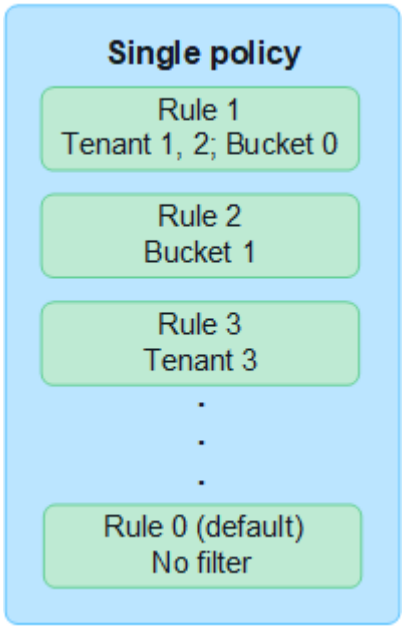
Uma ou muitas políticas ativas de ILM?

Você pode ter uma ou mais políticas ILM ativas de cada vez.

Uma política

Se sua grade usar um esquema simples de proteção de dados com poucas regras específicas do locatário e específicas do bucket, use uma única política de ILM ativa. As regras do ILM podem conter filtros para

gerenciar diferentes buckets ou locatários.



Quando você tiver apenas uma política e os requisitos de um locatário mudarem, você deverá criar uma nova política de ILM ou clonar a política existente para aplicar alterações, simular e ativar a nova política de ILM. Alterações na política ILM podem resultar em movimentos de objetos que podem levar muitos dias e causar latência do sistema.

Várias políticas

Para fornecer diferentes opções de qualidade do serviço aos locatários, é possível ter mais de uma política ativa por vez. Cada política pode gerenciar locatários específicos, buckets do S3 e objetos. Quando você aplica ou altera uma política para um conjunto específico de locatários ou objetos, as políticas aplicadas a outros locatários e objetos não são afetadas.

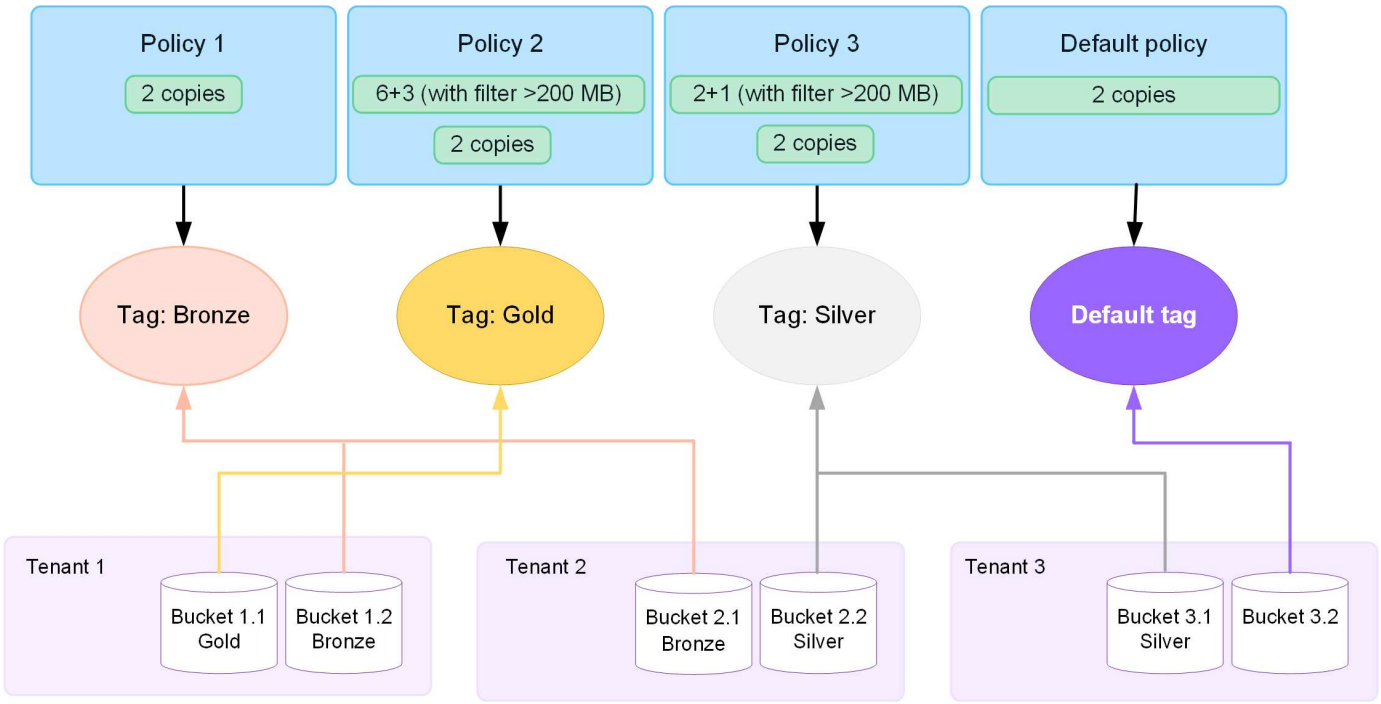
Tags de política ILM

Se você quiser permitir que os locatários alternem facilmente entre várias políticas de proteção de dados por bucket, use várias políticas de ILM com *ILM policy tags*. Você atribui cada política de ILM a uma tag e, em seguida, os locatários marcam um bucket para aplicar a política a esse bucket. Você pode definir tags de política ILM apenas em buckets do S3.

Por exemplo, você pode ter três tags chamadas Ouro, Prata e Bronze. Você pode atribuir uma política de ILM a cada tag, com base em quanto tempo e onde ela armazena objetos. Os locatários podem escolher qual política usar marcando seus buckets. Um bucket com a tag Gold é gerenciado pela política Gold e recebe o nível Gold de proteção e desempenho de dados.

Etiqueta de política ILM padrão

Uma tag de política ILM padrão é criada automaticamente quando você instala o StorageGRID. Cada grade deve ter uma política ativa que é atribuída à tag padrão. A política padrão se aplica a quaisquer buckets S3 não marcados.



Como uma política ILM avalia objetos?

Uma política ILM ativa controla o posicionamento, a duração e a proteção de dados de objetos.

Quando os clientes salvam objetos no StorageGRID, os objetos são avaliados em relação ao conjunto ordenado de regras ILM na política, como segue:

1. Se os filtros da primeira regra na política corresponderem a um objeto, o objeto será ingerido de acordo com o comportamento de ingestão dessa regra e armazenado de acordo com as instruções de colocação dessa regra.
2. Se os filtros da primeira regra não corresponderem ao objeto, o objeto será avaliado em relação a cada regra subsequente na política até que uma correspondência seja feita.
3. Se nenhuma regra corresponder a um objeto, as instruções de comportamento de ingestão e posicionamento da regra padrão na política serão aplicadas. A regra padrão é a última regra de uma política. A regra padrão deve ser aplicada a todos os locatários, todos os buckets do S3 e todas as versões de objetos, e não pode usar nenhum filtro avançado.

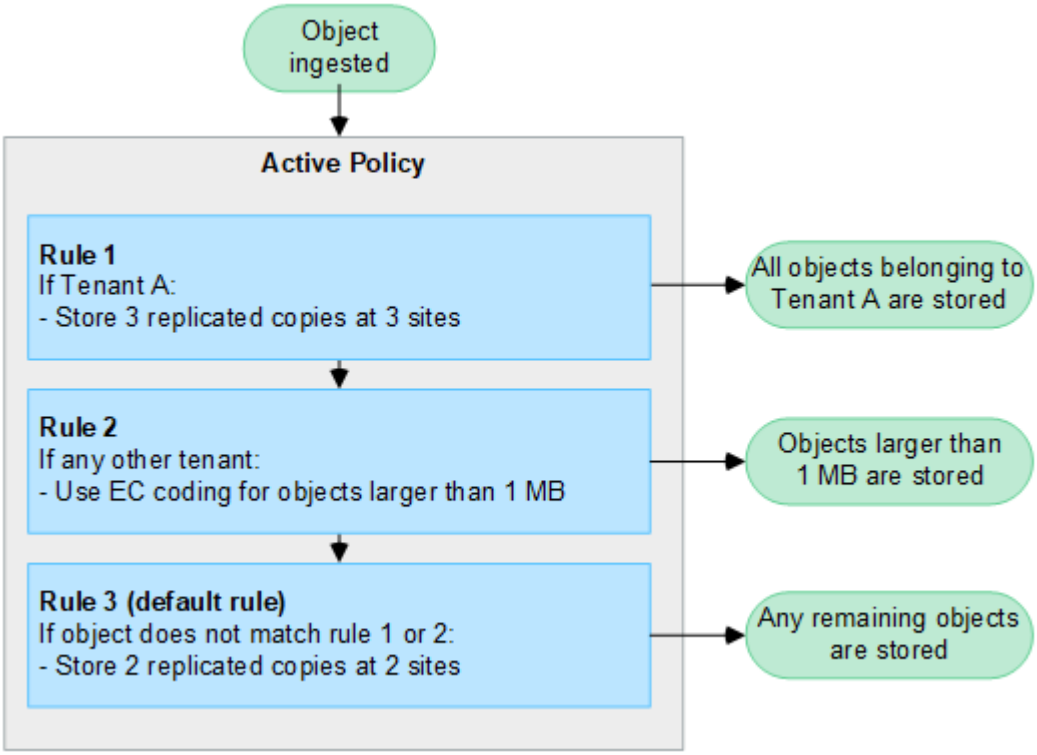
Exemplo de política ILM

Como exemplo, uma política ILM pode conter três regras ILM que especificam o seguinte:

- **Regra 1: Cópias replicadas para o locatário A**
  - Corresponder todos os objetos pertencentes ao locatário A..
  - Armazene esses objetos como três cópias replicadas em três locais.
  - Objetos pertencentes a outros inquilinos não são correspondidos pela regra 1, portanto, eles são avaliados em relação à regra 2.
- **Regra 2: Codificação de apagamento para objetos com mais de 1 MB**
  - Combine todos os objetos de outros inquilinos, mas somente se eles forem maiores que 1 MB. Esses objetos maiores são armazenados usando codificação de apagamento 6-3 em três locais.
  - Não corresponde a objetos de 1 MB ou menores, portanto, esses objetos são avaliados em relação à

regra 3.

- **Regra 3: 2 cópias 2 data centers** (padrão)
  - É a última regra e padrão na política. Não utiliza filtros.
  - Faça duas cópias replicadas de todos os objetos não correspondidos pela regra 1 ou regra 2 (objetos não pertencentes ao locatário A que tenham 1 MB ou menos).



O que são políticas ativas e inativas?

Cada sistema StorageGRID deve ter pelo menos uma política ILM ativa. Se você quiser ter mais de uma política ILM ativa, crie tags de política ILM e atribua uma política a cada tag. Os locatários então aplicam tags aos buckets do S3. A política padrão é aplicada a todos os objetos em buckets que não têm uma tag de política atribuída.

Quando você cria uma política ILM pela primeira vez, você seleciona uma ou mais regras ILM e as organiza em uma ordem específica. Depois de simular a política para confirmar seu comportamento, você a ativará.

Quando você ativa uma política de ILM, o StorageGRID usa essa política para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Os objetos existentes podem ser movidos para novos locais quando as regras ILM na nova política são implementadas.

Se você ativar mais de uma política de ILM de cada vez e os locatários aplicarem tags de política a buckets do S3, os objetos em cada bucket serão gerenciados de acordo com a política atribuída à tag.

Um sistema StorageGRID rastreia o histórico de políticas que foram ativadas ou desativadas.

Considerações para criar uma política ILM

- Utilize apenas a política fornecida pelo sistema, a política de cópias Baseline 2, em sistemas de teste. Para o StorageGRID 11,6 e versões anteriores, a regra fazer 2 cópias nesta política usa o pool de storage de todos os nós de storage, que contém todos os locais. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.

O pool de storage de todos os nós de storage é criado automaticamente durante a instalação do StorageGRID 11,6 e versões anteriores. Se você atualizar para uma versão posterior do StorageGRID, o pool todos os nós de storage ainda existirá. Se você instalar o StorageGRID 11,7 ou posterior como uma nova instalação, o pool todos os nós de storage não será criado.

- Ao projetar uma nova política, considere todos os diferentes tipos de objetos que podem ser ingeridos em sua grade. Certifique-se de que a política inclui regras para corresponder e colocar esses objetos conforme necessário.
- Mantenha a política ILM o mais simples possível. Isso evita situações potencialmente perigosas em que os dados de objetos não são protegidos como pretendido quando as alterações são feitas no sistema StorageGRID ao longo do tempo.
- Certifique-se de que as regras da política estão na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando na parte superior. Por exemplo, se a primeira regra de uma política corresponder a um objeto, esse objeto não será avaliado por nenhuma outra regra.
- A última regra em cada política ILM é a regra ILM padrão, que não pode usar nenhum filtro. Se um objeto não tiver sido correspondido por outra regra, a regra padrão controla onde esse objeto é colocado e por quanto tempo ele é retido.
- Antes de ativar uma nova política, revise todas as alterações que a política está fazendo no posicionamento de objetos existentes. Alterar a localização de um objeto existente pode resultar em problemas de recursos temporários quando os novos posicionamentos são avaliados e implementados.

Criar políticas ILM

Crie uma ou mais políticas de ILM para atender aos seus requisitos de qualidade do serviço.

Ter uma política ILM ativa permite que você aplique as mesmas regras ILM a todos os locatários e buckets.

Ter várias políticas de ILM ativas permite que você aplique as regras de ILM apropriadas a locatários e buckets específicos para atender a vários requisitos de qualidade do serviço.

Crie uma política ILM

Sobre esta tarefa

Antes de criar sua própria política, verifique se o "Política ILM padrão"não atende aos requisitos de storage.

Use apenas as políticas fornecidas pelo sistema, a Política de cópias 2 (para grades de um local) ou a cópia 1 por local (para grades de vários locais), em sistemas de teste. Para o StorageGRID 11,6 e versões anteriores, a regra padrão dessa política usa o pool de storage de todos os nós de storage, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.

Se o "A definição Global S3 Object Lock foi ativada", você deve garantir que a diretiva ILM esteja em conformidade com os requisitos dos buckets que têm o bloqueio de objeto S3 ativado. Nesta seção, siga as instruções que mencionam ter o bloqueio de objeto S3 ativado.

Antes de começar

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

- Você tem o "permissões de acesso necessárias".
- Você "Regras ILM criadas" tem baseado se o bloqueio de objeto S3 está ativado.

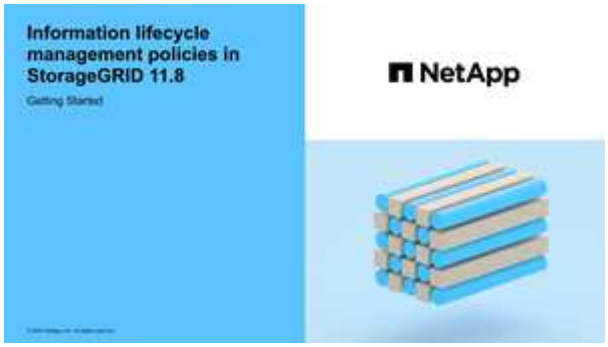
S3 bloqueio de objetos não ativado

- Você "Criou as regras ILM"deseja adicionar à política. Conforme necessário, você pode salvar uma política, criar regras adicionais e editar a política para adicionar as novas regras.
- Você tem "Criou uma regra ILM padrão" que não contém nenhum filtro.

S3 bloqueio de objetos ativado

- "A definição Global S3 Object Lock já está ativada"O para o sistema StorageGRID.
- Você "Criou as regras ILM em conformidade e não compatível"deseja adicionar à política. Conforme necessário, você pode salvar uma política, criar regras adicionais e editar a política para adicionar as novas regras.
- Você tem "Criou uma regra ILM padrão" para a política que é compatível.

- Opcionalmente, você assistiu ao vídeo: "Vídeo: Visão geral das políticas do ILM"



Consulte também "Use políticas ILM".

Passos

1. Selecione **ILM** > **políticas**.

   Se a configuração Global S3 Object Lock estiver ativada, a página ILM Policies (políticas ILM) indica quais regras ILM são compatíveis.

2. Determine como você deseja criar a política ILM.

Criar nova política

a. Selecione **criar política**.

Clonar a política existente

a. Marque a caixa de seleção da política com a qual deseja começar e selecione **Clone**.

Editar política existente

a. Se uma política estiver inativa, você poderá editá-la. Marque a caixa de seleção da política inativa com a qual deseja começar e selecione **Editar**.

3. No campo **Nome da política**, insira um nome exclusivo para a política.
4. Opcionalmente, no campo **motivo da mudança**, insira o motivo pelo qual você está criando uma nova política.
5. Para adicionar regras à política, selecione **Selecionar regras**. Selecione um nome de regra para exibir as configurações dessa regra.

   Se você estiver clonando uma política:

   - As regras usadas pela política de clonagem são selecionadas.
   - Se a política que você está clonando usou quaisquer regras sem filtros que não eram a regra padrão, você será solicitado a remover todas, exceto uma dessas regras.
   - Se a regra padrão usou um filtro, você será solicitado a selecionar uma nova regra padrão.
   - Se a regra padrão não for a última regra, você poderá mover a regra para o fim da nova política.

S3 bloqueio de objetos não ativado

a. Selecione uma regra padrão para a política. Para criar uma nova regra padrão, selecione **ILM rules page**.

   A regra padrão se aplica a quaisquer objetos que não correspondam a outra regra na política. A regra padrão não pode usar nenhum filtro e é sempre avaliada por último.

   > Não use a regra fazer cópias 2 como regra padrão para uma política. A regra fazer 2 cópias usa um único pool de storage, todos os nós de storage, que contém todos os locais. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.

S3 bloqueio de objetos ativado

a. Selecione uma regra padrão para a política. Para criar uma nova regra padrão, selecione **ILM rules page**.

   A lista de regras contém apenas as regras que são compatíveis e não usam filtros.

   > Não use a regra fazer cópias 2 como regra padrão para uma política. A regra fazer 2 cópias usa um único pool de storage, todos os nós de storage, que contém todos os locais. Se você usar essa regra, várias cópias de um objeto podem ser colocadas no mesmo site.

b. Se você precisar de uma regra "padrão" diferente para objetos em buckets S3 não compatíveis, selecione **incluir uma regra sem filtros para buckets S3 não compatíveis** e selecione uma regra não compatível que não use um filtro.

   Por exemplo, você pode querer usar um pool de armazenamento em nuvem para armazenar objetos em buckets que não têm o bloqueio de objeto S3 ativado.

   > Você só pode selecionar uma regra não compatível que não use um filtro.

Consulte também "Exemplo 7: Política de ILM compatível para bloqueio de objetos S3".

6. Quando terminar de selecionar a regra padrão, selecione **continuar**.
7. Para a etapa outras regras, selecione quaisquer outras regras que você deseja adicionar à política. Essas regras usam pelo menos um filtro (conta de locatário, nome do bucket, filtro avançado ou tempo de referência não atual). Em seguida, selecione **Select**.

   A janela criar uma política lista agora as regras selecionadas. A regra padrão está no final, com as outras regras acima dela.

   Se o bloqueio de objeto S3 estiver ativado e você também tiver selecionado uma regra "padrão" não compatível, essa regra será adicionada como a regra segunda a última na política.

   > Um aviso aparece se qualquer regra não reter objetos para sempre. Quando você ativa essa política, você deve confirmar que deseja que o StorageGRID exclua objetos quando as instruções de posicionamento da regra padrão decorrerem (a menos que um ciclo de vida de bucket mantenha os objetos por um período de tempo mais longo).

8. Arraste as linhas para as regras não padrão para determinar a ordem em que essas regras serão avaliadas.

   Não é possível mover a regra padrão. Se o bloqueio de objetos S3 estiver ativado, também não poderá mover a regra "padrão" não compatível se uma tiver sido selecionada.

   > 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.

9. Conforme necessário, selecione **Selecionar regras** para adicionar ou remover regras.
10. Quando terminar, selecione **Guardar**.
11. Repita estas etapas para criar políticas ILM adicionais.
12. Simule uma política de ILM. Você deve sempre simular uma política antes de ativá-la para garantir que ela funcione como esperado.

Simule uma política

Simule uma política em objetos de teste antes de ativar a política e aplicá-la aos dados de produção.

Antes de começar

- Você conhece o bucket/Object-key S3 para cada objeto que deseja testar.

Passos

1. Usando um cliente S3 ou o "S3 Console", ingira os objetos necessários para testar cada regra.
2. Na página políticas ILM, marque a caixa de seleção da política e selecione **simular**.
3. No campo **Object**, insira o S3 `bucket/object-key` para um objeto de teste. Por exemplo, `bucket-01/filename.png`.
4. Se o controle de versão S3 estiver ativado, insira opcionalmente um ID de versão para o objeto no campo **Version ID**.
5. Selecione **simular**.
6. Na seção resultados da simulação, confirme se cada objeto foi correspondido pela regra correta.

7. Para determinar qual pool de armazenamento ou perfil de codificação de apagamento está em vigor, selecione o nome da regra correspondente para ir para a página de detalhes da regra.

> 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.

Resultados

Quaisquer edições nas regras da política serão refletidas nos resultados da simulação e mostrarão a nova correspondência e a correspondência anterior. A janela de política simular mantém os objetos testados até selecionar **Clear All** (Limpar tudo) ou o ícone remove (remover) para cada objeto na lista Simulation Results (resultados da simulação).

Informações relacionadas

"Exemplo de simulações de política ILM"

Ative uma política

Quando você ativa uma única nova política de ILM, os objetos existentes e os objetos recém-ingeridos são gerenciados por essa política. Quando você ativa várias políticas, as tags de política ILM atribuídas aos buckets determinam os objetos a serem gerenciados.

Antes de ativar uma nova política:

1. Simule a política para confirmar que ela se comporta como você espera.
2. 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.

> Erros em uma política ILM podem causar perda de dados irrecuperável.

Sobre esta tarefa

Quando você ativa uma política de ILM, o sistema distribui a nova política para todos os nós. No entanto, a nova política ativa pode não ter efeito até que todos os nós de grade estejam disponíveis para receber a nova política. Em alguns casos, o sistema espera implementar uma nova política ativa para garantir que os objetos de grade não sejam removidos acidentalmente. Especificamente:

- Se você fizer alterações de política que **aumentem a redundância de dados ou a durabilidade**, essas alterações serão implementadas imediatamente. Por exemplo, se você ativar uma nova política que inclua uma regra de três cópias em vez de uma regra de duas cópias, essa política será implementada imediatamente porque aumenta a redundância de dados.
- Se você fizer alterações de política que **possam diminuir a redundância de dados ou a durabilidade**, essas alterações não serão implementadas até que todos os nós de grade estejam disponíveis. Por exemplo, se você ativar uma nova política que usa uma regra de duas cópias em vez de uma regra de três cópias, a nova política aparecerá na guia diretiva ativa, mas ela não entrará em vigor até que todos os nós estejam online e disponíveis.

Passos

Siga as etapas para ativar uma política ou várias políticas:

Ative uma política

Siga estes passos se tiver apenas uma política ativa. Se já tiver uma ou mais políticas ativas e estiver a ativar políticas adicionais, siga os passos para ativar várias políticas.

1. Quando estiver pronto para ativar uma política, selecione **ILM** > **políticas**.

   Alternativamente, você pode ativar uma única política na página **ILM** > **Policy tags**.

2. Na guia políticas, marque a caixa de seleção da política que deseja ativar e selecione **Ativar**.
3. Siga o passo apropriado:
   - Se uma mensagem de aviso solicitar que você confirme que deseja ativar a política, selecione **OK**.
   - Se for apresentada uma mensagem de aviso contendo detalhes sobre a política:
     i. Analise os detalhes para garantir que a política gerenciaria os dados conforme esperado.
     ii. Se a regra padrão armazenar objetos por um número limitado de dias, revise o diagrama de retenção e digite esse número de dias na caixa de texto.
     iii. Se a regra padrão armazenar objetos para sempre, mas uma ou mais outras regras tiver retenção limitada, digite **yes** na caixa de texto.
     iv. Selecione **Ativar política**.

Ative várias políticas

Para ativar várias políticas, você deve criar tags e atribuir uma política a cada tag.

> Quando várias tags estão em uso, se os locatários frequentemente reatribuírem tags de política a buckets, o desempenho da grade pode ser afetado. Se você tiver locatários não confiáveis, considere usar apenas a tag padrão.

1. Selecione **ILM** > **Policy tags**.
2. Selecione **criar**.
3. Na caixa de diálogo criar tag de política, digite um nome de tag e, opcionalmente, uma descrição para a tag.

   > Os nomes e as descrições das etiquetas são visíveis para os inquilinos. Escolha valores que ajudarão os locatários a tomar uma decisão informada ao selecionar as tags de política a serem atribuídas a seus buckets. Por exemplo, se a política atribuída excluir objetos após um período de tempo, você pode comunicar isso na descrição. Não inclua informações confidenciais nesses campos.

4. Selecione **criar tag**.
5. Na tabela etiquetas de política ILM, use a lista suspensa para selecionar uma política a ser atribuída à tag.
6. Se os avisos aparecerem na coluna limitações da política, selecione **Exibir detalhes da política** para revisar a política.
7. Garantir que cada política gerencie os dados conforme o esperado.
8. Selecione **Ativar políticas atribuídas**. Ou selecione **Limpar alterações** para remover a atribuição de políticas.

9. Na caixa de diálogo Ativar políticas com novas tags, revise as descrições de como cada tag, política e regra gerenciará objetos. Faça alterações conforme necessário para garantir que as políticas gerenciem objetos conforme o esperado.
10. Quando tiver certeza de que deseja ativar as políticas, digite **sim** na caixa de texto e selecione **Ativar políticas**.

Informações relacionadas

"Exemplo 6: Alterando uma política ILM"

Exemplo de simulações de política ILM

Os exemplos de simulações de políticas de ILM fornecem diretrizes para estruturar e modificar simulações para o seu ambiente.

Exemplo 1: Verificar regras ao simular uma política ILM

Este exemplo descreve como verificar regras ao simular uma política.

Neste exemplo, a política **exemplo de ILM** está sendo simulada contra os objetos ingeridos em dois buckets. A política inclui três regras, como segue:

- A primeira regra, **duas cópias, dois anos para bucket-a**, aplica-se apenas a objetos em bucket-a.
- A segunda regra, **objetos EC > 1 MB**, aplica-se a todos os intervalos, mas filtros em objetos com mais de 1 MB.
- A terceira regra, **duas cópias, dois data centers**, é a regra padrão. Ele não inclui nenhum filtro e não usa o tempo de referência não atual.

Depois de simular a política, confirme se cada objeto foi correspondido pela regra correta.

Neste exemplo:

- `bucket-a/bucket-a object.pdf` corresponde corretamente à primeira regra, que filtra os objetos no `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf` está em `bucket-b`, por isso não corresponde à primeira regra. Em vez disso, foi corretamente correspondido pela segunda regra, que filtra em objetos com mais de 1 MB.

- `bucket-b/test object less than 1 MB.pdf` não corresponde aos filtros nas duas primeiras regras, por isso será colocado pela regra padrão, que não inclui filtros.

Exemplo 2: Reordenar regras ao simular uma política ILM

Este exemplo mostra como você pode reordenar regras para alterar os resultados ao simular uma política.

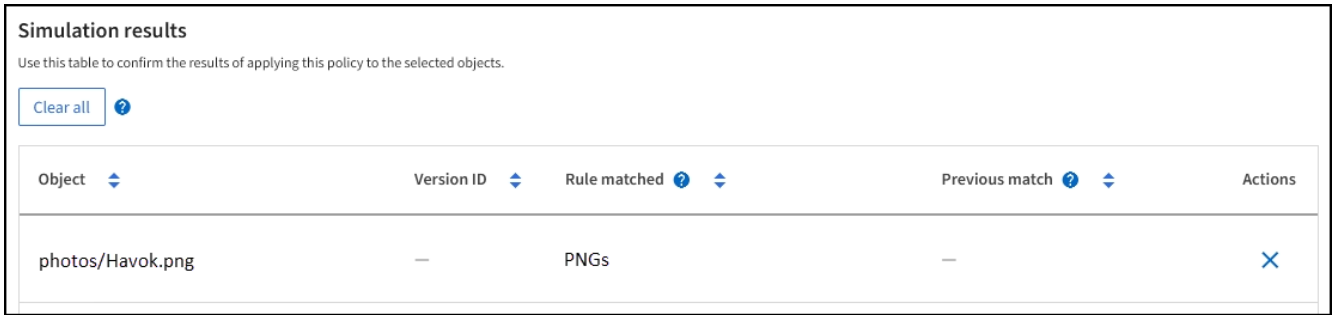
Neste exemplo, a política **Demo** está sendo simulada. Esta política, que se destina a encontrar objetos que tenham metadados de usuário de série X-men, inclui três regras, como segue:

- A primeira regra, **PNGs**, filtra os nomes das chaves que terminam em `.png`.
- A segunda regra, **X-meN**, aplica-se apenas a objetos para o locatário A e filtra os metadados `series=x-men` do usuário.
- A última regra, **duas cópias dois data centers**, é a regra padrão, que corresponde a quaisquer objetos que não correspondam às duas primeiras regras.

Passos

1. Depois de adicionar as regras e salvar a política, selecione **simular**.
2. No campo **Object**, insira o bucket/Object-key S3 para um objeto de teste e selecione **Simulate**.

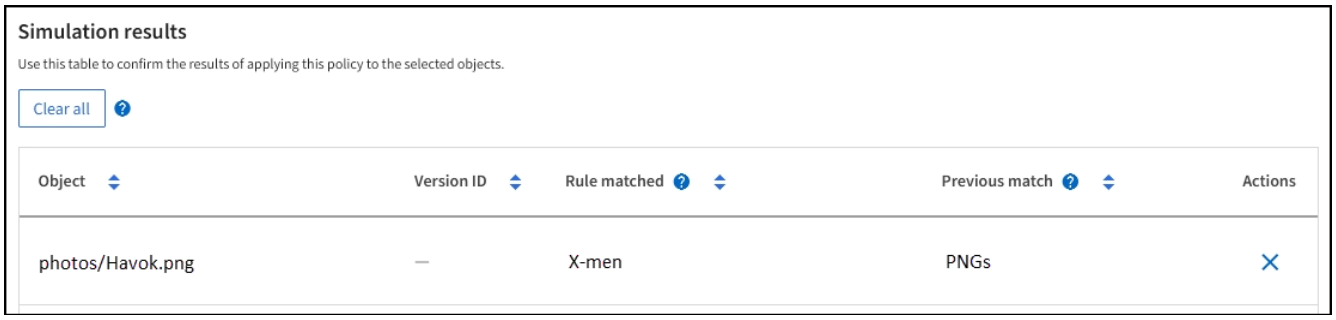
   Os resultados da simulação aparecem, mostrando que o `Havok.png` objeto foi correspondido pela regra **PNGs**.



   No entanto, `Havok.png` foi feito para testar a regra **X-men**.

3. Para resolver o problema, reordene as regras.
   a. Selecione **Finish** (concluir) para fechar a janela Simulate ILM Policy (simular política ILM).
   b. Selecione **Editar** para editar a política.
   c. Arraste a regra **X-man** para o topo da lista.
   d. Selecione **Guardar**.
4. Selecione **simular**.

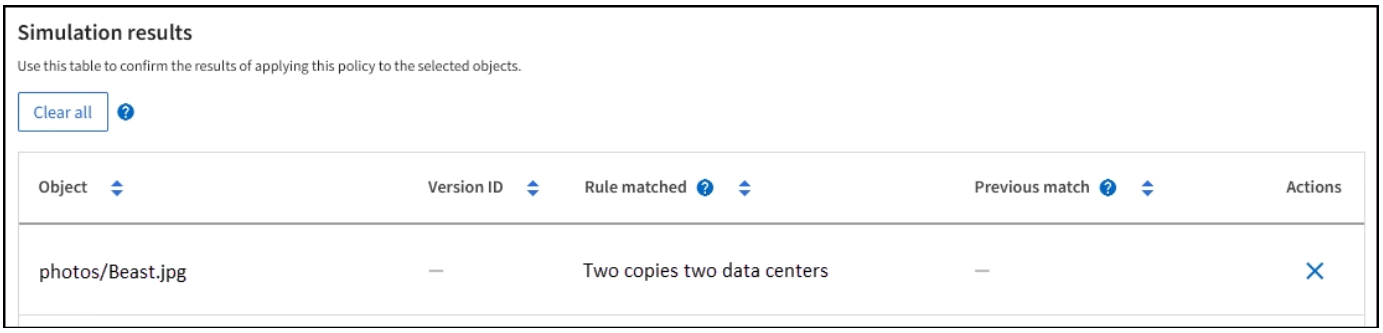
   Os objetos que você testou anteriormente são reavaliados em relação à política atualizada e os novos resultados da simulação são mostrados. No exemplo, a coluna Rule Matched mostra que o `Havok.png` objeto agora corresponde à regra de metadados X-men, conforme esperado. A coluna correspondência anterior mostra que a regra PNGs correspondia ao objeto na simulação anterior.



Exemplo 3: Corrija uma regra ao simular uma política ILM

Este exemplo mostra como simular uma política, corrigir uma regra na política e continuar a simulação.

Neste exemplo, a política **Demo** está sendo simulada. Esta política destina-se a localizar objetos que tenham `series=x-men` metadados de usuário. No entanto, resultados inesperados ocorreram ao simular essa política contra o `Beast.jpg` objeto. Em vez de corresponder à regra de metadados X-men, o objeto correspondia à regra padrão, duas cópias de dois data centers.



Quando um objeto de teste não é correspondido pela regra esperada na política, você deve examinar cada regra na política e corrigir quaisquer erros.

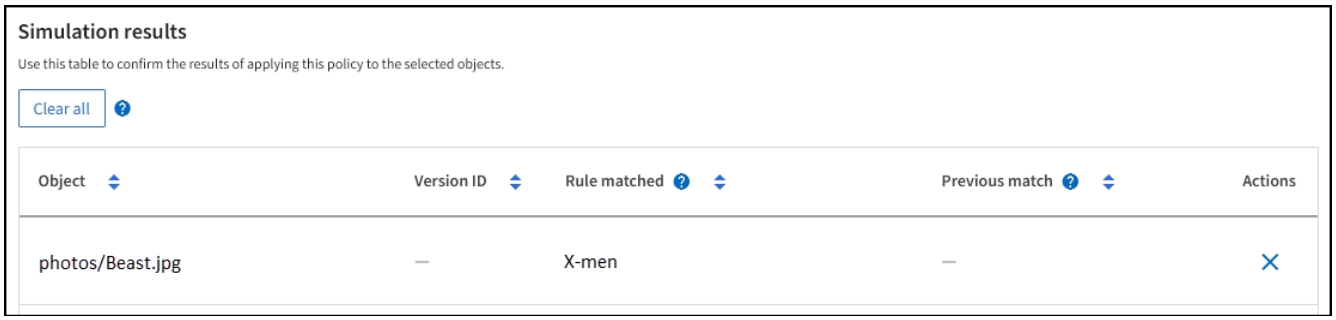
Passos

1. Selecione **Finish** (concluir) para fechar a caixa de diálogo Simulate policy (simular política). Na página de detalhes da política, selecione **Diagrama de retenção**. Em seguida, selecione **expandir tudo** ou **Exibir detalhes** para cada regra conforme necessário.
2. Revise a conta de locatário da regra, o tempo de referência e os critérios de filtragem.

   Como exemplo, suponha que os metadados para a regra X-men foram inseridos como "x-men01" em vez de "x-men".

3. Para resolver o erro, corrija a regra da seguinte forma:
   - Se a regra fizer parte da política, você pode clonar a regra ou remover a regra da política e editá-la.
   - Se a regra fizer parte da política ativa, você deverá clonar a regra. Não é possível editar ou remover uma regra da política ativa.
4. Execute a simulação novamente.

   Neste exemplo, a regra X-meN corrigida agora corresponde ao `Beast.jpg` objeto com base nos `series=x-men` metadados do usuário, conforme esperado.



Gerenciar tags de política ILM

Você pode exibir detalhes da tag de política ILM, editar uma tag ou remover uma tag.

Antes de começar

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

Ver detalhes da etiqueta de política ILM

Para ver os detalhes de uma tag:

1. Selecione **ILM** > **Policy tags**.
2. Selecione o nome da política na tabela. A página de detalhes da tag é exibida.
3. Na página de detalhes, veja o histórico anterior das políticas atribuídas.
4. Visualize uma política selecionando-a.

Editar etiqueta de política ILM

> Os nomes e as descrições das etiquetas são visíveis para os inquilinos. Escolha valores que ajudarão os locatários a tomar uma decisão informada ao selecionar as tags de política a serem atribuídas a seus buckets. Por exemplo, se a política atribuída excluir objetos após um período de tempo, você pode comunicar isso na descrição. Não inclua informações confidenciais nesses campos.

Para editar a descrição de uma tag existente:

1. Selecione **ILM** > **Policy tags**.
2. Marque a caixa de seleção para a tag e selecione **Editar**.

   Em alternativa, selecione o nome da etiqueta. A página de detalhes da tag é exibida e você pode selecionar **Editar** nessa página.

3. Altere a descrição da tag conforme necessário
4. Selecione **Guardar**.

Remova a etiqueta de política ILM

Quando você remove uma tag de política, todos os buckets atribuídos a essa tag terão a política padrão aplicada.

Para remover uma etiqueta:

1. Selecione **ILM** > **Policy tags**.
2. Marque a caixa de seleção para a tag e selecione **Remover**. É apresentada uma caixa de diálogo de confirmação.

   Em alternativa, selecione o nome da etiqueta. A página de detalhes da tag é exibida e você pode selecionar **Remover** nessa página.

3. Selecione **Sim** para excluir a tag.

Verifique uma política ILM com pesquisa de metadados de objeto

Depois de ativar uma política ILM, ingira objetos de teste representativos no sistema StorageGRID e, em seguida, execute uma pesquisa de metadados de objetos para confirmar que as cópias estão sendo feitas conforme o pretendido e colocadas nos locais corretos.

Antes de começar

Você tem um identificador de objeto, que pode ser um dos seguintes: * * * UUID*: O Identificador universalmente exclusivo do objeto. * **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. * * Bucket **S3 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. Se o bucket S3 estiver versionado e você quiser procurar uma versão específica de um objeto S3 usando o bucket e a chave do objeto, você tem o **version ID**.

Passos

1. Ingira o objeto.
2. Selecione **ILM** > **Object metadata lookup**.
3. Digite o identificador do objeto no campo **Identificador**. Você pode inserir um UUID, CBID ou uma chave de objeto/bucket do S3.
4. Opcionalmente, insira um ID de versão para o objeto (apenas S3).
5. Selecione **Procurar**.

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

   - Metadados do sistema, como ID de objeto (UUID), tipo de resultado (objeto, marcador de exclusão, bucket S3) e tamanho lógico do objeto. Consulte o exemplo de captura de tela abaixo para obter mais detalhes.
   - 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.

6. Confirme se o objeto está armazenado no local ou locais corretos e se é o tipo correto de cópia.

   Se a opção Auditoria estiver ativada, você também poderá monitorar o log de auditoria para a mensagem regras de objeto ORLM atendidas. A mensagem de auditoria ORLM pode fornecer mais informações sobre o status do processo de avaliação ILM, mas não pode fornecer informações sobre a correção do posicionamento dos dados do objeto ou a integridade da política ILM. Você deve avaliar isso sozinho. Para obter detalhes, "Rever registos de auditoria"consulte .

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.

> A captura de tela a seguir é um exemplo. Seus resultados variam de acordo com a versão do StorageGRID.

System Metadata

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

Replicated Copies

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

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Informações relacionadas

"USE A API REST DO S3"

Trabalhe com políticas ILM e regras ILM

À medida que seus requisitos de storage mudam, talvez seja necessário implementar políticas adicionais ou modificar as regras de ILM associadas a uma política. Você pode visualizar métricas ILM para determinar o desempenho do sistema.

Antes de começar

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

Ver políticas ILM

Para exibir políticas ILM ativas e inativas e histórico de ativação de políticas:

1. Selecione **ILM** > **políticas**.
2. Selecione **políticas** para exibir uma lista de políticas ativas e inativas. A tabela lista o nome de cada política, as tags às quais a política é atribuída e se a política está ativa ou inativa.
3. Selecione **Histórico de ativação** para ver uma lista de datas de início e término de ativação para políticas.
4. Selecione um nome de política para exibir os detalhes da política.

> Se você exibir os detalhes de uma política cujo status é editado ou excluído, uma mensagem será exibida explicando que você está exibindo a versão da política que estava ativa para o período de tempo especificado e que foi editada ou excluída.

Editar uma política ILM

Você só pode editar uma política inativa. Se você quiser editar uma política ativa, desative-a ou crie um clone e edite o clone.

Para editar uma política:

1. Selecione **ILM** > **políticas**.
2. Marque a caixa de seleção da política que deseja editar e selecione **Editar**.
3. Edite a política seguindo as instruções em "Criar políticas ILM".
4. Simule a política antes de a reativar.

> Uma política de ILM que foi configurada incorretamente pode resultar em perda de dados irrecuperável. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM e simule a política ILM. Confirme sempre que a política de ILM funcionará como pretendido.

Clonar uma política de ILM

Para clonar uma política ILM:

1. Selecione **ILM** > **políticas**.
2. Marque a caixa de seleção da política que deseja clonar e selecione **Clone**.
3. Crie uma nova política começando com a política clonada seguindo as instruções do "Criar políticas ILM".

> Uma política de ILM que foi configurada incorretamente pode resultar em perda de dados irrecuperável. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM e simule a política ILM. Confirme sempre que a política de ILM funcionará como pretendido.

Remover uma política ILM

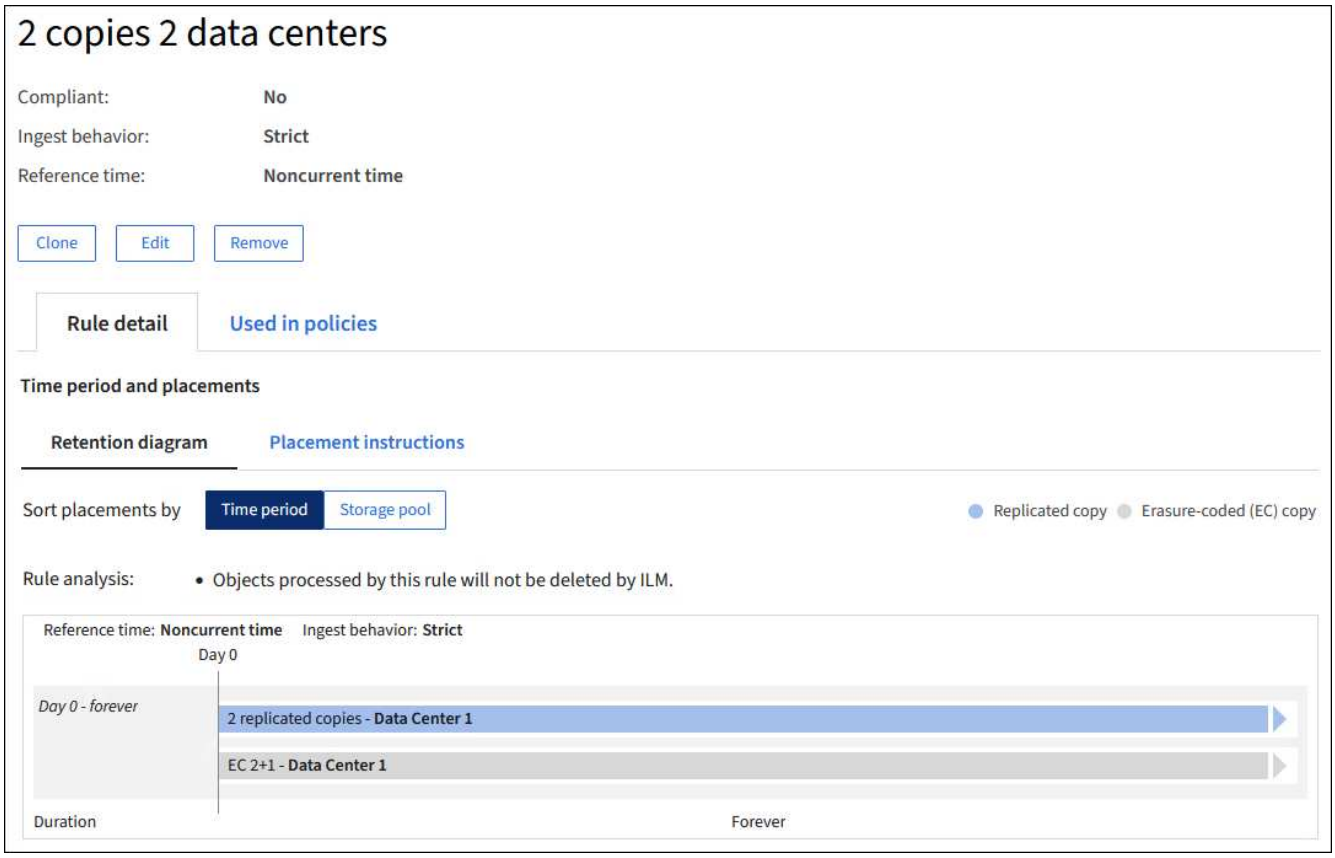
Você só pode remover uma política ILM se ela estiver inativa. Para remover uma política:

1. Selecione **ILM** > **políticas**.
2. Marque a caixa de seleção da política inativa que deseja remover.
3. Selecione **Remover**.

Exibir detalhes da regra ILM

Para exibir os detalhes de uma regra ILM, incluindo o diagrama de retenção e as instruções de posicionamento da regra:

1. Selecione **ILM** > **regras**.
2. Selecione o nome da regra cujos detalhes você deseja exibir. Exemplo:



Além disso, você pode usar a página de detalhes para clonar, editar ou remover uma regra. Você não pode editar ou remover uma regra se ela for usada em qualquer política.

Clonar uma regra ILM

Você pode clonar uma regra existente se quiser criar uma nova regra que use algumas das configurações da regra existente. Se você precisar editar uma regra usada em qualquer política, clonar a regra e fazer alterações no clone. Depois de fazer alterações no clone, você pode remover a regra original da política e substituí-la pela versão modificada, conforme necessário.

> Você não pode clonar uma regra ILM se ela foi criada usando o StorageGRID versão 10,2 ou anterior.

Passos

1. Selecione **ILM** > **regras**.
2. Marque a caixa de seleção da regra que deseja clonar e selecione **Clone**. Em alternativa, selecione o nome da regra e, em seguida, selecione **Clone** na página de detalhes da regra.
3. Atualize a regra clonada seguindo as etapas de Editar uma regra ILM e "Usando filtros avançados em regras ILM".

Ao clonar uma regra ILM, você deve inserir um novo nome.

Editar uma regra ILM

Talvez seja necessário editar uma regra ILM para alterar um filtro ou uma instrução de colocação.

Não é possível editar uma regra se ela for usada em qualquer política ILM. Em vez disso, você pode clone a regra e fazer todas as alterações necessárias na cópia clonada.

> Uma política de ILM que foi configurada incorretamente pode resultar em perda de dados irrecuperável. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM e simule a política ILM. Confirme sempre que a política de ILM funcionará como pretendido.

Passos

1. Selecione **ILM** > **regras**.
2. Confirme se a regra que você deseja editar não é usada em nenhuma política ILM.
3. Se a regra que você deseja editar não estiver em uso, marque a caixa de seleção da regra e selecione **ações** > **Editar**. Em alternativa, selecione o nome da regra e, em seguida, selecione **Editar** na página de detalhes da regra.
4. Conclua as etapas do assistente Editar regra ILM. Conforme necessário, siga os passos para "Criando uma regra ILM" e "Usando filtros avançados em regras ILM".

   Ao editar uma regra ILM, você não pode alterar seu nome.

Remova uma regra ILM

Para manter a lista de regras atuais do ILM gerenciável, remova todas as regras do ILM que você provavelmente não usará.

Passos

Para remover uma regra ILM que está atualmente usada em uma política ativa:

1. Clonar a política.
2. Remova a regra ILM do clone de política.
3. Salve, simule e ative a nova política para garantir que os objetos estejam protegidos conforme esperado.
4. Vá para as etapas para remover uma regra ILM que está sendo usada atualmente em uma política inativa.

Para remover uma regra ILM que está atualmente usada em uma política inativa:

1. Selecione a política inativa.
2. Remova a regra ILM da política ou remova a política.
3. Vá para as etapas para remover uma regra ILM que não é usada atualmente.

Para remover uma regra ILM que não é usada atualmente:

1. Selecione **ILM** > **regras**.
2. Confirme se a regra que você deseja remover não é usada em nenhuma política.

3. Se a regra que você deseja remover não estiver em uso, selecione a regra e selecione **ações** > **Remover**. Você pode selecionar várias regras e remover todas elas ao mesmo tempo.
4. Selecione **Sim** para confirmar que deseja remover a regra ILM.

Ver métricas ILM

Você pode exibir métricas para ILM, como o número de objetos na fila e a taxa de avaliação. Você pode monitorar essas métricas para determinar o desempenho do sistema. Uma fila grande ou taxa de avaliação pode indicar que o sistema não é capaz de acompanhar a taxa de ingestão, a carga dos aplicativos cliente é excessiva ou que existe alguma condição anormal.

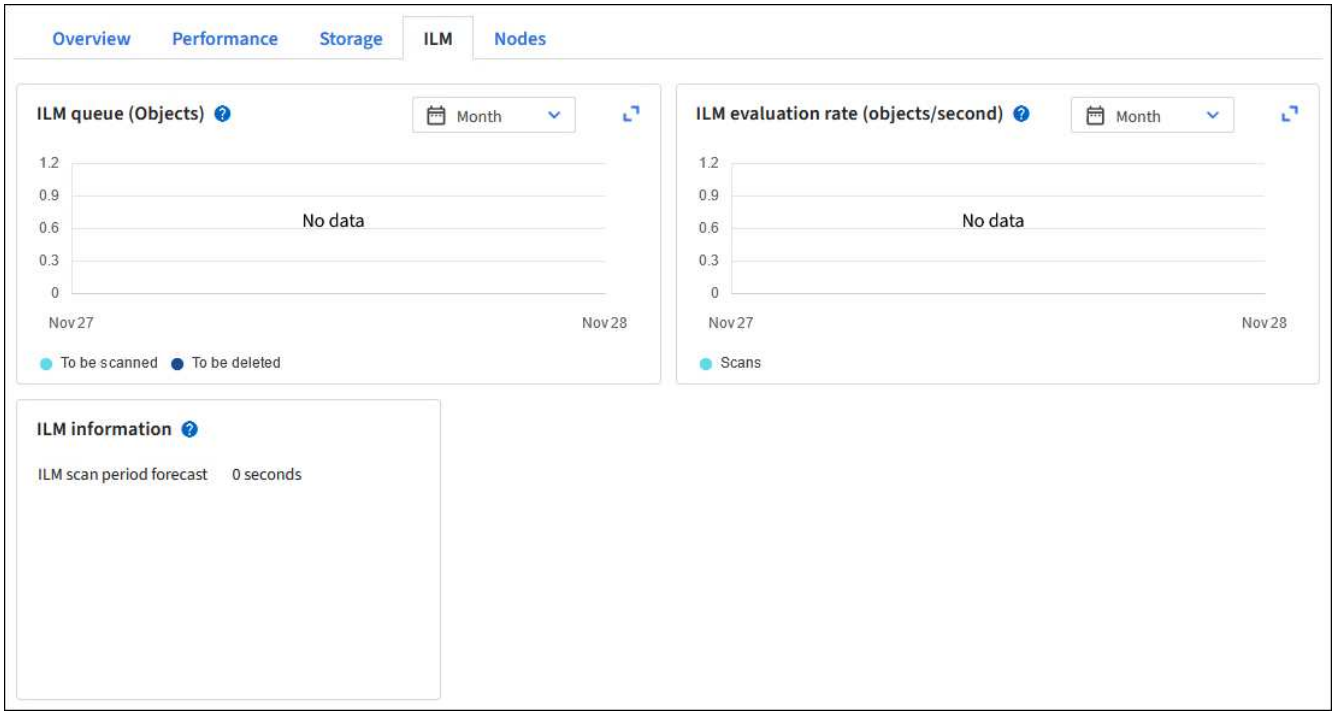
Passos

1. Selecione **Dashboard** > **ILM**.

   Como o painel pode ser personalizado, a guia ILM pode não estar disponível.

2. Monitore as métricas na guia ILM.

   Você pode selecionar o ponto de interrogação para ver uma descrição dos itens na guia ILM.



Use o bloqueio de objetos S3D.

Gerencie objetos com o S3 Object Lock

Como administrador de grade, você pode ativar o bloqueio de objeto S3 para seu sistema StorageGRID e implementar uma política ILM compatível para ajudar a garantir que os objetos em buckets S3 específicos não sejam excluídos ou substituídos por um período de tempo especificado.

O que é S3 Object Lock?

O recurso bloqueio de objetos do StorageGRID S3 é uma solução de proteção de objetos equivalente ao bloqueio de objetos do S3 no Amazon Simple Storage Service (Amazon S3).

Quando a configuração de bloqueio de objeto S3 global está ativada para um sistema StorageGRID, uma conta de locatário S3 pode criar buckets com ou sem bloqueio de objeto S3 ativado. Se um bucket tiver o bloqueio de objetos S3 ativado, o controle de versão do bucket é necessário e é ativado automaticamente.

Um bucket sem S3 Object Lock só pode ter objetos sem as configurações de retenção especificadas. Nenhum objeto ingerido terá configurações de retenção.

- Um bucket com S3 Object Lock* pode ter objetos com e sem configurações de retenção especificadas por aplicativos clientes S3. Alguns objetos ingeridos terão definições de retenção.

Um bucket com o bloqueio de objeto S3 e a retenção padrão configurada pode ter carregado objetos com configurações de retenção especificadas e novos objetos sem configurações de retenção. Os novos objetos usam a configuração padrão, porque a configuração de retenção não foi configurada no nível do objeto.

Efetivamente, todos os objetos recém-ingeridos têm configurações de retenção quando a retenção padrão é configurada. Os objetos existentes sem configurações de retenção de objetos permanecem inalterados.

Modos de retenção

O recurso bloqueio de objetos do StorageGRID S3 suporta dois modos de retenção para aplicar diferentes níveis de proteção aos objetos. Esses modos são equivalentes aos modos de retenção do Amazon S3.

- No modo de conformidade:
  - O objeto não pode ser excluído até que sua data de retenção seja alcançada.
  - O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- No modo de governança:
  - Os usuários com permissão especial podem usar um cabeçalho de desvio em solicitações para modificar determinadas configurações de retenção.
  - Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada.
  - Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto.

Configurações de retenção para versões de objetos

Se um bucket for criado com o bloqueio de objeto S3 ativado, os usuários poderão usar o aplicativo cliente S3 para especificar opcionalmente as seguintes configurações de retenção para cada objeto adicionado ao bucket:

- **Modo de retenção**: Conformidade ou governança.
- **Retent-until-date**: Se a data de retent-until de uma versão de objeto estiver no futuro, o objeto pode ser recuperado, mas não pode ser excluído.
- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar colocar uma retenção legal em um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até que seja explicitamente removida. As obrigações legais são independentes da retenção até à data.

Se um objeto estiver sob uma retenção legal, ninguém poderá excluir o objeto, independentemente de seu modo de retenção.

Para obter detalhes sobre as configurações do objeto, "Use a API REST do S3 para configurar o bloqueio de objetos do S3"consulte .

Configuração de retenção padrão para buckets

Se um bucket for criado com o bloqueio de objetos S3 ativado, os usuários podem especificar opcionalmente as seguintes configurações padrão para o bucket:

- **Modo de retenção padrão**: Conformidade ou governança.
- **Período de retenção padrão**: Quanto tempo as novas versões de objetos adicionadas a este intervalo devem ser mantidas, a partir do dia em que são adicionadas.

As configurações padrão de bucket se aplicam somente a novos objetos que não têm suas próprias configurações de retenção. Os objetos de bucket existentes não são afetados quando você adiciona ou altera essas configurações padrão.

"Crie um bucket do S3"Consulte e "Atualização S3 retenção padrão bloqueio Objeto".

Comparação do S3 Object Lock com a conformidade legada

O bloqueio de objetos S3 substitui o recurso de conformidade que estava disponível em versões anteriores do StorageGRID. Como o recurso de bloqueio de objetos S3 está em conformidade com os requisitos do Amazon S3, ele deprecia o recurso proprietário de conformidade do StorageGRID, que agora é chamado de "conformidade legada".

A configuração de conformidade global está obsoleta. Se você ativou essa configuração usando uma versão anterior do StorageGRID, a configuração bloqueio de objeto S3 será ativada automaticamente. Você pode continuar usando o StorageGRID para gerenciar as configurações de buckets em conformidade existentes; no entanto, não é possível criar novos buckets em conformidade. Para obter detalhes, "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5" consulte .

Se você usou o recurso de conformidade legado em uma versão anterior do StorageGRID, consulte a tabela a seguir para saber como ele se compara ao recurso bloqueio de objetos S3 no StorageGRID.

	S3 bloqueio de objetos	Conformidade (legado)
Como o recurso é ativado globalmente?	No Gerenciador de Grade, selecione **CONFIGURATION** > **System** > **S3 Object Lock**.	Já não é suportado.
Como o recurso está habilitado para um bucket?	Os usuários devem habilitar o bloqueio de objeto S3 ao criar um novo bucket usando o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3.	Já não é suportado.

	S3 bloqueio de objetos	Conformidade (legado)
O controle de versão do bucket é suportado?	Sim. O controle de versão do bucket é necessário e é ativado automaticamente quando o bloqueio de objetos S3 é ativado para o bucket.	Não
Como a retenção de objetos é definida?	Os usuários podem definir uma data de retenção até cada versão do objeto ou definir um período de retenção padrão para cada bucket.	Os usuários devem definir um período de retenção para todo o bucket. O período de retenção aplica-se a todos os objetos no balde.
O período de retenção pode ser alterado?	• No modo de conformidade, a data de retenção até uma versão de objeto pode ser aumentada, mas nunca diminuída. • No modo de governança, os usuários com permissões especiais podem diminuir ou até mesmo remover as configurações de retenção de um objeto.	O período de retenção de um balde pode ser aumentado, mas nunca diminuído.
Onde é controlada a guarda legal?	Os usuários podem colocar uma retenção legal ou levantar uma retenção legal para qualquer versão de objeto no bucket.	Uma retenção legal é colocada no balde e afeta todos os objetos no balde.
Quando os objetos podem ser excluídos?	• No modo de conformidade, uma versão de objeto pode ser excluída após a data de retenção ser alcançada, assumindo que o objeto não está sob retenção legal. • No modo de governança, os usuários com permissões especiais podem excluir um objeto antes de sua data de retenção ser alcançada, supondo que o objeto não esteja sob retenção legal.	Um objeto pode ser excluído após o período de retenção expirar, supondo que o intervalo não esteja sob retenção legal. Os objetos podem ser excluídos automaticamente ou manualmente.
A configuração do ciclo de vida do bucket é suportada?	Sim	Não

S3 tarefas de bloqueio de objetos

Como administrador de grade, você deve coordenar estreitamente com os usuários do locatário para garantir que os objetos estejam protegidos de uma maneira que atenda aos requisitos de retenção.

> A aplicação de configurações de locatário na grade pode levar 15 minutos ou mais com base na conetividade de rede, no status do nó e nas operações do Cassandra.

As listas a seguir para administradores de grade e usuários de locatário contêm as tarefas de alto nível para usar o recurso bloqueio de objeto S3.

Administrador de grade

- Ative a configuração global de bloqueio de objetos S3D para todo o sistema StorageGRID.
- Certifique-se de que as políticas de gerenciamento do ciclo de vida das informações (ILM) sejam *compatíveis*; ou seja, elas atendem "Requisitos de buckets com bloqueio de objeto S3 ativado"ao .
- Conforme necessário, permita que um locatário use a conformidade como modo de retenção. Caso contrário, somente o modo Governança é permitido.
- Conforme necessário, defina um período máximo de retenção para um locatário.

Utilizador inquilino

- Considerações de revisão para buckets e objetos com o S3 Object Lock.
- Conforme necessário, entre em Contato com o administrador de grade para habilitar a configuração global de bloqueio de objetos S3D e definir permissões.
- Crie buckets com o S3 Object Lock ativado.
- Opcionalmente, configure as configurações de retenção padrão para um bucket:
  - Modo de retenção padrão: Governança ou conformidade, se permitido pelo administrador da grade.
  - Período de retenção padrão: Deve ser menor ou igual ao período de retenção máximo definido pelo administrador da grade.
- Use o aplicativo cliente S3 para adicionar objetos e, opcionalmente, definir retenção específica de objeto:
  - Modo de retenção. Governança ou conformidade, se permitido pelo administrador da grade.
  - Reter Data até: Deve ser menor ou igual ao permitido pelo período de retenção máximo definido pelo administrador da grade.

Requisitos para o bloqueio de objetos S3

Você deve analisar os requisitos para ativar a configuração global de bloqueio de objetos S3, os requisitos para criar regras de ILM e políticas de ILM compatíveis e as restrições que o StorageGRID coloca em buckets e objetos que usam o bloqueio de objetos S3.

Requisitos para usar a configuração global S3 Object Lock

- Você deve ativar a configuração global de bloqueio de objetos S3 usando o Gerenciador de Grade ou a API de Gerenciamento de Grade antes que qualquer locatário S3 possa criar um bucket com o bloqueio de objetos S3 ativado.
- Ativar a configuração global S3 Object Lock permite que todas as contas de locatário do S3 criem buckets

com o S3 Object Lock ativado.

- Depois de ativar a definição global S3 Object Lock, não pode desativar a definição.
- Você não pode ativar o bloqueio de objetos S3 global a menos que a regra padrão em todas as políticas ILM ativas seja *compliant* (ou seja, a regra padrão deve cumprir com os requisitos de buckets com o bloqueio de objetos S3 ativado).
- Quando a configuração global S3 Object Lock está ativada, você não pode criar uma nova política ILM ou ativar uma política ILM existente, a menos que a regra padrão da política seja compatível. Depois que a configuração global S3 Object Lock tiver sido ativada, as páginas de regras ILM e políticas ILM indicam quais regras ILM são compatíveis.

Requisitos para regras ILM compatíveis

Se você quiser ativar a configuração global S3 Object Lock, certifique-se de que a regra padrão em todas as políticas ILM ativas seja compatível. Uma regra em conformidade satisfaz os requisitos de ambos os buckets com o S3 Object Lock ativado e quaisquer buckets existentes que tenham a conformidade legada ativada:

- Ele precisa criar pelo menos duas cópias de objeto replicadas ou uma cópia codificada por apagamento.
- Essas cópias devem existir nos nós de storage durante toda a duração de cada linha nas instruções de posicionamento.
- As cópias de objetos não podem ser salvas em um pool de armazenamento em nuvem.
- Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando **tempo de ingestão** como hora de referência.
- Pelo menos uma linha das instruções de colocação deve ser "para sempre".

Requisitos para políticas de ILM

Quando a configuração global S3 Object Lock está ativada, as políticas ILM ativas e inativas podem incluir regras compatíveis e não compatíveis.

- A regra padrão em uma política ILM ativa ou inativa deve ser compatível.
- Regras não compatíveis aplicam-se apenas a objetos em buckets que não tenham o bloqueio de objetos S3 ativado ou que não tenham o recurso de conformidade legado habilitado.
- Regras compatíveis podem se aplicar a objetos em qualquer bucket; o bloqueio de objetos do S3 ou a conformidade legada não precisam ser ativados para o bucket.

"Exemplo de uma política ILM compatível para o bloqueio de objetos S3"

Requisitos para buckets com bloqueio de objeto S3 ativado

- Se a configuração global de bloqueio de objeto S3 estiver ativada para o sistema StorageGRID, você poderá usar o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3 para criar buckets com o bloqueio de objeto S3 ativado.
- Se você planeja usar o bloqueio de objetos S3D, você deve ativar o bloqueio de objetos S3D ao criar o bucket. Não é possível ativar o bloqueio de objetos S3 para um bucket existente.
- Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket. Não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão para o bucket.
- Opcionalmente, você pode especificar um modo de retenção padrão e um período de retenção para cada bucket usando o Gerenciador de locatários, a API de gerenciamento do locatário ou a API REST do S3.

As configurações de retenção padrão do bucket se aplicam somente a novos objetos adicionados ao bucket que não têm suas próprias configurações de retenção. Você pode substituir essas configurações padrão especificando um modo de retenção e manter-até-data para cada versão do objeto quando ele é carregado.

- A configuração do ciclo de vida do bucket é compatível com buckets com o S3 Object Lock ativado.
- A replicação do CloudMirror não é compatível com buckets com o S3 Object Lock ativado.

Requisitos para objetos em buckets com o bloqueio de objetos S3 ativado

- Para proteger uma versão de objeto, você pode especificar configurações de retenção padrão para o bucket ou especificar configurações de retenção para cada versão do objeto. As configurações de retenção no nível do objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST S3.
- As configurações de retenção se aplicam a versões de objetos individuais. Uma versão de objeto pode ter uma configuração de retenção de data e de retenção legal, uma mas não a outra, ou nenhuma. Especificar uma configuração reter-até-data ou retenção legal para um objeto protege apenas a versão especificada na solicitação. Você pode criar novas versões do objeto, enquanto a versão anterior do objeto permanece bloqueada.

Ciclo de vida dos objetos em buckets com o bloqueio de objetos S3 ativado

Cada objeto que é salvo em um bucket com o S3 Object Lock ativado passa por estes estágios:

1. * Ingestão de objetos*

   Quando uma versão de objeto é adicionada ao bucket que tem o bloqueio de objeto S3 ativado, as configurações de retenção são aplicadas da seguinte forma:

   - Se as configurações de retenção forem especificadas para o objeto, as configurações de nível do objeto serão aplicadas. Todas as configurações padrão do bucket são ignoradas.
   - Se não forem especificadas configurações de retenção para o objeto, as configurações padrão de bucket serão aplicadas, se existirem.
   - Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não será protegido pelo bloqueio de objeto S3.

   Se as configurações de retenção forem aplicadas, o objeto e quaisquer metadados definidos pelo usuário do S3 serão protegidos.

2. * Retenção e exclusão de objetos*

   Várias cópias de cada objeto protegido são armazenadas pelo StorageGRID durante o período de retenção especificado. O número exato e o tipo de cópias de objetos e os locais de storage são determinados pelas regras em conformidade nas políticas ativas de ILM. Se um objeto protegido pode ser excluído antes de sua data de retenção ser alcançada depende de seu modo de retenção.

   - Se um objeto estiver sob uma retenção legal, ninguém poderá excluir o objeto, independentemente de seu modo de retenção.

Informações relacionadas

- "Crie um bucket do S3"
- "Atualização S3 retenção padrão bloqueio Objeto"
- "Use a API REST do S3 para configurar o bloqueio de objetos do S3"
- "Exemplo 7: Política de ILM compatível para bloqueio de objetos S3"

Ative o bloqueio de objetos S3 globalmente

Se uma conta de locatário do S3 precisar atender aos requisitos regulatórios ao salvar dados de objeto, você deverá ativar o bloqueio de objeto do S3 para todo o seu sistema StorageGRID. Ativar a configuração global S3 Object Lock permite que qualquer usuário do locatário do S3 crie e gerencie buckets e objetos com o S3 Object Lock.

Antes de começar

- Você tem o "Permissão de acesso à raiz".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você revisou o fluxo de trabalho do S3 Object Lock e entende as considerações.
- Você confirmou que a regra padrão na política ILM ativa é compatível. "Crie uma regra ILM padrão"Consulte para obter detalhes.

Sobre esta tarefa

Um administrador de grade deve habilitar a configuração global S3 Object Lock para permitir que os usuários do locatário criem novos buckets com o S3 Object Lock ativado. Depois que esta definição estiver ativada, não pode ser desativada.

Revise as configurações de conformidade dos locatários existentes depois de ativar a configuração global S3 Object Lock. Quando você ativa essa configuração, as configurações de bloqueio de objeto S3 por locatário dependem da versão do StorageGRID no momento em que o locatário foi criado.

> A configuração de conformidade global está obsoleta. Se você ativou essa configuração usando uma versão anterior do StorageGRID, a configuração bloqueio de objeto S3 será ativada automaticamente. Você pode continuar usando o StorageGRID para gerenciar as configurações de buckets em conformidade existentes; no entanto, não é possível criar novos buckets em conformidade. Para obter detalhes, "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5" consulte .

Passos

1. Selecione **CONFIGURATION** > **System** > **S3 Object Lock**.

   A página Configurações de bloqueio de objetos S3 é exibida.

2. Selecione **Ativar bloqueio de objetos S3**.
3. Selecione **aplicar**.

   Uma caixa de diálogo de confirmação é exibida e lembra que você não pode desativar o bloqueio de objeto S3 depois que ele estiver ativado.

4. Se tiver a certeza de que pretende ativar permanentemente o bloqueio de objetos S3D para todo o seu sistema, selecione **OK**.

   Quando você seleciona **OK**:

   - Se a regra padrão na política ILM ativa for compatível, o bloqueio de objetos S3 agora está ativado para toda a grade e não pode ser desativado.
   - Se a regra padrão não for compatível, um erro será exibido. Você deve criar e ativar uma nova política ILM que inclua uma regra compatível como regra padrão. Selecione **OK**. Em seguida, crie uma nova política, simule-a e ative-a. "Criar política ILM"Consulte para obter instruções.

Resolva erros de consistência ao atualizar o bloqueio de objetos S3 ou a configuração de conformidade legada

Se um site de data center ou vários nós de storage em um local ficarem indisponíveis, talvez seja necessário ajudar S3 usuários de locatários a aplicar alterações ao bloqueio de objetos S3 ou à configuração de conformidade legada.

Os usuários locatários que têm buckets com o bloqueio de objeto S3 (ou conformidade legada) habilitado podem alterar determinadas configurações. Por exemplo, um usuário de locatário usando o bloqueio de objeto S3 pode precisar colocar uma versão de objeto em retenção legal.

Quando um usuário do locatário atualiza as configurações de um bucket do S3 ou uma versão de objeto, o StorageGRID tenta atualizar imediatamente o bucket ou metadados de objeto na grade. Se o sistema não conseguir atualizar os metadados porque um site de data center ou vários nós de storage não estão disponíveis, ele retornará um erro:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Para resolver esse erro, siga estas etapas:

1. Tente disponibilizar novamente todos os nós de storage ou locais o mais rápido possível.
2. Se você não conseguir disponibilizar suficientes nós de storage em cada local, entre em Contato com o suporte técnico, que pode ajudá-lo a recuperar nós e garantir que as alterações sejam aplicadas consistentemente na grade.
3. Depois que o problema subjacente for resolvido, lembre o usuário do locatário de tentar novamente suas alterações de configuração.

Informações relacionadas

- "Use uma conta de locatário"
- "USE A API REST DO S3"
- "Recuperar e manter"

Exemplo de regras e políticas ILM

Exemplo 1: Regras e política de ILM para armazenamento de objetos

Você pode usar as seguintes regras e políticas de exemplo como ponto de partida ao definir uma política de ILM para atender aos requisitos de proteção e retenção de objetos.

> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará da forma pretendida para proteger o conteúdo da perda.

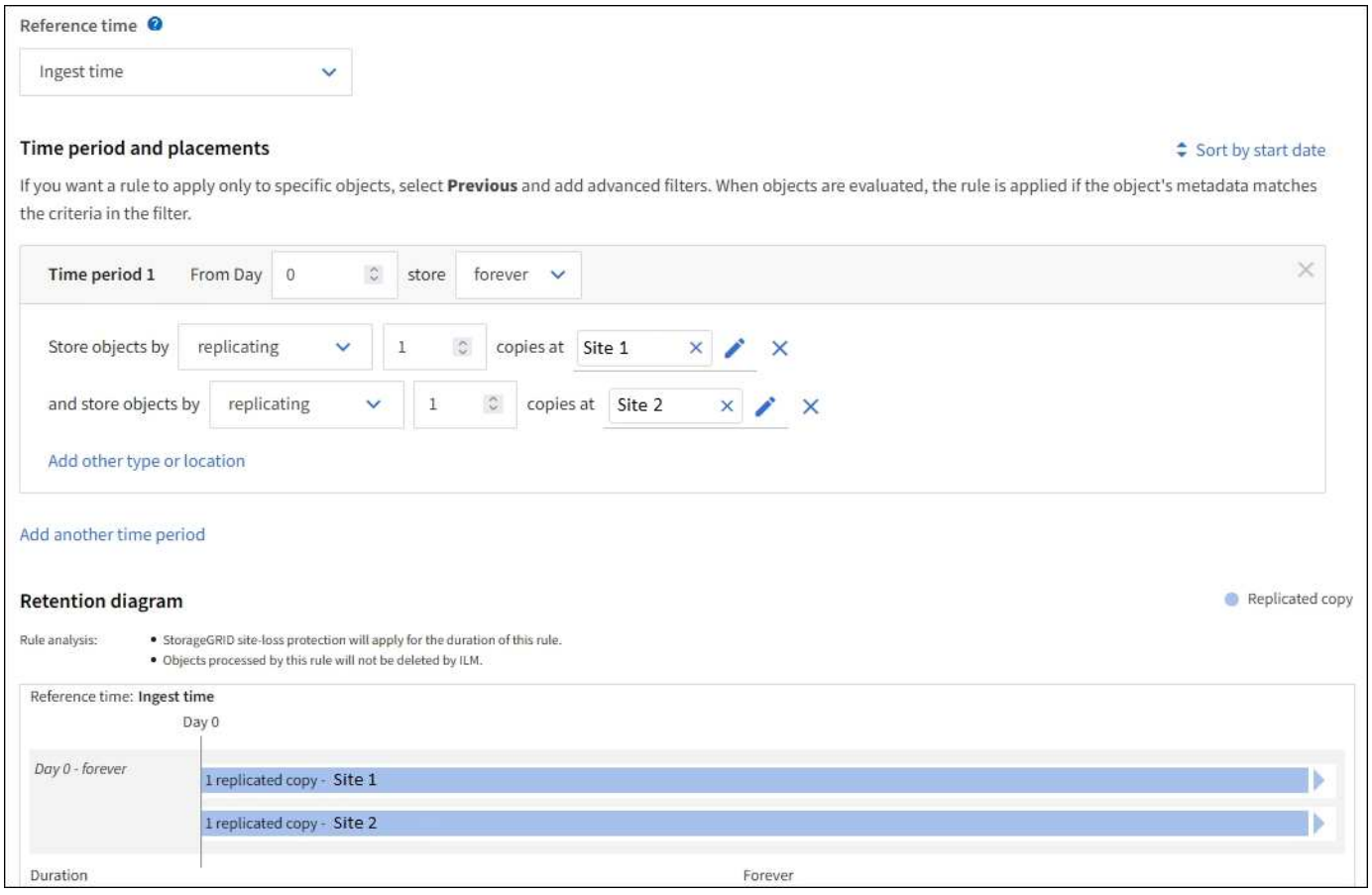
Regra ILM 1 por exemplo 1: Copiar dados de objeto para dois sites

Este exemplo de regra de ILM copia dados de objeto para pools de storage em dois locais.

Definição de regra	Exemplo de valor
Pools de armazenamento em um local	Dois pools de armazenamento, cada um contendo sites diferentes, denominados Site 1 e Site 2.
Nome da regra	Duas cópias de dois locais
Tempo de referência	Tempo de ingestão
Colocações	No dia 0 para sempre, mantenha uma cópia replicada no local 1 e uma cópia replicada no local 2.

A seção análise de regras do diagrama de retenção afirma:

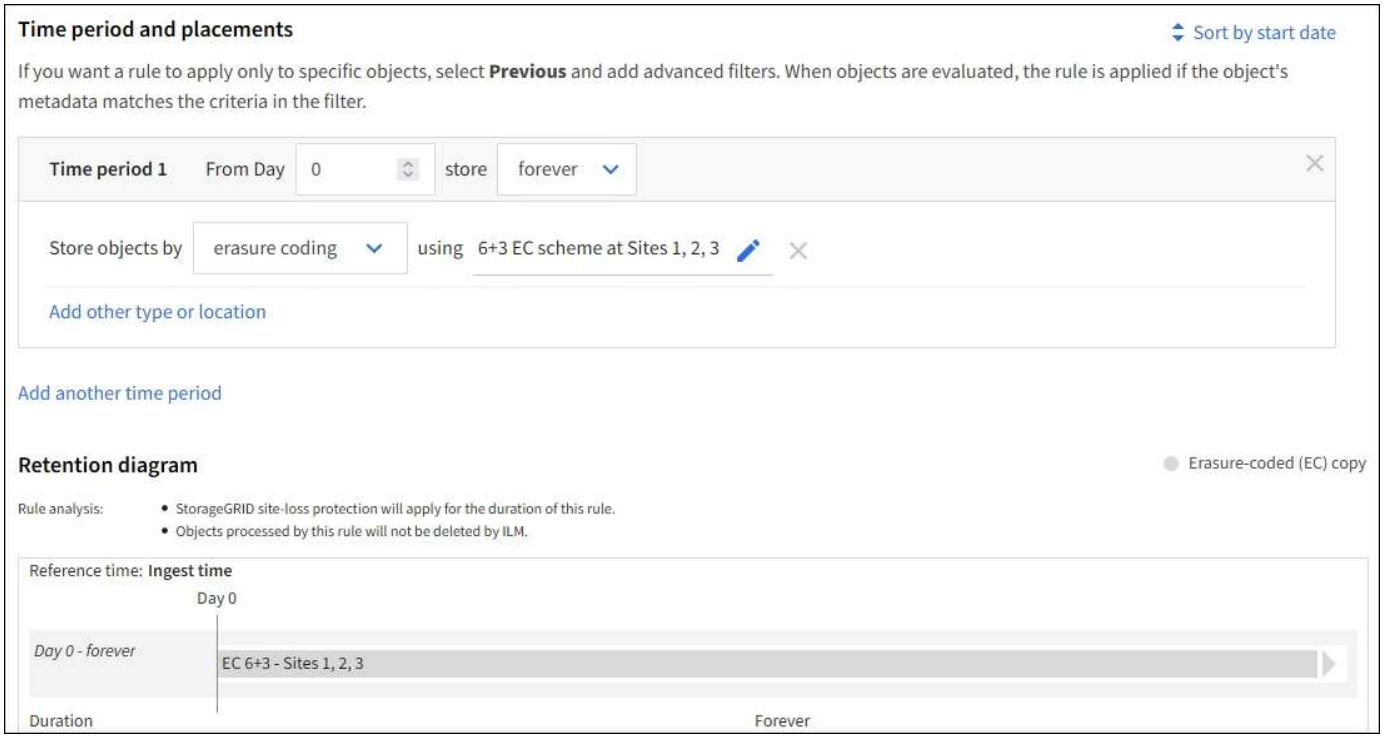
- A proteção contra perda de site da StorageGRID será aplicada durante a duração desta regra.
- Os objetos processados por esta regra não serão excluídos pelo ILM.



Regra ILM 2 por exemplo 1: Perfil de codificação de apagamento com correspondência de intervalo

Este exemplo de regra ILM usa um perfil de codificação de apagamento e um bucket do S3 para determinar onde e quanto tempo o objeto é armazenado.

Definição de regra	Exemplo de valor
Pool de armazenamento com vários locais	• Um pool de armazenamento em três locais (locais 1, 2, 3) • Use o esquema de codificação de apagamento 6-3
Nome da regra	S3 Bucket finance-Records
Tempo de referência	Tempo de ingestão
Colocações	Para objetos no bucket do S3 chamado finance-Records, crie uma cópia codificada por apagamento no pool especificado pelo perfil de codificação de apagamento. Guarde esta cópia para sempre.



Política de ILM, por exemplo, 1

Na prática, a maioria das políticas de ILM são simples, mesmo que o sistema StorageGRID permita que você projete políticas de ILM sofisticadas e complexas.

Uma política ILM típica para uma grade de vários sites pode incluir regras ILM, como as seguintes:

- Na ingestão, armazene todos os objetos pertencentes ao bucket S3 nomeado `finance-records` em um pool de armazenamento que contém três locais. Use a codificação de apagamento 6-3.
- Se um objeto não corresponder à primeira regra ILM, use a regra ILM padrão da política, duas cópias de dois Data Centers, para armazenar uma cópia desse objeto no Site 1 e uma cópia no Site 2.

Informações relacionadas

- "Use políticas ILM"

- "Criar políticas ILM"

Exemplo 2: Regras de ILM e política para filtragem de tamanho de objeto EC

Você pode usar as seguintes regras e políticas de exemplo como pontos de partida para definir uma política de ILM que filtra por tamanho do objeto para atender aos requisitos de EC recomendados.

> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará da forma pretendida para proteger o conteúdo da perda.

Regra ILM 1 por exemplo 2: Use EC para objetos maiores que 1 MB

Este exemplo ILM regra de apagamento codifica objetos que são maiores que 1 MB.

> A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.

Definição de regra	Exemplo de valor
Nome da regra	Objetos somente EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto superior a 1 MB
Colocações	Crie uma cópia codificada por apagamento 2-1 usando três sites

Regra ILM 2 por exemplo 2: Duas cópias replicadas

Este exemplo de regra ILM cria duas cópias replicadas e não filtra pelo tamanho do objeto. Esta regra é a regra padrão da política. Como a primeira regra filtra todos os objetos com mais de 1 MB, essa regra só se aplica a objetos com 1 MB ou menos.

Definição de regra	Exemplo de valor
Nome da regra	Duas cópias replicadas
Tempo de referência	Tempo de ingestão

Definição de regra	Exemplo de valor
Filtro avançado para tamanho do objeto	Nenhum
Colocações	No dia 0 para sempre, mantenha uma cópia replicada no local 1 e uma cópia replicada no local 2.

Política ILM por exemplo 2: Use EC para objetos maiores que 1 MB

Este exemplo de política ILM inclui duas regras ILM:

- A primeira regra de apagamento codifica todos os objetos com mais de 1 MB.
- A segunda regra ILM (padrão) cria duas cópias replicadas. Como objetos com mais de 1 MB foram filtrados pela regra 1, a regra 2 aplica-se apenas a objetos com 1 MB ou menos.

Exemplo 3: Regras e política de ILM para melhor proteção para arquivos de imagem

Você pode usar as regras e a política de exemplo a seguir para garantir que imagens maiores que 1 MB sejam codificadas por apagamento e que duas cópias sejam feitas de imagens menores.

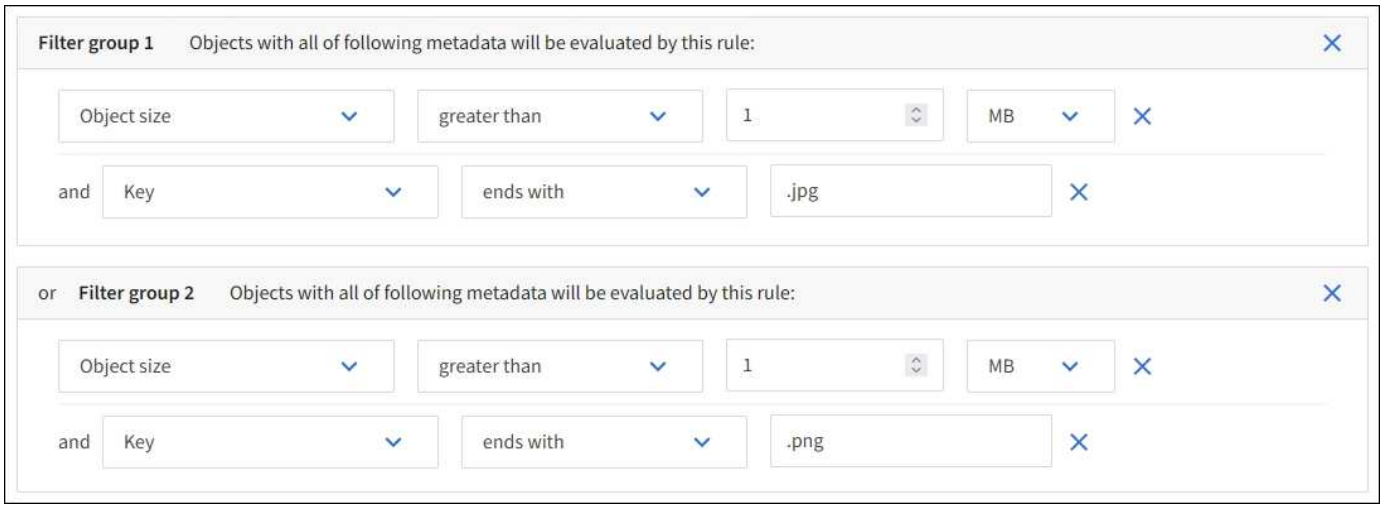
> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará da forma pretendida para proteger o conteúdo da perda.

Regra ILM 1 por exemplo 3: Use EC para arquivos de imagem maiores que 1 MB

Este exemplo de regra ILM usa filtragem avançada para codificar todos os arquivos de imagem com mais de 1 MB.

> A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.

Definição de regra	Exemplo de valor
Nome da regra	Ficheiros de imagem EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto superior a 1 MB
Filtros avançados para Key	• Termina com .jpg • Termina com .png
Colocações	Crie uma cópia codificada por apagamento 2-1 usando três sites



Como essa regra é configurada como a primeira regra na política, a instrução de colocação de codificação de apagamento só se aplica a arquivos .jpg e .png maiores que 1 MB.

Regra ILM 2 por exemplo 3: Crie 2 cópias replicadas para todos os arquivos de imagem restantes

Este exemplo de regra ILM usa filtragem avançada para especificar que arquivos de imagem menores sejam replicados. Como a primeira regra na política já corresponde a arquivos de imagem maiores que 1 MB, essa regra se aplica a arquivos de imagem com 1 MB ou menores.

Definição de regra	Exemplo de valor
Nome da regra	2 cópias para ficheiros de imagem
Tempo de referência	Tempo de ingestão
Filtros avançados para Key	• Termina com .jpg • Termina com .png
Colocações	Criar 2 cópias replicadas em dois pools de storage

Política ILM, por exemplo, 3: Melhor proteção para arquivos de imagem

Este exemplo de política ILM inclui três regras:

- A primeira regra de apagamento codifica todos os arquivos de imagem com mais de 1 MB.
- A segunda regra cria duas cópias de quaisquer arquivos de imagem restantes (ou seja, imagens com 1 MB ou menos).
- A regra padrão se aplica a todos os objetos restantes (ou seja, quaisquer arquivos que não sejam de imagem).

Exemplo 4: Regras ILM e política para objetos com versão S3

Se você tiver um bucket do S3 com controle de versão habilitado, poderá gerenciar as versões de objetos não atuais, incluindo regras na política do ILM que usam "tempo não

atual" como o tempo de referência.

> Se você especificar um tempo de retenção limitado para objetos, esses objetos serão excluídos permanentemente após o período de tempo ser atingido. Certifique-se de entender quanto tempo os objetos serão retidos.

Como este exemplo mostra, você pode controlar a quantidade de armazenamento usada por objetos com controle de versão usando instruções de posicionamento diferentes para versões de objetos não atuais.

> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará da forma pretendida para proteger o conteúdo da perda.

> Para executar a simulação de política ILM em uma versão não atual de um objeto, você deve conhecer o UUID ou CBID da versão do objeto. Para localizar UUID e CBID, use "pesquisa de metadados de objetos" enquanto o objeto ainda estiver atual.

Informações relacionadas

"Como os objetos são excluídos"

Regra ILM 1 por exemplo 4: Salve três cópias por 10 anos

Este exemplo de regra ILM armazena uma cópia de cada objeto em três locais por 10 anos.

Esta regra se aplica a todos os objetos, quer eles sejam ou não versionados.

Definição de regra	Exemplo de valor
Pools de armazenamento	Três pools de armazenamento, cada um composto por diferentes data centers, denominados Site 1, Site 2 e Site 3.
Nome da regra	Três cópias dez anos
Tempo de referência	Tempo de ingestão
Colocações	No dia 0, mantenha três cópias replicadas por 10 anos (3.652 dias), uma no local 1, uma no local 2 e uma no local 3. No final de 10 anos, exclua todas as cópias do objeto.

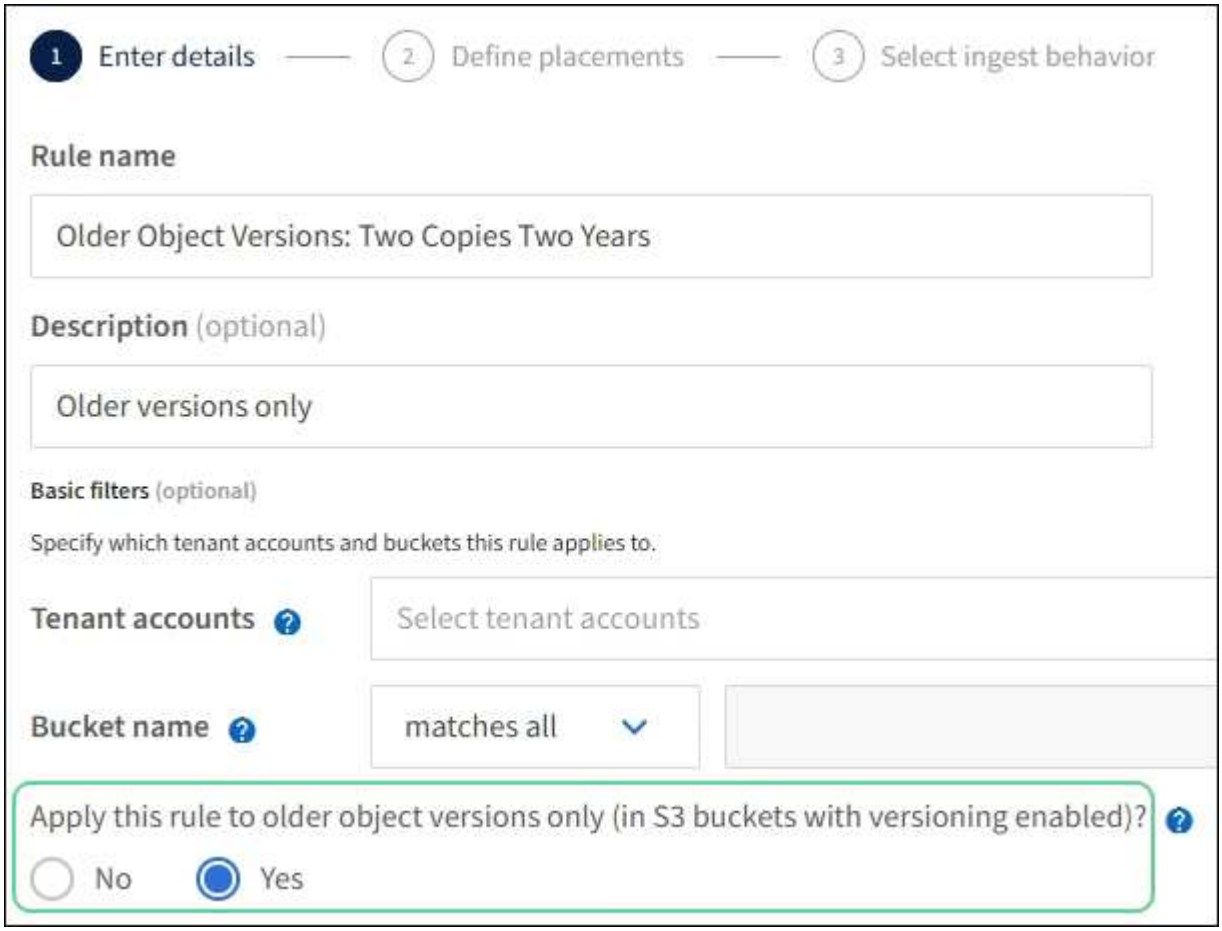
Regra ILM 2 por exemplo 4: Salve duas cópias de versões não atuais por 2 anos

Este exemplo de regra ILM armazena duas cópias das versões não atuais de um objeto com versão S3 por 2 anos.

Como a regra ILM 1 se aplica a todas as versões do objeto, você deve criar outra regra para filtrar quaisquer versões não atuais.

Para criar uma regra que use "hora não atual" como tempo de referência, selecione **Sim** para a pergunta, "aplicar esta regra apenas a versões de objetos mais antigas (em buckets S3 com controle de versão ativado)?" na Etapa 1 (Inserir detalhes) do assistente criar uma regra ILM. Quando você seleciona **Yes**, *Noncurrent Time* é selecionado automaticamente para a hora de referência e você não pode selecionar uma

hora de referência diferente.



Neste exemplo, apenas duas cópias das versões não atuais são armazenadas e essas cópias serão armazenadas por dois anos.

Definição de regra	Exemplo de valor
Pools de armazenamento	Dois pools de armazenamento, cada um em diferentes data centers, o Site 1 e o Site 2.
Nome da regra	Versões não atuais: Duas cópias dois anos
Tempo de referência	Hora não atual Selecionado automaticamente quando você seleciona **Sim** para a pergunta, "aplicar esta regra apenas a versões de objetos mais antigas (em buckets S3 com controle de versão ativado)?" no assistente criar uma regra ILM.
Colocações	No dia 0 em relação ao tempo não atual (ou seja, a partir do dia em que a versão do objeto se torna a versão não atual), mantenha duas cópias replicadas das versões de objetos não atuais por 2 anos (730 dias), uma no local 1 e outra no local 2. No final de 2 anos, exclua as versões não atuais.

Política ILM por exemplo 4: S3 objetos versionados

Se você quiser gerenciar versões mais antigas de um objeto de forma diferente da versão atual, as regras que usam "hora não atual" como tempo de referência devem aparecer na política ILM antes das regras que se aplicam à versão atual do objeto.

Uma política ILM para objetos com versão S3 pode incluir regras ILM, como as seguintes:

- Mantenha quaisquer versões mais antigas (não atuais) de cada objeto por 2 anos, a partir do dia em que a versão se tornou não atual.

> As regras de "hora não atual" devem aparecer na política antes das regras que se aplicam à versão atual do objeto. Caso contrário, as versões de objetos não atuais nunca serão correspondidas pela regra "tempo não atual".

- Na ingestão, crie três cópias replicadas e armazene uma cópia em cada um dos três locais. Mantenha cópias da versão atual do objeto por 10 anos.

Ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte forma:

- Qualquer versão de objeto não atual seria correspondida pela primeira regra. Se uma versão de objeto não atual tiver mais de 2 anos, ela será excluída permanentemente pelo ILM (todas as cópias da versão não atual removidas da grade).
- A versão atual do objeto seria correspondida pela segunda regra. Quando a versão atual do objeto é armazenada por 10 anos, o processo ILM adiciona um marcador de exclusão como a versão atual do objeto e torna a versão anterior do objeto "não atual". Na próxima vez que a avaliação do ILM ocorrer, essa versão não atual é correspondida pela primeira regra. Como resultado, a cópia no local 3 é purgada e as duas cópias no local 1 e no local 2 são armazenadas por mais 2 anos.

Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa

Você pode usar um filtro de local e o comportamento estrito de ingestão em uma regra para evitar que objetos sejam salvos em um local específico do data center.

Neste exemplo, um inquilino com sede em Paris não quer armazenar alguns objetos fora da UE devido a preocupações regulatórias. Outros objetos, incluindo todos os objetos de outras contas de inquilino, podem ser armazenados no data center de Paris ou no data center dos EUA.

> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará da forma pretendida para proteger o conteúdo da perda.

Informações relacionadas

- "Opções de ingestão"
- "Criar regra ILM: Selecione comportamento de ingestão"

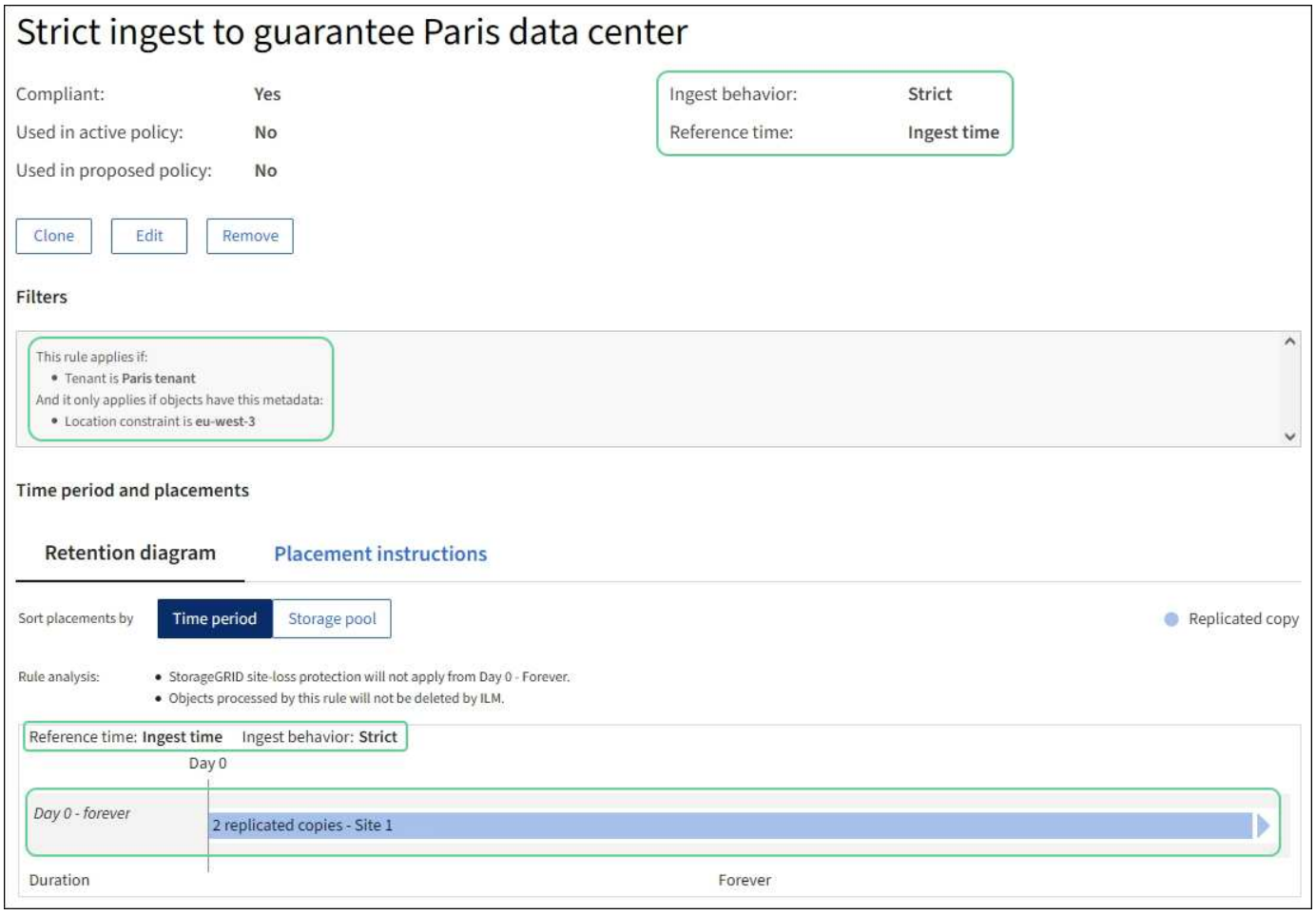
Regra 1 do ILM, por exemplo, 5: Ingestão rigorosa para garantir o data center de Paris

Este exemplo de regra de ILM usa o comportamento de ingestão rigoroso para garantir que os objetos salvos por um locatário baseado em Paris em buckets do S3 com a região definida como região eu-oeste-3 (Paris) nunca sejam armazenados no data center dos EUA.

Esta regra se aplica a objetos que pertencem ao inquilino de Paris e que têm a região de bucket S3 definida

como eu-West-3 (Paris).

Definição de regra	Exemplo de valor
Conta de locatário	Inquilino de Paris
Filtro avançado	A restrição de localização é igual à eu-West-3
Pools de armazenamento	Local 1 (Paris)
Nome da regra	Ingestão rigorosa para garantir o data center de Paris
Tempo de referência	Tempo de ingestão
Colocações	No dia 0, mantenha duas cópias replicadas para sempre no Site 1 (Paris)
Comportamento de ingestão	Rigoroso. Sempre use os posicionamentos desta regra na ingestão. A ingestão falha se não for possível armazenar duas cópias do objeto no data center de Paris.



Regra ILM 2 por exemplo 5: Ingestão equilibrada para outros objetos

Este exemplo de regra de ILM usa o comportamento de ingestão equilibrada para fornecer eficiência ideal de ILM para quaisquer objetos não correspondidos pela primeira regra. Duas cópias de todos os objetos correspondentes a essa regra serão armazenadas: Uma no data center dos EUA e outra no data center de Paris. Se a regra não puder ser satisfeita imediatamente, as cópias provisórias serão armazenadas em qualquer local disponível.

Esta regra se aplica a objetos que pertencem a qualquer locatário e a qualquer região.

Definição de regra	Exemplo de valor
Conta de locatário	Ignorar
Filtro avançado	*Não especificado*
Pools de armazenamento	Local 1 (Paris) e local 2 (EUA)
Nome da regra	2 cópias 2 Data Centers
Tempo de referência	Tempo de ingestão
Colocações	No dia 0, mantenha duas cópias replicadas para sempre em dois data centers
Comportamento de ingestão	Equilibrado. Os objetos que correspondem a essa regra são colocados de acordo com as instruções de colocação da regra, se possível. Caso contrário, cópias provisórias são feitas em qualquer local disponível.

Política de ILM, por exemplo, 5: Combinando comportamentos de ingestão

O exemplo de política ILM inclui duas regras que têm comportamentos de ingestão diferentes.

Uma política de ILM que usa dois comportamentos de ingestão diferentes pode incluir regras de ILM, como as seguintes:

- Armazene objetos que pertencem ao inquilino de Paris e que tenham a região de bucket S3 definida como eu-West-3 (Paris) apenas no data center de Paris. Falha na ingestão se o data center Paris não estiver disponível.
- Armazene todos os outros objetos (incluindo aqueles que pertencem ao locatário de Paris, mas que têm uma região de intervalo diferente) no data center dos EUA e no data center de Paris. Faça cópias provisórias em qualquer local disponível se a instrução de colocação não puder ser satisfeita.

Ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte forma:

- Quaisquer objetos que pertençam ao inquilino de Paris e que tenham a região de bucket S3 definida como eu-West-3 são correspondidos pela primeira regra e são armazenados no data center de Paris. Como a primeira regra usa ingestão rigorosa, esses objetos nunca são armazenados no data center dos EUA. Se os nós de storage no data center de Paris não estiverem disponíveis, a ingestão falhará.
- Todos os outros objetos são correspondidos pela segunda regra, incluindo objetos que pertencem ao inquilino de Paris e que não têm a região de bucket S3 definida como eu-West-3. Uma cópia de cada

objeto é salva em cada data center. No entanto, como a segunda regra usa ingestão equilibrada, se um data center não estiver disponível, duas cópias provisórias serão salvas em qualquer local disponível.

Exemplo 6: Alterar uma política ILM

Se sua proteção de dados precisar ser alterada ou você adicionar novos sites, você poderá criar e ativar uma nova política de ILM.

Antes de alterar uma política, você deve entender como as alterações nos posicionamentos de ILM podem afetar temporariamente o desempenho geral de um sistema StorageGRID.

Neste exemplo, um novo site StorageGRID foi adicionado em uma expansão e uma nova política ILM ativa precisa ser implementada para armazenar dados no novo site. Para implementar uma nova política ativa, primeiro "crie uma política". Depois disso, você deve "simular" e, em seguida"ativar", a nova política.

> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará da forma pretendida para proteger o conteúdo da perda.

Como alterar uma política ILM afeta o desempenho

Quando você ativa uma nova política de ILM, o desempenho do seu sistema StorageGRID pode ser temporariamente afetado, especialmente se as instruções de colocação na nova política exigirem que muitos objetos existentes sejam movidos para novos locais.

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.

Para garantir que uma nova política de ILM não afete o posicionamento de objetos replicados e codificados por apagamento existentes, é possível "Crie uma regra ILM com um filtro de tempo de ingestão". Por exemplo, **o tempo de ingestão *está ativado ou depois de*__**, de modo que a nova regra se aplique apenas a objetos ingeridos na ou após a data e hora especificadas.

Os tipos de alterações de política ILM que podem afetar temporariamente o desempenho do StorageGRID incluem o seguinte:

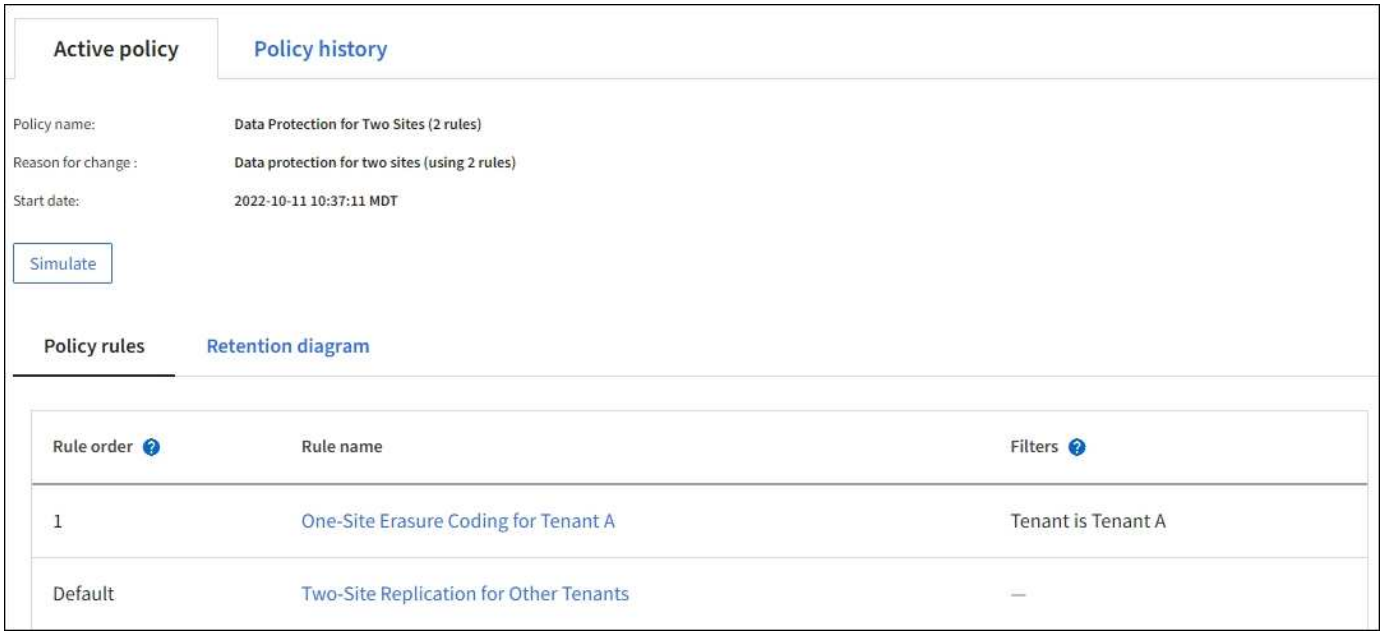
- Aplicar um perfil de codificação de apagamento diferente a objetos codificados por apagamento existentes.

  > O StorageGRID considera que cada perfil de codificação de apagamento é exclusivo e não reutiliza fragmentos de codificação de apagamento quando um novo perfil é usado.

- Alterar o tipo de cópias necessárias para objetos existentes; por exemplo, converter uma grande porcentagem de objetos replicados em objetos codificados por apagamento.
- Mover cópias de objetos existentes para um local completamente diferente; por exemplo, mover um grande número de objetos de ou para um pool de armazenamento em nuvem ou de ou para um local remoto.

Política ILM ativa, por exemplo, 6: Proteção de dados em dois locais

Neste exemplo, a política ILM ativa foi inicialmente projetada para um sistema StorageGRID de dois locais e usa duas regras ILM.



Nesta política de ILM, os objetos pertencentes ao Tenant A são protegidos pela codificação de apagamento 2-1 em um único local, enquanto os objetos pertencentes a todos os outros locatários são protegidos em dois sites que usam replicação de cópia 2.

Regra 1: Codificação de apagamento de um local para o Locatário A.

Definição de regra	Exemplo de valor
Nome da regra	Codificação de apagamento de um local para o Locatário A.
Conta de locatário	Inquilino A
Pool de storage	Local 1
Colocações	Codificação de apagamento 2-1 no local 1 do dia 0 para sempre

Regra 2: Replicação de dois locais para outros locatários

Definição de regra	Exemplo de valor
Nome da regra	Replicação de dois locais para outros locatários
Conta de locatário	Ignorar
Pools de armazenamento	Site 1 e Site 2

Definição de regra	Exemplo de valor
Colocações	Duas cópias replicadas do dia 0 para sempre: Uma cópia no local 1 e uma cópia no local 2.

Política de ILM, por exemplo, 6: Proteção de dados em três locais

Neste exemplo, a política ILM está sendo substituída por uma nova política para um sistema StorageGRID de três locais.

Depois de executar uma expansão para adicionar o novo local, o administrador da grade criou dois novos pools de storage: Um pool de storage para o local 3 e um pool de storage contendo todos os três locais (não o mesmo que o pool de storage padrão todos os nós de storage). Em seguida, o administrador criou duas novas regras ILM e uma nova política ILM, que foi projetada para proteger dados em todos os três locais.

Quando esta nova política ILM é ativada, os objetos pertencentes ao Locatário A serão protegidos pela codificação de apagamento 2-1 em três sites, enquanto os objetos pertencentes a outros locatários (e objetos menores pertencentes ao Locatário A) serão protegidos em três sites que usam replicação de 3-copy.

Regra 1: Codificação de apagamento de três locais para o Locatário A.

Definição de regra	Exemplo de valor
Nome da regra	Codificação de apagamento de três locais para o Locatário A
Conta de locatário	Inquilino A
Pool de storage	Todos os sites 3 (inclui Site 1, Site 2 e Site 3)
Colocações	Codificação de apagamento 2-1 em todos os 3 sites do dia 0 para sempre

Regra 2: Replicação de três locais para outros locatários

Definição de regra	Exemplo de valor
Nome da regra	Replicação de três locais para outros locatários
Conta de locatário	Ignorar
Pools de armazenamento	Site 1, Site 2 e Site 3
Colocações	Três cópias replicadas do dia 0 para sempre: Uma cópia no local 1, uma cópia no local 2 e uma cópia no local 3.

Ativar a política ILM, por exemplo, 6

Quando você ativa uma nova política ILM, objetos existentes podem ser movidos para novos locais ou novas cópias de objetos podem ser criadas para objetos existentes, com base nas instruções de posicionamento em

quaisquer regras novas ou atualizadas.

> Erros em uma política ILM podem causar perda de dados irrecuperável. 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.

O que acontece quando as instruções de codificação de apagamento mudam

Na política ILM atualmente ativa para este exemplo, os objetos pertencentes ao Tenant A são protegidos usando codificação de apagamento 2-1 no Site 1. Na nova política ILM, os objetos pertencentes ao Tenant A serão protegidos usando codificação de apagamento 2-1 nos sites 1, 2 e 3.

Quando a nova política ILM é ativada, ocorrem as seguintes operações ILM:

- Novos objetos ingeridos pelo Tenant A são divididos em dois fragmentos de dados e um fragmento de paridade é adicionado. Em seguida, cada um dos três fragmentos é armazenado em um local diferente.
- Os objetos existentes pertencentes ao locatário A são reavaliados durante o processo de digitalização ILM em curso. Como as instruções de posicionamento do ILM usam um novo perfil de codificação de apagamento, fragmentos totalmente novos codificados de apagamento são criados e distribuídos para os três sites.

> Os fragmentos existentes de 2 e 1 no local 1 não são reutilizados. O StorageGRID considera que cada perfil de codificação de apagamento é exclusivo e não reutiliza fragmentos de codificação de apagamento quando um novo perfil é usado.

O que acontece quando as instruções de replicação mudam

Na política de ILM atualmente ativa, neste exemplo, os objetos pertencentes a outros locatários são protegidos usando duas cópias replicadas em pools de storage nos locais 1 e 2. Na nova política de ILM, os objetos pertencentes a outros locatários serão protegidos com o uso de três cópias replicadas em pools de storage nos locais 1, 2 e 3.

Quando a nova política ILM é ativada, ocorrem as seguintes operações ILM:

- Quando qualquer locatário que não o Locatário Ingere um novo objeto, o StorageGRID cria três cópias e salva uma cópia em cada local.
- Os objetos existentes pertencentes a esses outros inquilinos são reavaliados durante o processo de digitalização ILM em curso. Como as cópias de objeto existentes no local 1 e no local 2 continuam a satisfazer os requisitos de replicação da nova regra ILM, o StorageGRID só precisa criar uma nova cópia do objeto para o local 3.

Impacto da ativação desta política no desempenho

Quando a política ILM neste exemplo é ativada, o desempenho geral deste sistema StorageGRID será temporariamente afetado. Níveis mais altos do que o normal de recursos de grade serão necessários para criar novos fragmentos codificados por apagamento para os objetos existentes do Locatário A e novas cópias

replicadas no local 3 para objetos existentes de outros locatários.

Como resultado da mudança de política do ILM, as solicitações de leitura e gravação do cliente podem ter latências temporariamente maiores do que as normais. As latências retornarão aos níveis normais depois que as instruções de colocação forem totalmente implementadas em toda a grade.

Para evitar problemas de recursos ao ativar uma nova política de ILM, você pode usar o filtro avançado de tempo de ingestão em qualquer regra que possa alterar o local de um grande número de objetos existentes. Defina o tempo de ingestão para ser maior ou igual ao tempo aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.

> Entre em Contato com o suporte técnico se precisar diminuir ou aumentar a taxa na qual os objetos são processados após uma alteração de política ILM.

Exemplo 7: Política de ILM compatível para bloqueio de objetos S3

Você pode usar o bucket S3, as regras ILM e a política ILM neste exemplo como ponto de partida ao definir uma política ILM para atender aos requisitos de proteção e retenção de objetos em buckets com o bloqueio de objetos S3 ativado.

> Se você usou o recurso de conformidade legada em versões anteriores do StorageGRID, também poderá usar este exemplo para ajudar a gerenciar quaisquer buckets existentes que tenham o recurso de conformidade legada habilitado.

> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará da forma pretendida para proteger o conteúdo da perda.

Informações relacionadas

- "Gerencie objetos com o S3 Object Lock"
- "Crie uma política ILM"

Bucket e objetos para o exemplo de bloqueio de objetos do S3

Neste exemplo, uma conta de locatário do S3 chamada Bank of ABC usou o Gerenciador do Locatário para criar um bucket com o bloqueio de objeto do S3 habilitado para armazenar Registros bancários críticos.

Definição do balde	Exemplo de valor
Nome da conta do locatário	Banco do ABC
Nome do balde	registos bancários
Região do balde	us-east-1 (predefinição)

Cada versão de objeto e objeto adicionada ao bucket de Registros bancários usará os seguintes valores para `retain-until-date` as configurações e `legal hold`.

Definição para cada objeto	Exemplo de valor
`retain-until-date`	"2030-12-30T23:59:59Z" (30 de dezembro de 2030) Cada versão de objeto tem sua `retain-until-date` própria configuração. Esta definição pode ser aumentada, mas não diminuída.
`legal hold`	"DESLIGADO" (não em vigor) Uma retenção legal pode ser colocada ou levantada em qualquer versão do objeto a qualquer momento durante o período de retenção. Se um objeto estiver sob uma retenção legal, o objeto não poderá ser excluído mesmo que o `retain-until-date` tenha sido alcançado.

Regra 1 do ILM para o S3 Object Lock exemplo: Perfil de codificação de apagamento com correspondência de intervalo

Este exemplo de regra ILM aplica-se apenas à conta de locatário S3 chamada Bank of ABC. Ele corresponde a qualquer objeto no `bank-records` bucket e, em seguida, usa a codificação de apagamento para armazenar o objeto em nós de storage em três locais de data center usando um perfil de codificação de apagamento de mais de 6 horas por dia, 3 dias por semana. Essa regra atende aos requisitos dos buckets com o bloqueio de objetos S3 ativado: Uma cópia é mantida nos nós de storage do dia 0 para sempre, usando o tempo de ingestão como o tempo de referência.

Definição de regra	Exemplo de valor
Nome da regra	Regra compatível: Objetos EC no bucket de Registros bancários - Banco do ABC
Conta de locatário	Banco do ABC
Nome do balde	`bank-records`
Filtro avançado	Tamanho do objeto (MB) maior que 1 **Nota:** este filtro garante que a codificação de apagamento não seja usada para objetos de 1 MB ou menores.

Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Colocações	Desde o dia 0 loja para sempre
Perfil de codificação de apagamento	• Crie uma cópia codificada por apagamento em nós de storage em três locais de data center • Usa o esquema de codificação de apagamento 6-3

Regra ILM 2 para o exemplo de bloqueio de objetos S3: Regra não compatível

Este exemplo de regra de ILM armazena inicialmente duas cópias de objeto replicadas em nós de storage. Após um ano, ele armazena uma cópia em um pool de storage de nuvem para sempre. Como essa regra usa um pool de armazenamento em nuvem, ela não é compatível e não se aplica aos objetos em buckets com o bloqueio de objetos do S3 ativado.

Definição de regra	Exemplo de valor
Nome da regra	Regra não compatível: Use o Cloud Storage Pool
Contas de inquilino	Não especificado
Nome do intervalo	Não especificado, mas só se aplicará a buckets que não tenham o bloqueio de objeto S3 (ou o recurso de conformidade legado) habilitado.
Filtro avançado	Não especificado

Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Colocações	• No dia 0, mantenha duas cópias replicadas nos nós de storage no data center 1 e no data center 2 por 365 dias • Após 1 ano, mantenha uma cópia replicada em um pool de storage de nuvem para sempre

Regra ILM 3 para o exemplo de bloqueio de objetos S3: Regra padrão

Este exemplo de regra de ILM copia dados de objetos para pools de storage em dois data centers. Esta regra compatível foi projetada para ser a regra padrão na política ILM. Ele não inclui nenhum filtro, não usa o tempo de referência não atual e satisfaz os requisitos de buckets com o bloqueio de objeto S3 ativado: Duas cópias de objeto são mantidas em nós de armazenamento do dia 0 para sempre, usando a ingestão como o tempo de referência.

Definição de regra	Exemplo de valor
Nome da regra	Regra de conformidade padrão: Duas cópias dois Data Centers
Conta de locatário	Não especificado
Nome do intervalo	Não especificado
Filtro avançado	Não especificado

Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão

Definição de regra	Exemplo de valor
Colocações	Do dia 0 até sempre, mantenha duas cópias replicadas: Uma em nós de storage no data center 1 e uma em nós de storage no data center 2.

Política ILM compatível para o exemplo de bloqueio de objetos S3

Para criar uma política de ILM que proteja efetivamente todos os objetos em seu sistema, incluindo aqueles em buckets com o bloqueio de objetos S3 ativado, você deve selecionar regras de ILM que atendam aos requisitos de armazenamento de todos os objetos. Em seguida, você deve simular e ativar a política.

Adicione regras à política

Neste exemplo, a política ILM inclui três regras ILM, na seguinte ordem:

1. Uma regra compatível que usa codificação de apagamento para proteger objetos com mais de 1 MB em um bucket específico com o bloqueio de objetos S3 ativado. Os objetos são armazenados nos nós de storage do dia 0 para sempre.
2. Regra não compatível que cria duas cópias de objetos replicadas em nós de storage por um ano e move uma cópia de objeto para um pool de storage de nuvem para sempre. Esta regra não se aplica a buckets com o bloqueio de objetos do S3 ativado porque usa um pool de armazenamento em nuvem.
3. A regra em conformidade padrão que cria duas cópias de objetos replicadas nos nós de storage do dia 0 para sempre.

Simule a política

Depois de adicionar regras à política, escolher uma regra compatível padrão e organizar as outras regras, você deve simular a política testando objetos do bucket com o bloqueio de objetos S3 ativado e de outros buckets. Por exemplo, quando você simula a política de exemplo, espera-se que os objetos de teste sejam avaliados da seguinte forma:

- A primeira regra só corresponderá a objetos de teste maiores que 1 MB nos Registros de banco de buckets para o locatário do Bank of ABC.
- A segunda regra corresponderá a todos os objetos em todos os buckets não compatíveis para todas as outras contas de inquilino.
- A regra padrão corresponderá a estes objetos:
  - Objetos 1 MB ou mais pequenos nos Registros de banco de buckets para o inquilino do Banco do ABC.
  - Objetos em qualquer outro bucket que tenha o bloqueio de objeto S3 ativado para todas as outras contas de locatário.

Ative a política

Quando você estiver completamente satisfeito que a nova política protege os dados de objetos conforme esperado, você pode ativá-los.

Exemplo 8: Prioridades para o ciclo de vida do bucket do S3 e a política de ILM

Dependendo da configuração do ciclo de vida, os objetos seguem as configurações de retenção do ciclo de vida do bucket do S3 ou de uma política ILM.

Exemplo de ciclo de vida do bucket tendo prioridade sobre a política de ILM

Política de ILM

- Regra baseada em referência não atual: No dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): No dia 0, mantenha X cópias por 50 dias

Ciclo de vida do bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Resultado

- Um objeto chamado "docs/text" é ingerido. Ele corresponde ao filtro de ciclo de vida do bucket do prefixo "docs/".
  - Após 100 dias, um marcador de exclusão é criado e "docs/text" torna-se não atual.
  - Após 5 dias, um total de 105 dias desde a ingestão, "docs/text" é excluído.
  - Após 95 dias, um total de 200 dias desde a ingestão e 100 dias desde que o marcador de exclusão foi criado, o marcador de exclusão expirado é excluído.
- Um objeto chamado "vídeo/filme" é ingerido. Ele não corresponde ao filtro e usa a política de retenção ILM.
  - Após 50 dias, um marcador de exclusão é criado e "vídeo/filme" torna-se não atual.
  - Após 20 dias, um total de 70 dias desde a ingestão, "vídeo/filme" é excluído.
  - Após 30 dias, um total de 100 dias desde a ingestão e 50 dias desde que o marcador de exclusão foi criado, o marcador de exclusão expirado é excluído.

Exemplo de ciclo de vida do bucket implicitamente keeping-Forever

Política de ILM

- Regra baseada em referência não atual: No dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): No dia 0, mantenha X cópias por 50 dias

Ciclo de vida do bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

Resultado

- Um objeto chamado "docs/text" é ingerido. Ele corresponde ao filtro de ciclo de vida do bucket do prefixo "docs/".

  A `Expiration` ação aplica-se apenas aos marcadores de exclusão expirados, o que implica manter tudo o resto para sempre (começando com "docs/").

  Excluir marcadores que começam com "docs/" são removidos quando expiram.

- Um objeto chamado "vídeo/filme" é ingerido. Ele não corresponde ao filtro e usa a política de retenção ILM.
  - Após 50 dias, um marcador de exclusão é criado e "vídeo/filme" torna-se não atual.
  - Após 20 dias, um total de 70 dias desde a ingestão, "vídeo/filme" é excluído.
  - Após 30 dias, um total de 100 dias desde a ingestão e 50 dias desde que o marcador de exclusão

foi criado, o marcador de exclusão expirado é excluído.

Exemplo de uso do ciclo de vida do bucket para duplicar o ILM e limpar marcadores de exclusão expirados

Política de ILM

- Regra baseada em referência não atual: No dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): No dia 0, mantenha X cópias para sempre

Ciclo de vida do bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Resultado

- A política de ILM é duplicada no ciclo de vida do bucket.
  - A regra Forever da política ILM foi projetada para remover objetos manualmente e limpar versões não atuais após 20 dias. Consequentemente, a regra de tempo de ingestão manterá marcadores de exclusão expirados para sempre.
  - O ciclo de vida do bucket duplica o comportamento da política ILM ao adicionar `"ExpiredObjectDeleteMarker": true`, que remove marcadores de exclusão depois que eles expirarem
- Um objeto é ingerido. Nenhum filtro significa que o ciclo de vida do bucket se aplica a todos os objetos e substitui as configurações de retenção do ILM.
  - Quando um locatário emite uma solicitação de exclusão de objeto, um marcador de exclusão é criado e o objeto se torna não atual.
  - Após 20 dias, o objeto não atual é excluído e o marcador de exclusão fica expirado.
  - Pouco tempo depois, o marcador de exclusão expirado é excluído.

Endurecimento do sistema

Considerações gerais para o endurecimento do sistema

O fortalecimento do sistema é o processo de eliminar o maior número possível de riscos de segurança a partir de um sistema StorageGRID.

À medida que você instala e configura o StorageGRID, use estas diretrizes para ajudá-lo a cumprir quaisquer objetivos de segurança prescritos quanto a confidencialidade, integridade e disponibilidade.

Você já deve estar usando as melhores práticas padrão do setor para o fortalecimento do sistema. Por exemplo, você usa senhas fortes para StorageGRID, usa HTTPS em vez de HTTP e ativa autenticação baseada em certificado quando disponível.

StorageGRID segue o "Política de tratamento de vulnerabilidades do NetApp". Vulnerabilidades relatadas são verificadas e resolvidas de acordo com o processo de resposta a incidentes de segurança do produto.

Ao endurecer um sistema StorageGRID, considere o seguinte:

- **Qual das três redes StorageGRID** você implementou. Todos os sistemas StorageGRID devem usar a rede de grade, mas você também pode estar usando a rede de administrador, a rede de cliente ou ambos. Cada rede tem diferentes considerações de segurança.

- **O tipo de plataformas** que você usa para os nós individuais em seu sistema StorageGRID. Os nós do StorageGRID podem ser implantados em máquinas virtuais VMware, dentro de um mecanismo de contêiner em hosts Linux ou como dispositivos de hardware dedicados. Cada tipo de plataforma tem seu próprio conjunto de melhores práticas de endurecimento.
- **Como as contas de inquilino são confiáveis**. Se você for um provedor de serviços com contas de inquilino não confiáveis, terá preocupações de segurança diferentes do que se você usar apenas locatários internos confiáveis.
- **Que requisitos e convenções de segurança** sua organização segue. Talvez seja necessário cumprir requisitos específicos de regulamentação ou de empresas.

Diretrizes de fortalecimento para atualizações de software

Você deve manter seu sistema StorageGRID e serviços relacionados atualizados para se defender contra ataques.

Atualizações para o software StorageGRID

Sempre que possível, você deve atualizar o software StorageGRID para a versão principal mais recente ou para a versão principal anterior. Manter o StorageGRID atualizado ajuda a reduzir o tempo em que as vulnerabilidades conhecidas estão ativas e reduz a área geral da superfície de ataque. Além disso, as versões mais recentes do StorageGRID geralmente contêm recursos de proteção de segurança que não estão incluídos em versões anteriores.

Consulte o "Ferramenta de Matriz de interoperabilidade do NetApp" (IMT) para determinar qual versão do software StorageGRID você deve usar. Quando um hotfix é necessário, o NetApp prioriza a criação de atualizações para as versões mais recentes. Alguns patches podem não ser compatíveis com versões anteriores.

- Para baixar as versões e hotfixes mais recentes do StorageGRID, vá para "NetApp Downloads: StorageGRID".
- Para atualizar o software StorageGRID, consulte "instruções de atualização".
- Para aplicar um hotfix, consulte "Procedimento de correção do StorageGRID".

Upgrades para serviços externos

Os serviços externos podem ter vulnerabilidades que afetam o StorageGRID indiretamente. Você deve garantir que os serviços dos quais o StorageGRID depende são atualizados. Esses serviços incluem LDAP, KMS (ou servidor KMIP), DNS e NTP.

Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Atualizações para hypervisors

Se seus nós do StorageGRID estiverem em execução no VMware ou em outro hypervisor, você deverá garantir que o software e o firmware do hypervisor estejam atualizados.

Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

*** Atualizações para nós Linux***

Se seus nós do StorageGRID estiverem usando plataformas host Linux, você deve garantir que as atualizações de segurança e as atualizações do kernel sejam aplicadas ao sistema operacional do host. Além disso, você deve aplicar atualizações de firmware a hardware vulnerável quando essas atualizações estiverem disponíveis.

Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Diretrizes de fortalecimento para redes StorageGRID

O sistema StorageGRID suporta até três interfaces de rede por nó de grade, permitindo que você configure a rede para cada nó de grade individual de acordo com seus requisitos de segurança e acesso.

Para obter informações detalhadas sobre redes StorageGRID, consulte "Tipos de rede StorageGRID".

Diretrizes para rede de Grade

Você deve configurar uma rede de grade para todo o tráfego interno do StorageGRID. Todos os nós de grade estão na rede de grade e eles devem ser capazes de falar com todos os outros nós.

Ao configurar a rede de Grade, siga estas diretrizes:

- Certifique-se de que a rede está protegida de clientes não fidedignos, como os que se encontram na Internet aberta.
- Quando possível, use a rede de Grade exclusivamente para tráfego interno. Tanto a rede Admin quanto a rede Client têm restrições adicionais de firewall que bloqueiam o tráfego externo para serviços internos. O uso da rede de Grade para tráfego de cliente externo é suportado, mas esse uso oferece menos camadas de proteção.
- Se a implantação do StorageGRID abranger vários data centers, use uma rede privada virtual (VPN) ou equivalente na rede de grade para fornecer proteção adicional para o tráfego interno.
- Alguns procedimentos de manutenção exigem acesso de shell seguro (SSH) na porta 22 entre o nó de administração principal e todos os outros nós de grade. Use um firewall externo para restringir o acesso SSH a clientes confiáveis.

Diretrizes para Admin Network

A rede de administração é normalmente usada para tarefas administrativas (funcionários confiáveis usando o Gerenciador de Grade ou SSH) e para se comunicar com outros serviços confiáveis, como LDAP, DNS, NTP ou KMS (ou servidor KMIP). No entanto, o StorageGRID não aplica esse uso internamente.

Se você estiver usando a rede Admin, siga estas diretrizes:

- Bloqueie todas as portas de tráfego internas na rede Admin. Consulte "lista de portas internas".
- Se os clientes não confiáveis puderem acessar a rede de administração, bloqueie o acesso ao StorageGRID na rede de administração com um firewall externo.

Diretrizes para rede de clientes

A rede do cliente é normalmente usada para locatários e para se comunicar com serviços externos, como o

serviço de replicação do CloudMirror ou outro serviço de plataforma. No entanto, o StorageGRID não aplica esse uso internamente.

Se você estiver usando a rede de clientes, siga estas diretrizes:

- Bloqueie todas as portas de tráfego internas na rede do cliente. Consulte "lista de portas internas".
- Aceite o tráfego de clientes de entrada apenas em endpoints explicitamente configurados. Consulte as informações sobre "gerenciamento de controles de firewall"o .

Diretrizes de fortalecimento para nós de StorageGRID

Os nós do StorageGRID podem ser implantados em máquinas virtuais VMware, dentro de um mecanismo de contêiner em hosts Linux ou como dispositivos de hardware dedicados. Cada tipo de plataforma e cada tipo de nó tem seu próprio conjunto de práticas recomendadas de endurecimento.

Controle o acesso remoto IPMI ao BMC

Você pode ativar ou desativar o acesso remoto IPMI para todos os dispositivos que contêm um BMC. A interface IPMI remota permite o acesso de hardware de baixo nível aos seus dispositivos StorageGRID por qualquer pessoa com uma conta e senha do BMC. Se você não precisar de acesso remoto IPMI ao BMC, desative esta opção.

- Para controlar o acesso remoto IPMI ao BMC no Gerenciador de Grade, vá para **CONFIGURATION** > **Security** > **Security settings** > **Appliances**:
  - Desmarque a caixa de seleção **Enable Remote IPMI Access** (Ativar acesso remoto IPMI) para desativar o acesso IPMI ao BMC.
  - Marque a caixa de seleção **Enable Remote IPMI Access** (Ativar acesso remoto IPMI) para habilitar o acesso IPMI ao BMC.

Configuração da firewall

Como parte do processo de fortalecimento do sistema, você deve revisar as configurações de firewall externo e modificá-las para que o tráfego seja aceito apenas a partir dos endereços IP e nas portas a partir das quais é estritamente necessário.

O StorageGRID inclui um firewall interno em cada nó que aumenta a segurança da sua grade, permitindo que você controle o acesso da rede ao nó. Você deve "gerenciar controles internos de firewall"impedir o acesso à rede em todas as portas, exceto as necessárias para a implantação da grade específica. As alterações de configuração feitas na página de controle do Firewall são implantadas em cada nó.

Especificamente, você pode gerenciar essas áreas:

- **Endereços privilegiados**: Você pode permitir que endereços IP ou sub-redes selecionadas acessem portas fechadas por configurações na guia Gerenciar acesso externo.
- **Gerenciar acesso externo**: Você pode fechar portas abertas por padrão ou reabrir portas previamente fechadas.
- **Rede cliente não confiável**: Você pode especificar se um nó confia no tráfego de entrada da rede cliente, bem como as portas adicionais que deseja abrir quando a rede cliente não confiável está configurada.

Embora esse firewall interno forneça uma camada adicional de proteção contra algumas ameaças comuns,

ele não remove a necessidade de um firewall externo.

Para obter uma lista de todas as portas internas e externas usadas pelo StorageGRID, "Referência da porta de rede"consulte .

Desativar serviços não utilizados

Para todos os nós do StorageGRID, você deve desativar ou bloquear o acesso a serviços não utilizados. Por exemplo, se você não estiver planejando usar DHCP, use o Gerenciador de Grade para fechar a porta 68. Selecione **CONFIGURATION** > **Firewall control** > **Manage external access**. Em seguida, altere a opção Status para a porta 68 de **Open** para **Closed**.

Virtualização, contêineres e hardware compartilhado

Para todos os nós do StorageGRID, evite executar o StorageGRID no mesmo hardware físico que o software não confiável. Não assuma que as proteções do hipervisor irão impedir que o malware acesse dados protegidos pela StorageGRID se o StorageGRID e o malware existirem no mesmo hardware físico. Por exemplo, os ataques Meltdown e Spectre exploram vulnerabilidades críticas em processadores modernos e permitem que programas roubem dados na memória no mesmo computador.

Proteja os nós durante a instalação

Não permita que usuários não confiáveis acessem nós do StorageGRID pela rede quando os nós estiverem sendo instalados. Os nós não são totalmente seguros até que eles se juntem à grade.

Diretrizes para nós de administração

Os nós de administração fornecem serviços de gerenciamento, como configuração, monitoramento e log do sistema. Quando você entra no Gerenciador de Grade ou no Gerenciador de Tenant, você está se conetando a um nó Admin.

Siga estas diretrizes para proteger os nós de administração no seu sistema StorageGRID:

- Proteja todos os nós de administração de clientes não confiáveis, como aqueles na Internet aberta. Certifique-se de que nenhum cliente não confiável possa acessar qualquer nó Admin na rede de Grade, na rede Admin ou na rede Cliente.
- Os grupos StorageGRID controlam o acesso aos recursos do Gerenciador de Grade e do Gerenciador de Locatário. Conceda a cada grupo de usuários as permissões mínimas necessárias para sua função e use o modo de acesso somente leitura para impedir que os usuários alterem a configuração.
- Ao usar pontos de extremidade do balanceador de carga do StorageGRID, use nós de gateway em vez de nós de administrador para obter tráfego de cliente não confiável.
- Se você tiver locatários não confiáveis, não permita que eles tenham acesso direto ao Gerenciador do Locatário ou à API de Gerenciamento do Locatário. Em vez disso, peça a qualquer inquilino não confiável que use um portal de locatário ou um sistema de gerenciamento de inquilino externo, que interage com a API de gerenciamento do locatário.
- Opcionalmente, use um proxy de administrador para obter mais controle sobre a comunicação do AutoSupport de nós de administração para o suporte do NetApp. Consulte os passos para "criando um proxy de administrador".
- Opcionalmente, use as portas 8443 e 9443 restritas para separar as comunicações do Grid Manager e do Tenant Manager. Bloqueie a porta compartilhada 443 e limite as solicitações do locatário à porta 9443 para proteção adicional.
- Opcionalmente, use nós de administração separados para administradores de grade e usuários de

locatário.

Para obter mais informações, consulte as instruções para "Administrando o StorageGRID".

Diretrizes para nós de storage

Os nós de storage gerenciam e armazenam dados e metadados de objetos. Siga estas diretrizes para proteger os nós de storage em seu sistema StorageGRID.

- Não permita que clientes não confiáveis se conetem diretamente aos nós de storage. Use um ponto de extremidade do balanceador de carga servido por um nó de gateway ou um balanceador de carga de terceiros.
- Não ative serviços de saída para locatários não confiáveis. Por exemplo, ao criar a conta para um locatário não confiável, não permita que o locatário use sua própria fonte de identidade e não permita o uso de serviços de plataforma. Consulte os passos para "criando uma conta de locatário".
- Use um balanceador de carga de terceiros para tráfego de clientes não confiável. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques.
- Como opção, use um proxy de storage para obter mais controle sobre a comunicação de pools de storage em nuvem e serviços de plataforma dos nós de storage para serviços externos. Consulte os passos para "criando um proxy de armazenamento".
- Opcionalmente, conete-se a serviços externos usando a rede do cliente. Em seguida, selecione **CONFIGURATION** > **Security** > **Firewall control** > **UnTrusted Client Networks** e indique que a rede do cliente no nó de armazenamento não é confiável. O nó de armazenamento não aceita mais nenhum tráfego de entrada na rede do cliente, mas continua a permitir solicitações de saída para Serviços de plataforma.

Diretrizes para nós de gateway

Os nós de gateway fornecem uma interface de balanceamento de carga opcional que os aplicativos clientes podem usar para se conetar ao StorageGRID. Siga estas diretrizes para proteger quaisquer nós de gateway no seu sistema StorageGRID:

- Configure e use pontos de extremidade do balanceador de carga. "Considerações para balanceamento de carga"Consulte .
- Use um balanceador de carga de terceiros entre o cliente e o nó de gateway ou nós de storage para obter tráfego de cliente não confiável. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques. Se você usar um balanceador de carga de terceiros, o tráfego de rede ainda poderá ser configurado opcionalmente para passar por um ponto de extremidade do balanceador de carga interno ou ser enviado diretamente para nós de storage.
- Se você estiver usando pontos de extremidade do balanceador de carga, opcionalmente, faça com que os clientes se conetem pela rede do cliente. Em seguida, selecione **CONFIGURATION** > **Security** > **Firewall control** > **UnTrusted Client Networks** e indique que a rede Client no Gateway Node não é confiável. O Gateway Node aceita apenas tráfego de entrada nas portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

Diretrizes para nós de dispositivos de hardware

Os aparelhos de hardware StorageGRID são especialmente projetados para uso em um sistema StorageGRID. Alguns dispositivos podem ser usados como nós de storage. Outros dispositivos podem ser usados como nós de administrador ou nós de gateway. Você pode combinar nós de dispositivo com nós baseados em software ou implantar grades totalmente projetadas para todos os dispositivos.

Siga estas diretrizes para proteger todos os nós de dispositivos de hardware no seu sistema StorageGRID:

- Se o dispositivo usar o Gerenciador de sistema do SANtricity para o gerenciamento do controlador de storage, evite que clientes não confiáveis acessem o Gerenciador de sistema do SANtricity pela rede.
- Se o dispositivo tiver um controlador de gerenciamento de placa base (BMC), esteja ciente de que a porta de gerenciamento BMC permite acesso a hardware de baixo nível. Conete a porta de gerenciamento BMC somente a uma rede de gerenciamento interna segura, confiável. Se nenhuma rede estiver disponível, deixe a porta de gerenciamento do BMC desconetada ou bloqueada, a menos que uma conexão BMC seja solicitada pelo suporte técnico.
- Se o dispositivo suportar o gerenciamento remoto do hardware do controlador via Ethernet usando o padrão IPMI (Intelligent Platform Management Interface), bloqueie o tráfego não confiável na porta 623.

> Você pode ativar ou desativar o acesso remoto IPMI para todos os dispositivos que contêm um BMC. A interface IPMI remota permite o acesso de hardware de baixo nível aos seus dispositivos StorageGRID por qualquer pessoa com uma conta e senha do BMC. Se você não precisar de acesso remoto IPMI ao BMC, desative esta opção usando um dos seguintes métodos: No Gerenciador de Grade, vá para **CONFIGURATION** > **Security** > **Security** > **Security settings** > **Appliances** e desmarque a caixa de seleção **Enable Remote IPMI Access**. Na API de gerenciamento de grade, use o endpoint privado: `PUT /private/bmc`.

- Para modelos de dispositivo que contêm unidades SED, FDE ou FIPS NL-SAS que você gerencia com o SANtricity System Manager, "Ative e configure a Segurança da Unidade SANtricity".
- Para modelos de dispositivo que contêm SSDs NVMe FIPS ou SED que você gerencia usando o instalador de dispositivos StorageGRID e o Gerenciador de Grade, "Ativar e configurar a encriptação da unidade StorageGRID".
- Para dispositivos sem unidades SED, FDE ou FIPS, habilite e configure a criptografia de nó de software do StorageGRID "Usando um servidor de gerenciamento de chaves (KMS)" .

Diretrizes de fortalecimento para TLS e SSH

Você deve substituir os certificados padrão criados durante a instalação e selecionar a diretiva de segurança apropriada para conexões TLS e SSH.

Diretrizes de endurecimento para certificados

Você deve substituir os certificados padrão criados durante a instalação por seus próprios certificados personalizados.

Para muitas organizações, o certificado digital autoassinado para o acesso à Web StorageGRID não é compatível com suas políticas de segurança de informações. Em sistemas de produção, você deve instalar um certificado digital assinado pela CA para uso na autenticação do StorageGRID.

Especificamente, você deve usar certificados de servidor personalizados em vez desses certificados padrão:

- **Certificado de interface de gerenciamento**: Usado para proteger o acesso ao Gerenciador de Grade, ao Gerenciador de locatário, à API de gerenciamento de grade e à API de gerenciamento do locatário.
- **S3 API certificate**: Usado para proteger o acesso aos nós de armazenamento e nós de Gateway, que os aplicativos clientes S3 usam para carregar e baixar dados de objetos.

"Gerenciar certificados de segurança"Consulte para obter detalhes e instruções.

O StorageGRID gerencia os certificados usados para pontos de extremidade do balanceador de carga separadamente. Para configurar os certificados do balanceador de carga, "Configurar pontos de extremidade do balanceador de carga"consulte .

Ao usar certificados de servidor personalizados, siga estas diretrizes:

- Os certificados devem ter um `subjectAltName` que corresponda às entradas de DNS para StorageGRID. Para obter detalhes, consulte a seção 4,2.1,6, "Nome alternativo do assunto", em "RFC 5280: Certificado PKIX e perfil CRL".
- Quando possível, evite o uso de certificados curinga. Uma exceção a essa diretriz é o certificado para um endpoint de estilo hospedado virtual S3, que requer o uso de um curinga se os nomes de bucket não forem conhecidos antecipadamente.
- Quando você deve usar curingas em certificados, você deve tomar medidas adicionais para reduzir os riscos. Use um padrão curinga como `*.s3.example.com` , e não use o `s3.example.com` sufixo para outros aplicativos. Esse padrão também funciona com acesso S3D de estilo caminho, como `dc1-s1.s3.example.com/mybucket` .
- Defina os tempos de expiração do certificado como curtos (por exemplo, 2 meses) e use a API Grid Management para automatizar a rotação do certificado. Isso é especialmente importante para certificados curinga.

Além disso, os clientes devem usar uma verificação rigorosa do nome de host ao se comunicar com o StorageGRID.

Diretrizes de fortalecimento para a política TLS e SSH

Você pode selecionar uma política de segurança para determinar quais protocolos e cifras são usados para estabelecer conexões TLS seguras com aplicativos cliente e conexões SSH seguras com serviços StorageGRID internos.

A política de segurança controla como TLS e SSH criptografam dados em movimento. Como prática recomendada, você deve desativar as opções de criptografia que não são necessárias para a compatibilidade de aplicativos. Use a política moderna padrão, a menos que seu sistema precise ser compatível com critérios comuns ou que você precise usar outras cifras.

"Gerencie a política TLS e SSH"Consulte para obter detalhes e instruções.

Outras diretrizes de endurecimento

Além de seguir as diretrizes de proteção para redes e nós StorageGRID, você deve seguir as diretrizes de proteção para outras áreas do sistema StorageGRID.

Palavra-passe de instalação temporária

Para proteger o sistema StorageGRID durante a instalação, defina uma senha na página de senha do instalador temporário na IU de instalação do StorageGRID ou na API de instalação. Quando definida, essa senha se aplica a todos os métodos de instalação do StorageGRID, incluindo a interface do usuário, a API de instalação e `configure-storagegrid.py` o script.

Para obter mais informações, consulte:

- "Instale o StorageGRID no Red Hat Enterprise Linux"

- "Instale o StorageGRID no Ubuntu ou Debian"
- "Instale o StorageGRID no VMware"
- "Instale o dispositivo StorageGRID"

Logs e mensagens de auditoria

Proteja sempre os logs do StorageGRID e a saída de mensagens de auditoria de forma segura. Os logs do StorageGRID e as mensagens de auditoria fornecem informações inestimáveis do ponto de vista de suporte e disponibilidade do sistema. Além disso, as informações e detalhes contidos nos logs do StorageGRID e na saída de mensagens de auditoria são geralmente de natureza sensível.

Configure o StorageGRID para enviar eventos de segurança para um servidor syslog externo. Se estiver usando a exportação syslog, selecione TLS e RELP/TLS para os protocolos de transporte.

Consulte o "Referência de ficheiros de registo" para obter mais informações sobre os registos do StorageGRID. Consulte "Auditar mensagens" para obter mais informações sobre mensagens de auditoria do StorageGRID.

NetApp AutoSupport

O recurso AutoSupport do StorageGRID permite que você monitore proativamente a integridade do seu sistema e envie automaticamente pacotes para o site de suporte da NetApp, a equipe de suporte interna da sua organização ou um parceiro de suporte. Por padrão, o envio de pacotes AutoSupport para o NetApp é ativado quando o StorageGRID é configurado pela primeira vez.

O recurso AutoSupport pode ser desativado. No entanto, o NetApp recomenda habilitá-lo, pois o AutoSupport ajuda a acelerar a identificação e resolução de problemas caso surja algum problema no seu sistema StorageGRID.

O AutoSupport suporta HTTPS, HTTP e SMTP para protocolos de transporte. Devido à natureza sensível dos pacotes AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar pacotes AutoSupport para o NetApp.

Compartilhamento de recursos entre origens (CORS)

Você pode configurar o compartilhamento de recursos entre origens (CORS) para um bucket do S3 se quiser que esse bucket e objetos nesse bucket estejam acessíveis a aplicativos da Web em outros domínios. Em geral, não ative o CORS a menos que seja necessário. Se CORS for necessário, restrinja-o a origens confiáveis.

Consulte os passos para "Configurando o compartilhamento de recursos entre origens (CORS)".

Dispositivos de segurança externos

Uma solução completa de endurecimento deve abordar mecanismos de segurança fora do StorageGRID. O uso de dispositivos de infraestrutura adicionais para filtrar e limitar o acesso ao StorageGRID é uma maneira eficaz de estabelecer e manter uma postura de segurança rigorosa. Esses dispositivos de segurança externos incluem firewalls, sistemas de prevenção de intrusão (IPSs) e outros dispositivos de segurança.

Um balanceador de carga de terceiros é recomendado para tráfego de clientes não confiável. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques.

Mitigação de ransomware

Ajude a proteger os dados de objetos de ataques de ransomware seguindo as recomendações da "Defesa contra ransomware com o StorageGRID".

Configurar o StorageGRID para FabricPool

Configurar o StorageGRID para FabricPool

Se você usar o software NetApp ONTAP, poderá usar o NetApp FabricPool para categorizar dados inativos em um sistema de storage de objetos NetApp StorageGRID.

Use estas instruções para:

- Conheça as considerações e práticas recomendadas para configurar o StorageGRID para uma carga de trabalho do FabricPool.
- Saiba como configurar um sistema de armazenamento de objetos StorageGRID para uso com o FabricPool.
- Saiba como fornecer os valores necessários ao ONTAP ao anexar o StorageGRID como uma camada de nuvem do FabricPool.

Início rápido para configurar o StorageGRID para FabricPool

1 **Planeje sua configuração**

- Decida qual política de disposição em categorias de volume do FabricPool você usará para categorizar dados do ONTAP inativos no StorageGRID.
- Planejar e instalar um sistema StorageGRID para atender às suas necessidades de capacidade de storage e performance.
- Familiarize-se com o software de sistema StorageGRID, incluindo o "Gerenciador de grade" e o "Gerente do locatário".
- Consulte as práticas recomendadas do FabricPool para "Grupos HA", "balanceamento de carga", "ILM"e "mais".
- Revise esses recursos adicionais, que fornecem detalhes sobre como usar e configurar o ONTAP e o FabricPool:

  "TR-4598: Melhores práticas da FabricPool em ONTAP"

  "Documentação do ONTAP para FabricPool"

2 **Executar tarefas pré-requisitos**

Obter o "Informações necessárias para anexar o StorageGRID como uma categoria de nuvem", incluindo:

- Endereços IP
- Nomes de domínio
- Certificado SSL

Opcionalmente, configure "federação de identidade" e "logon único".

3 Configure as definições do StorageGRID

Use StorageGRID para obter os valores que o ONTAP precisa para se conetar à grade.

Usar o "Assistente de configuração do FabricPool" é a maneira recomendada e mais rápida de configurar todos os itens, mas você também pode configurar cada entidade manualmente, se necessário.

4 Configurar ONTAP e DNS

Use ONTAP para "adicionar uma camada de nuvem" que use os valores StorageGRID. Em seguida, "Configurar entradas DNS" para associar endereços IP a qualquer nome de domínio que você pretende usar.

5 Monitorar e gerenciar

Quando o sistema estiver funcionando, execute tarefas contínuas no ONTAP e no StorageGRID para gerenciar e monitorar a disposição de dados em camadas do FabricPool ao longo do tempo.

O que é o FabricPool?

O FabricPool é uma solução de storage híbrido da ONTAP que usa um agregado flash de alto desempenho como a categoria de performance e um armazenamento de objetos como a categoria de nuvem. O uso de agregados habilitados para FabricPool ajuda a reduzir custos de storage sem comprometer a performance, a eficiência ou a proteção.

O FabricPool associa uma camada de nuvem (um armazenamento de objetos externo, como o StorageGRID) a uma camada local (um agregado de storage ONTAP) para criar uma coleção composta de discos. Os volumes no FabricPool podem aproveitar a disposição em categorias mantendo os dados ativos (quentes) no storage de alta performance (a camada local) e a disposição em camadas inativada (fria) no armazenamento de objetos externo (a camada de nuvem).

Nenhuma mudança de arquitetura é necessária. Assim, você continua gerenciando seus dados e ambiente da aplicação usando o sistema de storage central da ONTAP.

O que é o StorageGRID?

O NetApp StorageGRID é uma arquitetura de storage que gerencia dados como objetos, em vez de outras arquiteturas de storage, como storage de arquivos ou blocos. Os objetos são mantidos dentro de um único contentor (como um bucket) e não são aninhados como arquivos dentro de um diretório dentro de outros diretórios. Embora o storage de objetos geralmente forneça performance inferior ao storage de arquivos ou blocos, ele é significativamente mais dimensionável. Os buckets do StorageGRID podem armazenar petabytes de dados e bilhões de objetos.

Por que usar o StorageGRID como uma categoria de nuvem do FabricPool?

O FabricPool pode categorizar dados do ONTAP em vários fornecedores de storage de objetos, incluindo o StorageGRID. Ao contrário de nuvens públicas que podem definir um número máximo de operações de entrada/saída por segundo (IOPS) com suporte no nível do bucket ou do contêiner, a performance do StorageGRID é dimensionada de acordo com o número de nós em um sistema. O uso do StorageGRID como uma categoria de nuvem do FabricPool permite que você mantenha os dados inativos na sua própria nuvem privada para obter a mais alta performance e controle total sobre os dados.

Além disso, não é necessária uma licença FabricPool ao usar o StorageGRID como camada de nuvem.

Informações necessárias para anexar o StorageGRID como uma categoria de nuvem

Antes de anexar o StorageGRID como uma categoria de nuvem para o FabricPool, você deve executar as etapas de configuração no StorageGRID e obter certos valores para uso no ONTAP.

Quais valores eu preciso?

A tabela a seguir mostra os valores que você deve configurar no StorageGRID e como esses valores são usados pelo ONTAP e pelo servidor DNS.

Valor	Onde o valor está configurado	Onde o valor é usado
Endereços IP virtuais (VIP)	StorageGRID > grupo HA	Entrada DNS
Porta	StorageGRID > ponto final do balanceador de carga	Gerenciador de sistema do ONTAP > Adicionar nível de nuvem
Certificado SSL	StorageGRID > ponto final do balanceador de carga	Gerenciador de sistema do ONTAP > Adicionar nível de nuvem
Nome do servidor (FQDN)	StorageGRID > ponto final do balanceador de carga	Entrada DNS
ID da chave de acesso e chave de acesso secreta	StorageGRID > locatário e balde	Gerenciador de sistema do ONTAP > Adicionar nível de nuvem
Nome do balde/recipiente	StorageGRID > locatário e balde	Gerenciador de sistema do ONTAP > Adicionar nível de nuvem

Como obtenho esses valores?

Dependendo de seus requisitos, você pode fazer um dos seguintes procedimentos para obter as informações de que precisa:

- Utilize a "Assistente de configuração do FabricPool". O assistente de configuração do FabricPool ajuda você a configurar rapidamente os valores necessários no StorageGRID e envia um arquivo que você pode usar para configurar o Gerenciador de sistema do ONTAP. O assistente orienta você pelas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID e do FabricPool.
- Configure cada item manualmente. Em seguida, insira os valores no Gerenciador de sistema do ONTAP ou na CLI do ONTAP. Siga estes passos:
  a. "Configurar um grupo de alta disponibilidade (HA) para o FabricPool".
  b. "Crie um ponto de extremidade do balanceador de carga para o FabricPool".
  c. "Crie uma conta de locatário para o FabricPool".

d. Faça login na conta do locatário e "crie o bucket e as chaves de acesso para o usuário raiz".

e. Crie uma regra ILM para dados do FabricPool e adicione-a às suas políticas ILM ativas. "Configure o ILM para dados do FabricPool"Consulte .

f. Opcionalmente"Crie uma política de classificação de tráfego para o FabricPool", .

Use o assistente de configuração do FabricPool

Use o assistente de configuração do FabricPool: Considerações e requisitos

Você pode usar o assistente de configuração do FabricPool para configurar o StorageGRID como o sistema de storage de objetos para uma camada de nuvem do FabricPool. Depois de concluir o assistente de configuração, você pode inserir os detalhes necessários no Gerenciador de sistema do ONTAP.

Quando utilizar o assistente de configuração do FabricPool

O assistente de configuração do FabricPool orienta você em cada etapa da configuração do StorageGRID para uso com o FabricPool e configura automaticamente determinadas entidades para você, como o ILM e as políticas de classificação de tráfego. Como parte da conclusão do assistente, você baixa um arquivo que pode ser usado para inserir valores no Gerenciador de sistemas do ONTAP. Use o assistente para configurar o sistema mais rapidamente e para garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID e do FabricPool.

Supondo que você tenha permissão de acesso root, você pode concluir o assistente de configuração do FabricPool quando começar a usar o Gerenciador de Grade do StorageGRID, ou você pode acessar e concluir o assistente a qualquer momento posterior. Dependendo de seus requisitos, você também pode configurar alguns ou todos os itens necessários manualmente e, em seguida, usar o assistente para montar os valores que o ONTAP precisa em um único arquivo.

Use o assistente de configuração do FabricPool, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá uma personalização significativa.

Antes de utilizar o assistente

Confirme que concluiu estes passos de pré-requisito.

Reveja as práticas recomendadas

- Você tem uma compreensão geral do "Informações necessárias para anexar o StorageGRID como uma categoria de nuvem".
- Você analisou as práticas recomendadas da FabricPool para:
  - "Grupos de alta disponibilidade (HA)"
  - "Balanceamento de carga"
  - "Regras e política do ILM"

Obtenha endereços IP e configure interfaces VLAN

Se você configurar um grupo de HA, saberá a quais nós o ONTAP se conetará e a qual rede StorageGRID será usada. Você também sabe quais valores inserir para o CIDR de sub-rede, endereço IP de gateway e endereços IP virtual (VIP).

Se você planeja usar uma LAN virtual para segregar o tráfego FabricPool, já configurou a interface VLAN. "Configurar interfaces VLAN"Consulte .

Configure a federação de identidade e o SSO

Se você planeja usar federação de identidade ou logon único (SSO) para seu sistema StorageGRID, ativou esses recursos. Você também sabe qual grupo federado deve ter acesso root para a conta de locatário que o ONTAP usará. "Use a federação de identidade"Consulte e "Configurar o logon único".

Obter e configurar nomes de domínio

- Você sabe qual nome de domínio totalmente qualificado (FQDN) usar para o StorageGRID. As entradas do servidor de nomes de domínio (DNS) mapearão esse FQDN para os endereços IP virtuais (VIP) do grupo HA criado usando o assistente. "Configure o servidor DNS"Consulte .
- Se você planeja usar S3 solicitações virtuais de estilo hospedado, você tem "Configurados S3 nomes de domínio de endpoint"o . O ONTAP usa URLs de estilo caminho por padrão, mas o uso de solicitações virtuais de estilo hospedado é recomendado.

Revise os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga do StorageGRID, revisou o "considerações para balanceamento de carga"geral . Você tem os certificados que você vai carregar ou os valores que você precisa para gerar um certificado.

Se você planeja usar um endpoint de balanceador de carga externo (de terceiros), terá o nome de domínio totalmente qualificado (FQDN), a porta e o certificado para esse balanceador de carga.

Confirme a configuração do conjunto de armazenamento ILM

Se você instalou inicialmente o StorageGRID 11,6 ou anterior, configurou o pool de armazenamento que usará. Em geral, você deve criar um pool de armazenamento para cada site do StorageGRID que você usará para armazenar dados do ONTAP.

> Este pré-requisito não se aplica se você instalou inicialmente o StorageGRID 11,7 ou 11,8. Quando você instala inicialmente uma dessas versões, os pools de armazenamento são criados automaticamente para cada site.

Relação entre a ONTAP e a camada de nuvem da StorageGRID

O assistente do FabricPool orienta você pelo processo de criação de uma única camada de nuvem do StorageGRID que inclui um locatário do StorageGRID, um conjunto de chaves de acesso e um bucket do StorageGRID. É possível anexar essa categoria de nuvem do StorageGRID a uma ou mais categorias locais do ONTAP.

A prática recomendada geral é anexar uma única camada de nuvem a vários níveis locais em um cluster. No entanto, dependendo dos seus requisitos, você pode usar mais de um bucket ou até mais de um locatário do StorageGRID para as camadas locais em um único cluster. O uso de buckets e locatários diferentes permite isolar dados e acesso a dados entre as camadas locais do ONTAP, mas é um pouco mais complexo de configurar e gerenciar.

O NetApp não recomenda anexar uma única camada de nuvem a camadas locais em vários clusters.

Para obter as melhores práticas para usar o StorageGRID com o NetApp MetroCluster e o FabricPool Mirror, "TR-4598: Melhores práticas da FabricPool em ONTAP" consulte .

Opcional: Use um balde diferente para cada nível local

Para usar mais de um bucket nas categorias locais em um cluster do ONTAP, adicione mais de uma categoria de nuvem do StorageGRID no ONTAP. Cada camada de nuvem compartilha o mesmo grupo de HA, o ponto de extremidade do balanceador de carga, o locatário e as chaves de acesso, mas usa um contêiner diferente (bucket do StorageGRID). Siga estes passos gerais:

1. No Gerenciador de Grade do StorageGRID, conclua o assistente de configuração do FabricPool para o primeiro nível de nuvem.
2. No Gerenciador de sistemas do ONTAP, adicione uma camada de nuvem e use o arquivo baixado do StorageGRID para fornecer os valores necessários.
3. A partir do Gerenciador do Locatário do StorageGRID, faça login no locatário que foi criado pelo assistente e crie um segundo bucket.
4. Conclua o assistente FabricPool novamente. Selecione o grupo de HA existente, o ponto de extremidade do balanceador de carga e o locatário. Em seguida, selecione o novo intervalo criado manualmente. Crie uma nova regra ILM para o novo bucket e ative uma política ILM para incluir essa regra.
5. Da ONTAP, adicione uma segunda camada de nuvem, mas forneça o novo nome do bucket.

Opcional: Use um locatário e bucket diferentes para cada nível local

Para usar mais de um locatário e conjuntos diferentes de chaves de acesso para os níveis locais em um cluster do ONTAP, adicione mais de uma camada de nuvem do StorageGRID no ONTAP. Cada camada de nuvem compartilha o mesmo ponto de extremidade do balanceador de carga e grupo de HA, mas usa um locatário, chaves de acesso e contêiner diferentes (bucket do StorageGRID). Siga estes passos gerais:

1. No Gerenciador de Grade do StorageGRID, conclua o assistente de configuração do FabricPool para o primeiro nível de nuvem.
2. No Gerenciador de sistemas do ONTAP, adicione uma camada de nuvem e use o arquivo baixado do StorageGRID para fornecer os valores necessários.
3. Conclua o assistente FabricPool novamente. Selecione o grupo de HA existente e o ponto de extremidade do balanceador de carga. Crie um novo locatário e bucket. Crie uma nova regra ILM para o novo bucket e ative uma política ILM para incluir essa regra.
4. No ONTAP, adicione uma segunda camada de nuvem, mas forneça a nova chave de acesso, a chave secreta e o nome do bucket.

Acesse e conclua o assistente de configuração do FabricPool

Você pode usar o assistente de configuração do FabricPool para configurar o StorageGRID como o sistema de storage de objetos para uma camada de nuvem do FabricPool.

Antes de começar

- Analisou "considerações e requisitos"o para utilizar o assistente de configuração do FabricPool.

Se você quiser configurar o StorageGRID para uso com qualquer outro aplicativo cliente S3, vá para "Utilize o assistente de configuração S3".

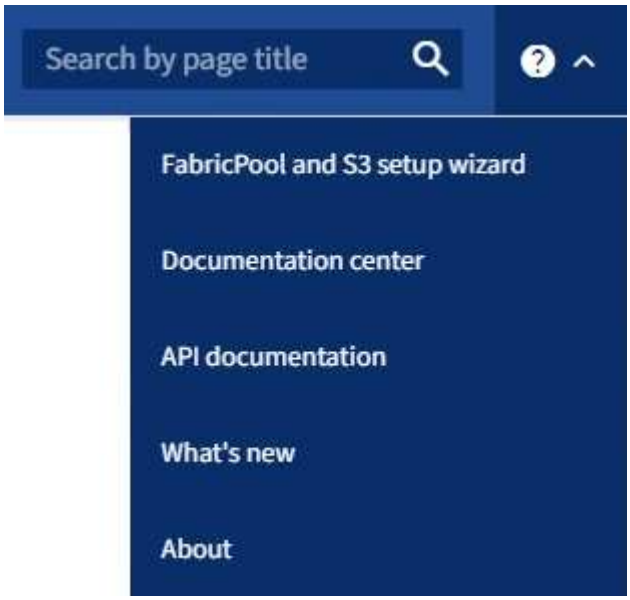
- Você tem o "Permissão de acesso à raiz".

Acesse o assistente

Você pode concluir o assistente de configuração do FabricPool quando começar a usar o Gerenciador de Grade do StorageGRID, ou você pode acessar e concluir o assistente a qualquer momento posterior.

Passos

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Se o banner **FabricPool and S3 setup wizard** for exibido no painel, selecione o link no banner. Se o banner não for mais exibido, selecione o ícone de ajuda na barra de cabeçalho no Gerenciador de Grade e selecione **Assistente de configuração FabricPool e S3**.



3. Na seção FabricPool da página do assistente de configuração FabricPool e S3, selecione **Configurar agora**.

   Etapa 1 de 9: Configurar grupo HA é exibido.

Etapa 1 de 9: Configurar o grupo HA

Um grupo de alta disponibilidade (HA) é uma coleção de nós que contêm cada um o serviço de balanceador de carga do StorageGRID. Um grupo de HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo de HA para ajudar a manter as conexões de dados do FabricPool disponíveis. Um grupo de HA usa endereços IP virtuais (VIPs) para fornecer acesso altamente disponível ao serviço Load Balancer. Se a interface ativa no grupo de HA falhar, uma interface de backup poderá gerenciar o workload com pouco impacto nas operações do FabricPool

Para obter detalhes sobre esta tarefa, "Gerenciar grupos de alta disponibilidade" consulte e "Práticas recomendadas para grupos de alta disponibilidade".

Passos

1. Se você pretende usar um balanceador de carga externo, não precisa criar um grupo de HA. Selecione **Ignorar este passo** e vá para Etapa 2 de 9: Configurar o ponto final do balanceador de carga.
2. Para usar o balanceador de carga do StorageGRID, crie um novo grupo de HA ou use um grupo de HA

existente.

Criar grupo HA

a. Para criar um novo grupo HA, selecione **criar grupo HA**.

b. Para a etapa **Digite detalhes**, preencha os campos a seguir.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

c. Para a etapa **Adicionar interfaces**, selecione as interfaces de nó que deseja usar neste grupo HA.

Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

d. Para a etapa **priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para esse grupo de HA.

Arraste linhas para alterar os valores na coluna **Priority Order**.

A primeira interface na lista é a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.

Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços IP virtual (VIP) serão movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup, e assim por diante. Quando as falhas são resolvidas, os endereços VIP voltam para a interface de maior prioridade disponível.

e. Para a etapa **Inserir endereços IP**, preencha os campos a seguir.

Campo	Descrição
CIDR de sub-rede	O endereço da sub-rede VIP na notação CIDR& n.o 8212;um endereço IPv4 seguido de uma barra e o comprimento da sub-rede (0-32). O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.
Endereço IP do gateway (opcional)	Opcional. Se os endereços IP do ONTAP usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do StorageGRID VIP. O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Introduza pelo menos um e não mais de dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP e todos estarão ativos ao mesmo tempo na interface ativa. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

f. Selecione **Create HA group** e, em seguida, selecione **Finish** para retornar ao assistente de configuração do FabricPool.

g. Selecione **continuar** para ir para a etapa do balanceador de carga.

Use o grupo HA existente

a. Para usar um grupo HA existente, selecione o nome do grupo HA na lista suspensa **Selecione um grupo HA**.

b. Selecione **continuar** para ir para a etapa do balanceador de carga.

Etapa 2 de 9: Configurar o ponto final do balanceador de carga

O StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos clientes, como o FabricPool. O balanceamento de carga maximiza a velocidade e a capacidade de conexão em vários nós de storage.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós de gateway e administrador, ou pode se conetar a um balanceador de carga externo (de terceiros). Recomenda-se a utilização do balanceador de carga StorageGRID.

Para obter detalhes sobre esta tarefa, consulte o "considerações para balanceamento de carga"geral e o "Práticas recomendadas para balanceamento de carga para FabricPool".

Passos

1. Selecione ou crie um ponto de extremidade do balanceador de carga StorageGRID ou use um balanceador de carga externo.

Criar endpoint

a. Selecione **criar endpoint**.

b. Para a etapa **Digite os detalhes do endpoint**, preencha os campos a seguir.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo é padrão para 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada. Se você inserir 80 ou 443, o endpoint será configurado apenas em nós de Gateway, porque essas portas serão reservadas em nós de administração. **Observação:** as portas usadas por outros serviços de grade não são permitidas. Consulte "Referência da porta de rede".
Tipo de cliente	Deve ser **S3**.
Protocolo de rede	Selecione **HTTPS**. **Nota**: A comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

c. Para a etapa **Select Binding mode** (Selecionar modo de encadernação), especifique o modo de encadernação. O modo de vinculação controla como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP específicos e interfaces de rede.

Modo	Descrição
Global (predefinição)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global** (padrão), a menos que você precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos de HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo de HA para acessar esse endpoint. Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nós	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar esse endpoint.

Modo	Descrição
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway para acessar esse ponto final.

d. Para a etapa **Acesso ao locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de inquilino podem usar esse endpoint para acessar seus buckets. **Permitir todos os inquilinos** é quase sempre a opção apropriada para o ponto de extremidade do balanceador de carga usado para o FabricPool. Você deve selecionar essa opção se estiver usando o assistente de configuração do FabricPool para um novo sistema StorageGRID e ainda não tiver criado nenhuma conta de locatário.
Permitir inquilinos selecionados	Somente as contas de locatário selecionadas podem usar esse endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar esse endpoint para acessar seus buckets. Todos os outros inquilinos podem usar este endpoint.

e. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use essa opção para carregar um certificado de servidor assinado pela CA, uma chave privada de certificado e um pacote de CA opcional.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Consulte "Configurar pontos de extremidade do balanceador de carga" para obter detalhes sobre o que introduzir.
Use o certificado StorageGRID S3	Esta opção só está disponível se você já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID. "Configure os certificados API do S3"Consulte para obter detalhes.

f. Selecione **Finish** para retornar ao assistente de configuração do FabricPool.

g. Selecione **Continue** para ir para a etapa de locatário e bucket.

As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Use o ponto de extremidade do balanceador de carga existente

a. Selecione o nome de um endpoint existente na lista suspensa **Selecione um endpoint do balanceador de carga**.

b. Selecione **Continue** para ir para a etapa de locatário e bucket.

Use balanceador de carga externo

a. Preencha os campos a seguir para o balanceador de carga externo.

Campo	Descrição
FQDN	O nome de domínio totalmente qualificado (FQDN) do balanceador de carga externo.
Porta	O número da porta que o FabricPool usará para conetar ao balanceador de carga externo.
Certificado	Copie o certificado do servidor para o balanceador de carga externo e cole-o neste campo.

b. Selecione **Continue** para ir para a etapa de locatário e bucket.

Passo 3 de 9: Locatário e balde

Um locatário é uma entidade que pode usar aplicativos S3 para armazenar e recuperar objetos no StorageGRID. Cada locatário tem seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos. Você deve criar um locatário do StorageGRID antes de criar o bucket que o FabricPool usará.

Um bucket é um contentor usado para armazenar os objetos e metadados de objetos de um locatário. Embora alguns locatários possam ter muitos buckets, o assistente permite criar ou selecionar apenas um locatário e um bucket de cada vez. Você pode usar o Gerenciador do Locatário posteriormente para adicionar quaisquer buckets adicionais que você precisar.

Você pode criar um novo locatário e bucket para uso no FabricPool ou selecionar um locatário e bucket existentes. Se você criar um novo locatário, o sistema criará automaticamente o ID da chave de acesso e a chave de acesso secreta para o usuário raiz do locatário.

Para obter detalhes sobre esta tarefa, "Crie uma conta de locatário para o FabricPool" consulte e "Crie um bucket do S3 e obtenha uma chave de acesso".

Passos

Crie um novo locatário e bucket ou selecione um locatário existente.

Novo locatário e balde

1. Para criar um novo locatário e intervalo, insira um **Nome do locatário**. Por exemplo, `FabricPool tenant`.
2. Defina o acesso root para a conta de locatário, com base se o sistema StorageGRID usa "federação de identidade", "Logon único (SSO)"ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver ativada	Especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade estiver ativada	a. Selecione um grupo federado existente para ter permissão de acesso root para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso root para o locatário. Nenhum usuário local pode entrar.

3. Para **Nome do balde**, introduza o nome do bucket que o FabricPool utilizará para armazenar dados do ONTAP. Por exemplo, `fabricpool-bucket`.

   Não é possível alterar o nome do bucket depois de criar o bucket.

4. Selecione a **região** para este intervalo.

   Use a região (`us-east-1`padrão) a menos que você espere usar o ILM no futuro para filtrar objetos com base na região do bucket.

5. Selecione **criar e continuar** para criar o locatário e o bucket e ir para a etapa de download de dados

Selecione locatário e intervalo

A conta de locatário existente deve ter pelo menos um bucket que não tenha o controle de versão habilitado. Não é possível selecionar uma conta de locatário existente se nenhum intervalo existir para esse locatário.

1. Selecione o locatário existente na lista suspensa **Nome do locatário**.
2. Selecione o intervalo existente na lista suspensa **Nome do balde**.

   O FabricPool não oferece suporte ao controle de versão de objetos, portanto, os buckets que têm controle de versão habilitado não são exibidos.

   Não selecione um bucket que tenha o bloqueio de objeto S3 ativado para uso com o FabricPool.

3. Selecione **continuar** para ir para a etapa de download de dados.

Passo 4 de 9: Baixe as configurações do ONTAP

Durante esta etapa, você faz o download de um arquivo que pode ser usado para inserir valores no Gerenciador do sistema do ONTAP.

Passos

1. Opcionalmente, selecione o ícone de cópia ( ) para copiar o ID da chave de acesso e a chave de acesso secreta para a área de transferência.

   Esses valores estão incluídos no arquivo de download, mas você pode querer salvá-los separadamente.

2. Selecione **Download ONTAP settings** para baixar um arquivo de texto que contém os valores inseridos até o momento.

   ```
   `ONTAP_FabricPool_settings___bucketname__.txt`O arquivo inclui as informações de que você precisa para configurar o StorageGRID como o sistema de storage de objetos para uma categoria de nuvem do FabricPool, incluindo:
   ```

   - Detalhes da conexão do balanceador de carga, incluindo o nome do servidor (FQDN), a porta e o certificado
   - Nome do intervalo
   - ID da chave de acesso e chave de acesso secreta para o usuário raiz da conta de locatário

3. Salve as chaves copiadas e o arquivo baixado em um local seguro.

   Não feche esta página até que você tenha copiado ambas as chaves de acesso, baixado as configurações do ONTAP ou ambas. As chaves não estarão disponíveis depois de fechar esta página. Certifique-se de salvar essas informações em um local seguro, pois elas podem ser usadas para obter dados do seu sistema StorageGRID.

4. Marque a caixa de seleção para confirmar que você baixou ou copiou o ID da chave de acesso e a chave de acesso secreta.
5. Selecione **Continue** para ir para a etapa do conjunto de armazenamento ILM.

Passo 5 de 9: Selecione um pool de armazenamento

Um pool de storage é um grupo de nós de storage. Ao selecionar um pool de storage, você determina quais nós o StorageGRID usará para armazenar os dados dispostos em camadas no ONTAP.

Para obter detalhes sobre esta etapa, "Crie um pool de armazenamento"consulte .

Passos

1. Na lista suspensa **Site**, selecione o site StorageGRID que deseja usar para os dados dispostos no ONTAP.
2. Na lista suspensa **Storage pool**, selecione o pool de armazenamento para esse site.

   O pool de storage de um local inclui todos os nós de storage nesse local.

3. Selecione **Continue** para ir para a etapa de regra ILM.

Passo 6 de 9: Revise a regra ILM para FabricPool

As regras de gerenciamento do ciclo de vida das informações (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos em seu sistema StorageGRID.

O assistente de configuração do FabricPool cria automaticamente a regra de ILM recomendada para uso no FabricPool. Esta regra aplica-se apenas ao intervalo especificado. Ele usa codificação de apagamento 2-1 em um único local para armazenar os dados dispostos em camadas do ONTAP.

Para obter detalhes sobre esta etapa, "Criar regra ILM"consulte e "Práticas recomendadas para usar o ILM com dados do FabricPool".

Passos

1. Reveja os detalhes da regra.

Campo	Descrição
Nome da regra	Gerado automaticamente e não pode ser alterado
Descrição	Gerado automaticamente e não pode ser alterado
Filtro	O nome do intervalo Esta regra só se aplica a objetos salvos no intervalo especificado.
Tempo de referência	Tempo de ingestão A instrução de colocação começa quando os objetos são inicialmente guardados no balde.
Instrução de colocação	Use a codificação de apagamento 2-1

2. Classifique o diagrama de retenção por **período de tempo** e **conjunto de armazenamento** para confirmar a instrução de colocação.
   - O **período de tempo** para a regra é **dia 0 - para sempre**. **Dia 0** significa que a regra é aplicada quando os dados são dispostos em camadas do ONTAP. **Forever** significa que o StorageGRID ILM não excluirá os dados que foram dispostos em camadas do ONTAP.
   - O **pool de armazenamento** da regra é o pool de armazenamento selecionado. **EC 2-1** significa que os dados serão armazenados usando codificação de apagamento 2-1. Cada objeto será salvo como dois fragmentos de dados e um fragmento de paridade. Os três fragmentos de cada objeto serão salvos em nós de storage diferentes em um único local.
3. Selecione **criar e continuar** para criar esta regra e ir para a etapa de política ILM.

Passo 7 de 9: Revise e ative a política ILM

Depois que o assistente de configuração do FabricPool criar a regra ILM para uso do FabricPool, ele cria uma política ILM. Você deve simular e revisar cuidadosamente esta política antes de ativá-la.

Para obter detalhes sobre esta etapa, "Criar política ILM"consulte e "Práticas recomendadas para usar o ILM com dados do FabricPool".

Quando você ativa uma nova política de ILM, o StorageGRID usa essa política para gerenciar o posicionamento, a duração e a proteção de dados de todos os objetos na grade, incluindo objetos existentes e objetos recém-ingeridos. Em alguns casos, ativar uma nova política pode fazer com que objetos existentes sejam movidos para novos locais.

Para evitar a perda de dados, não use uma regra de ILM que expirará ou excluirá os dados da camada de nuvem do FabricPool. Defina o período de retenção como **Forever** para garantir que os objetos FabricPool não sejam excluídos pelo StorageGRID ILM.

Passos

1. Opcionalmente, atualize o **Nome da política** gerado pelo sistema. Por padrão, o sistema adiciona " FabricPool" ao nome da política ativa ou inativa, mas você pode fornecer seu próprio nome.
2. Reveja a lista de regras na política inativa.
   - Se sua grade não tiver uma política ILM inativa, o assistente criará uma política inativa clonando sua política ativa e adicionando a nova regra à parte superior.
   - Se sua grade já tiver uma política ILM inativa e essa política usar as mesmas regras e a mesma ordem que a política ILM ativa, o assistente adicionará a nova regra à parte superior da política inativa.
   - Se a política inativa contiver regras diferentes ou uma ordem diferente da política ativa, o assistente criará uma nova política inativa clonando a política ativa e adicionando a nova regra à parte superior.
3. Reveja a ordem das regras na nova política inativa.

   Como a regra FabricPool é a primeira regra, todos os objetos no bucket do FabricPool são colocados antes que as outras regras da política sejam avaliadas. Objetos em qualquer outro buckets são colocados por regras subsequentes na política.

4. Revise o diagrama de retenção para saber como objetos diferentes serão retidos.
   a. Selecione **expandir tudo** para ver um diagrama de retenção para cada regra na política inativa.
   b. Selecione **período de tempo** e **conjunto de armazenamento** para rever o diagrama de retenção. Confirme se todas as regras que se aplicam ao bucket do FabricPool ou ao locatário retêm objetos **Forever**.
5. Quando tiver revisto a política inativa, selecione **Ativar e continuar** para ativar a política e vá para a etapa de classificação de tráfego.

Erros em uma política de ILM podem causar perda de dados irreparável. Reveja cuidadosamente a política antes de ativar.

Passo 8 de 9: Criar política de classificação de tráfego

Como opção, o assistente de configuração do FabricPool pode criar uma política de classificação de tráfego que você pode usar para monitorar a carga de trabalho do FabricPool. A política criada pelo sistema usa uma regra correspondente para identificar todo o tráfego de rede relacionado ao intervalo que você criou. Esta política monitoriza apenas o tráfego; não limita o tráfego para FabricPool ou quaisquer outros clientes.

Para obter detalhes sobre esta etapa, "Crie uma política de classificação de tráfego para o FabricPool"consulte .

Passos

1. Reveja a política.

2. Se pretender criar esta política de classificação de tráfego, selecione **criar e continuar**.

   Assim que o FabricPool começar a separar dados em categorias para o StorageGRID, você pode ir para a página políticas de classificação de tráfego para exibir as métricas de tráfego de rede para essa política. Posteriormente, você também pode adicionar regras para limitar outros workloads e garantir que o workload do FabricPool tenha a maior parte da largura de banda.

3. Caso contrário, selecione **Skip this step**.

Passo 9 de 9: Rever resumo

O resumo fornece detalhes sobre os itens configurados, incluindo o nome do balanceador de carga, locatário e bucket, a política de classificação de tráfego e a política ILM ativa,

Passos

1. Reveja o resumo.
2. Selecione **Finish**.

Próximas etapas

Depois de concluir o assistente FabricPool, execute estas etapas adicionais.

Passos

1. Aceda a "Configure o Gerenciador do sistema ONTAP" para introduzir os valores guardados e para concluir o lado ONTAP da ligação. Você deve adicionar o StorageGRID como uma categoria de nuvem, anexar a categoria de nuvem a uma categoria local para criar um FabricPool e definir políticas de disposição em categorias de volume.
2. Aceda a "Configure o servidor DNS" e certifique-se de que o DNS inclui um registo para associar o nome do servidor StorageGRID (nome de domínio totalmente qualificado) a cada endereço IP StorageGRID que irá utilizar.
3. "Outras práticas recomendadas para StorageGRID e FabricPool"Acesse para conhecer as práticas recomendadas para logs de auditoria do StorageGRID e outras opções de configuração global.

Configure o StorageGRID manualmente

Criar um grupo de alta disponibilidade (HA) para o FabricPool

Ao configurar o StorageGRID para uso com o FabricPool, você pode, opcionalmente, criar um ou mais grupos de alta disponibilidade (HA). Um grupo de HA é uma coleção de nós que contêm cada um o serviço StorageGRID Load Balancer. Um grupo de HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo de HA para ajudar a manter as conexões de dados do FabricPool disponíveis. Um grupo de HA usa endereços IP virtuais (VIPs) para fornecer acesso altamente disponível ao serviço Load Balancer. Se a interface ativa no grupo de HA falhar, uma interface de backup poderá gerenciar o workload com pouco impacto nas operações do FabricPool.

Para obter detalhes sobre esta tarefa, "Gerenciar grupos de alta disponibilidade"consulte . Para usar o assistente de configuração do FabricPool para concluir esta tarefa, vá para "Acesse e conclua o assistente de configuração do FabricPool".

Antes de começar

- Você revisou o "práticas recomendadas para grupos de alta disponibilidade".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Se você planeja usar uma VLAN, criou a interface VLAN. "Configurar interfaces VLAN"Consulte .

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selecione **criar**.
3. Para a etapa **Digite detalhes**, preencha os campos a seguir.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

4. Para a etapa **Adicionar interfaces**, selecione as interfaces de nó que deseja usar neste grupo HA.

   Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

   Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

5. Para a etapa **priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para esse grupo de HA.

   Arraste linhas para alterar os valores na coluna **Priority Order**.

   A primeira interface na lista é a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.

   Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços IP virtual (VIP) serão movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup, e assim por diante. Quando as falhas são resolvidas, os endereços VIP voltam para a interface de maior prioridade disponível.

6. Para a etapa **Inserir endereços IP**, preencha os campos a seguir.

Campo	Descrição
CIDR de sub-rede	O endereço da sub-rede VIP na notação CIDR& n.o 8212;um endereço IPv4 seguido de uma barra e o comprimento da sub-rede (0-32). O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.

Campo	Descrição
Endereço IP do gateway (opcional)	Opcional. Se os endereços IP do ONTAP usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do StorageGRID VIP. O endereço IP do gateway local deve estar dentro da sub-rede VIP.
Endereço IP virtual	Introduza pelo menos um e não mais de dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

7. Selecione **Create HA group** e, em seguida, selecione **Finish**.

Crie um ponto de extremidade do balanceador de carga para o FabricPool

O StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos clientes, como o FabricPool. O balanceamento de carga maximiza a velocidade e a capacidade de conexão em vários nós de storage.

Ao configurar o StorageGRID para uso com o FabricPool, você deve configurar um ponto de extremidade do balanceador de carga e fazer upload ou gerar um certificado de ponto de extremidade do balanceador de carga, que é usado para proteger a conexão entre o ONTAP e o StorageGRID.

Para usar o assistente de configuração do FabricPool para concluir esta tarefa, vá para "Acesse e conclua o assistente de configuração do FabricPool".

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Você revisou o geral"considerações para balanceamento de carga", bem como o "Práticas recomendadas para balanceamento de carga para FabricPool".

Passos

1. Selecione **CONFIGURATION** > **Network** > **Load balancer endpoints**.
2. Selecione **criar**.
3. Para a etapa **Digite os detalhes do endpoint**, preencha os campos a seguir.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.

Campo	Descrição
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo é padrão para 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada. Se você digitar 80 ou 443, o endpoint será configurado somente em nós do Gateway. Essas portas são reservadas em nós de administração. **Observação:** as portas usadas por outros serviços de grade não são permitidas. Consulte "Referência da porta de rede". Você fornecerá esse número ao ONTAP ao anexar o StorageGRID como uma categoria de nuvem do FabricPool.
Tipo de cliente	Selecione **S3**.
Protocolo de rede	Selecione **HTTPS**. **Nota**: A comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

4. Para a etapa **Select Binding mode** (Selecionar modo de encadernação), especifique o modo de encadernação. O modo de vinculação controla como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP específicos e interfaces de rede.

Modo	Descrição
Global (predefinição)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global** (padrão), a menos que você precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos de HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo de HA para acessar esse endpoint. Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nós	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar esse endpoint.
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway para acessar esse ponto final.

5. Para a etapa **Acesso ao locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de inquilino podem usar esse endpoint para acessar seus buckets. **Permitir todos os inquilinos** é quase sempre a opção apropriada para o ponto de extremidade do balanceador de carga usado para o FabricPool. Você deve selecionar essa opção se ainda não tiver criado nenhuma conta de locatário.
Permitir inquilinos selecionados	Somente as contas de locatário selecionadas podem usar esse endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar esse endpoint para acessar seus buckets. Todos os outros inquilinos podem usar este endpoint.

6. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use essa opção para carregar um certificado de servidor assinado pela CA, uma chave privada de certificado e um pacote de CA opcional.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Consulte "Configurar pontos de extremidade do balanceador de carga" para obter detalhes sobre o que introduzir.
Use o certificado StorageGRID S3	Esta opção só está disponível se você já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID. "Configure os certificados API do S3"Consulte para obter detalhes.

7. Selecione **criar**.

> As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Crie uma conta de locatário para o FabricPool

Você deve criar uma conta de locatário no Gerenciador de Grade para uso do FabricPool.

As contas de inquilino permitem que aplicativos clientes armazenem e recuperem objetos no StorageGRID. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários autorizados, buckets e objetos.

Para obter detalhes sobre esta tarefa, "Crie uma conta de locatário"consulte . Para usar o assistente de configuração do FabricPool para concluir esta tarefa, vá para "Acesse e conclua o assistente de configuração

do FabricPool".

Antes de começar

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

Passos

1. Selecione **TENANTS**.
2. Selecione **criar**.
3. Para os passos Enter details (introduzir detalhes), introduza as seguintes informações.

Campo	Descrição
Nome	Um nome para a conta de locatário. Os nomes de inquilinos não precisam ser únicos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.
Descrição (opcional)	Uma descrição para ajudar a identificar o inquilino.
Tipo de cliente	Deve ser **S3** para FabricPool.
Cota de armazenamento (opcional)	Deixe este campo em branco para FabricPool.

4. Para a etapa Selecionar permissões:
   a. Não selecione **permitir serviços de plataforma**.

      Os locatários do FabricPool geralmente não precisam usar serviços de plataforma, como a replicação do CloudMirror.

   b. Opcionalmente, selecione **Use own Identity source**.
   c. Não selecione **permitir S3 Select**.

      Os inquilinos do FabricPool normalmente não precisam usar o S3 Select.

   d. Opcionalmente, selecione **usar conexão de federação de grade** para permitir que o locatário use um "conexão de federação de grade" para clone de conta e replicação entre grade. Em seguida, selecione a conexão de federação de grade a ser usada.
5. Para a etapa Definir acesso raiz, especifique qual usuário terá a permissão de acesso raiz inicial para a conta de locatário, com base no uso do sistema StorageGRID "federação de identidade" "Logon único (SSO)", ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver ativada	Especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.

Opção	Faça isso
Se a federação de identidade estiver ativada	a. Selecione um grupo federado existente para ter permissão de acesso root para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso root para o locatário. Nenhum usuário local pode entrar.

6. Selecione **criar inquilino**.

Crie um bucket do S3 e obtenha chaves de acesso

Antes de usar o StorageGRID com um workload do FabricPool, você precisa criar um bucket do S3 para seus dados do FabricPool. Você também precisa obter uma chave de acesso e uma chave de acesso secreta para a conta de locatário que você usará para o FabricPool.

Para obter detalhes sobre esta tarefa, "Crie um balde S3D." consulte e "Crie suas próprias chaves de acesso S3". Para usar o assistente de configuração do FabricPool para concluir esta tarefa, vá para "Acesse e conclua o assistente de configuração do FabricPool".

Antes de começar

- Você criou uma conta de locatário para uso do FabricPool.
- Você tem acesso root à conta de locatário.

Passos

1. Inicie sessão no Gestor do Locatário.

   Você pode fazer um dos seguintes procedimentos:

   - Na página Contas do Locatário no Gerenciador de Grade, selecione o link **entrar** para o locatário e insira suas credenciais.
   - Insira o URL da conta de locatário em um navegador da Web e insira suas credenciais.

2. Crie um bucket do S3 para dados do FabricPool.

   É necessário criar um bucket exclusivo para cada cluster do ONTAP que você planeja usar.

   a. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
   b. Selecione **criar bucket**.
   c. Introduza o nome do bucket do StorageGRID que pretende utilizar com o FabricPool. Por exemplo, `fabricpool-bucket`.

      Não é possível alterar o nome do bucket depois de criar o bucket.

   d. Selecione a região para este intervalo.

Por padrão, todos os buckets são criados na `us-east-1` região.

e. Selecione **continuar**.

f. Selecione **criar bucket**.

> Não selecione **Ativar versão de objetos** para o bucket do FabricPool. Da mesma forma, não edite um bucket do FabricPool para usar **Available** ou uma consistência não padrão. A consistência de bucket recomendada para buckets do FabricPool é **Read-after-novo-write**, que é a consistência padrão para um novo bucket.

3. Crie uma chave de acesso e uma chave de acesso secreta.

a. Selecione **ARMAZENAMENTO (S3)** > **as minhas chaves de acesso**.

b. Selecione **criar chave**.

c. Selecione **criar chave de acesso**.

d. Copie o ID da chave de acesso e a chave de acesso secreta para um local seguro ou selecione **Transferir .csv** para guardar um ficheiro de folha de cálculo que contenha a ID da chave de acesso e a chave de acesso secreta.

Você inserirá esses valores no ONTAP quando configurar o StorageGRID como um nível de nuvem do FabricPool.

> Se você gerar uma nova chave de acesso e chave de acesso secreta no StorageGRID no futuro, insira as novas chaves no ONTAP antes de excluir os valores antigos do StorageGRID. Caso contrário, o ONTAP poderá perder temporariamente o seu acesso ao StorageGRID.

Configure o ILM para dados do FabricPool

Você pode usar essa política de exemplo simples como ponto de partida para suas próprias regras e políticas ILM.

Este exemplo pressupõe que você esteja projetando as regras de ILM e uma política de ILM para um sistema StorageGRID que tenha quatro nós de storage em um único data center em Denver, Colorado. Os dados do FabricPool neste exemplo usam um bucket `fabricpool-bucket` chamado .

> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará da forma pretendida para proteger o conteúdo da perda. Para saber mais, "Gerenciar objetos com ILM"consulte .

> Para evitar a perda de dados, não use uma regra de ILM que expirará ou excluirá os dados da camada de nuvem do FabricPool. Defina o período de retenção como **Forever** para garantir que os objetos FabricPool não sejam excluídos pelo StorageGRID ILM.

Antes de começar

- Você revisou o "Práticas recomendadas para usar o ILM com dados do FabricPool".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

- Você tem o "Permissão de acesso ILM ou root".
- Se você atualizou para o StorageGRID 11,9 de uma versão anterior do StorageGRID, configurou o pool de armazenamento que usará. Em geral, você deve criar um pool de armazenamento para cada site do StorageGRID que você usará para armazenar dados.

> Este pré-requisito não se aplica se você instalou inicialmente o StorageGRID 11,7 ou 11,8. Quando você instala inicialmente uma dessas versões, os pools de armazenamento são criados automaticamente para cada site.

Passos

1. Crie uma regra ILM que se aplique apenas aos dados no `fabricpool-bucket`. esta regra de exemplo cria cópias codificadas por apagamento.

Definição de regra	Exemplo de valor
Nome da regra	Codificação de apagamento 2 mais 1 para dados FabricPool
Nome do intervalo	`fabricpool-bucket` Você também pode filtrar na conta de locatário do FabricPool.
Filtros avançados	Tamanho do objeto superior a 0,2 MB. **Observação:** o FabricPool só grava objetos de 4 MB, mas você deve adicionar um filtro de tamanho de objeto porque essa regra usa codificação de apagamento.
Tempo de referência	Tempo de ingestão
Período de tempo e colocações	Da loja do dia 0 para sempre Armazene objetos por codificação de apagamento usando o esquema EC 2-1 em Denver e guarde esses objetos no StorageGRID Forever. Para evitar a perda de dados, não use uma regra de ILM que expirará ou excluirá os dados da camada de nuvem do FabricPool.
Comportamento de ingestão	Equilibrado

2. Crie uma regra ILM padrão que criará duas cópias replicadas de quaisquer objetos não correlacionados com a primeira regra. Não selecione um filtro básico (conta de locatário ou nome do bucket) ou quaisquer filtros avançados.

Definição de regra	Exemplo de valor
Nome da regra	Duas cópias replicadas

Definição de regra	Exemplo de valor
Nome do intervalo	*none*
Filtros avançados	*none*
Tempo de referência	Tempo de ingestão
Período de tempo e colocações	Da loja do dia 0 para sempre Armazene objetos replicando cópias 2 em Denver.
Comportamento de ingestão	Equilibrado

3. Crie uma política ILM e selecione as duas regras. Como a regra de replicação não usa filtros, ela pode ser a regra padrão (última) para a política.
4. Ingira objetos de teste na grade.
5. Simule a política com os objetos de teste para verificar o comportamento.
6. Ative a política.

Quando esta política é ativada, o StorageGRID coloca os dados de objeto da seguinte forma:

- Os dados dispostos em camadas em FabricPool in `fabricpool-bucket` serão codificados para apagamento usando o esquema de codificação de apagamento 2-1. Dois fragmentos de dados e um fragmento de paridade serão colocados em três nós de storage diferentes.
- Todos os objetos em todos os outros buckets serão replicados. Duas cópias serão criadas e colocadas em dois nós de storage diferentes.
- As cópias serão mantidas em StorageGRID para sempre. StorageGRID ILM não excluirá esses objetos.

Crie uma política de classificação de tráfego para o FabricPool

Você pode, opcionalmente, projetar uma política de classificação de tráfego StorageGRID para otimizar a qualidade do serviço para o workload do FabricPool.

Para obter detalhes sobre esta tarefa, "Gerenciar políticas de classificação de tráfego"consulte . Para usar o assistente de configuração do FabricPool para concluir esta tarefa, vá para "Acesse e conclua o assistente de configuração do FabricPool".

Antes de começar

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

Sobre esta tarefa

As práticas recomendadas para criar uma política de classificação de tráfego para FabricPool dependem da carga de trabalho, como segue:

- Se você planeja categorizar os dados do workload primário do FabricPool para o StorageGRID, certifique-se de que o workload do FabricPool tenha a maior parte da largura de banda. Você pode criar uma política

de classificação de tráfego para limitar todas as outras cargas de trabalho.

> Em geral, as operações de leitura do FabricPool são mais importantes para priorizar do que as operações de gravação.

Por exemplo, se outros clientes S3 usarem esse sistema StorageGRID, você deve criar uma política de classificação de tráfego. Você pode limitar o tráfego de rede para outros buckets, locatários, sub-redes IP ou pontos de extremidade do balanceador de carga.

- Em geral, você não deve impor limites de qualidade de serviço a qualquer workload do FabricPool; limitar apenas os outros workloads.
- Os limites colocados em outras cargas de trabalho devem levar em conta o comportamento dessas cargas de trabalho. Os limites impostos também variam de acordo com o dimensionamento e as capacidades da sua grade e qual é a quantidade esperada de utilização.

Passos

1. Selecione **CONFIGURATION** > **Network** > **Traffic Classification**.
2. Selecione **criar**.
3. Introduza um nome e uma descrição (opcional) para a política e selecione **continuar**.
4. Para a etapa Adicionar regras de correspondência, adicione pelo menos uma regra.
   a. Selecione **Adicionar regra**
   b. Para tipo, selecione **ponto final do balanceador de carga** e selecione o ponto final do balanceador de carga criado para o FabricPool.

      Você também pode selecionar a conta de locatário ou o intervalo do FabricPool.

   c. Se você quiser que essa política de tráfego limite o tráfego para os outros endpoints, selecione **correspondência inversa**.
5. Opcionalmente, adicione um ou mais limites para controlar o tráfego de rede correspondente à regra.

   > O StorageGRID coleta métricas mesmo que você não adicione limites, para que você possa entender as tendências de tráfego.

   a. Selecione **Adicionar um limite**.
   b. Selecione o tipo de tráfego que pretende limitar e o limite a aplicar.
6. Selecione **continuar**.
7. Leia e reveja a política de classificação de tráfego. Use o botão **anterior** para voltar e fazer alterações conforme necessário. Quando estiver satisfeito com a política, selecione **Salvar e continuar**.

Depois de terminar

"Exibir métricas de tráfego de rede" para verificar se as políticas estão aplicando os limites de tráfego que você espera.

Configure o Gerenciador do sistema ONTAP

Depois de obter as informações StorageGRID necessárias, acesse o ONTAP para adicionar StorageGRID como uma categoria de nuvem.

Antes de começar

- Se tiver concluído o assistente de configuração do FabricPool, terá o `ONTAP_FabricPool_settings_bucketname.txt` ficheiro que transferiu.
- Se você configurou o StorageGRID manualmente, você tem o nome de domínio totalmente qualificado (FQDN) que está usando para StorageGRID ou o endereço IP virtual (VIP) para o grupo StorageGRID HA, o número da porta para o endpoint do balanceador de carga, o certificado do balanceador de carga, o ID da chave de acesso e a chave secreta para o usuário raiz da conta de locatário e o nome do bucket ONTAP usará nesse locatário.

Acesse o Gerenciador do sistema do ONTAP

Essas instruções descrevem como usar o Gerenciador de sistemas do ONTAP para adicionar o StorageGRID como uma camada de nuvem. Você pode concluir a mesma configuração usando a CLI do ONTAP. Para obter instruções, vá "Documentação do ONTAP para FabricPool" para .

Passos

1. Acesse o Gerenciador de sistema do cluster do ONTAP que você deseja categorizar no StorageGRID.
2. Inicie sessão como administrador do cluster.
3. Navegue até **STORAGE** > **tiers** > **Add Cloud Tier**.
4. Selecione **StorageGRID** na lista de provedores de armazenamento de objetos.

Introduza valores StorageGRID

Consulte "Documentação do ONTAP para FabricPool" para obter mais informações.

Passos

1. Preencha o formulário Adicionar nível de nuvem, usando o `ONTAP_FabricPool_settings_bucketname.txt` arquivo ou os valores obtidos manualmente.

Campo	Descrição
Nome	Insira um nome exclusivo para esse nível de nuvem. Você pode aceitar o valor padrão.
Estilo de URL	Se "Configurados S3 nomes de domínio de endpoint"você , selecione **URL Virtual Hosted-Style**. **URL de estilo de caminho** é o padrão para o ONTAP, mas o uso de solicitações virtuais de estilo hospedado é recomendado para o StorageGRID. Você deve usar **URL de estilo de caminho** se você fornecer um endereço IP em vez de um nome de domínio para o campo **Nome do servidor (FQDN)**.

Campo	Descrição
Nome do servidor (FQDN)	Insira o nome de domínio totalmente qualificado (FQDN) que você está usando para StorageGRID ou o endereço IP virtual (VIP) para o grupo HA do StorageGRID. Por exemplo, `s3.storagegrid.company.com`. Observe o seguinte: • O endereço IP ou nome de domínio que você especificar aqui deve corresponder ao certificado que você carregou ou gerou para o endpoint do balanceador de carga do StorageGRID. • Se você fornecer um nome de domínio, o Registro DNS deve mapear para cada endereço IP que você usará para se conetar ao StorageGRID. "Configure o servidor DNS"Consulte .
SSL	Activado (predefinição).
Certificado de armazenamento de objetos	Cole o PEM de certificado que você está usando para o ponto de extremidade do balanceador de carga do StorageGRID, incluindo: `-----BEGIN CERTIFICATE-----` E `-----END CERTIFICATE-----`. **Nota:** se uma CA intermediária emitiu o certificado StorageGRID, você deve fornecer o certificado CA intermediário. Se o certificado StorageGRID tiver sido emitido diretamente pela CA raiz, você deverá fornecer o certificado CA raiz.
Porta	Insira a porta usada pelo ponto de extremidade do balanceador de carga do StorageGRID. O ONTAP usará essa porta quando se conetar ao StorageGRID. Por exemplo, 10433.
Chave de acesso e chave secreta	Insira o ID da chave de acesso e a chave de acesso secreta para o usuário raiz da conta de locatário do StorageGRID. **Dica**: Se você gerar uma nova chave de acesso e chave de acesso secreta no StorageGRID no futuro, insira as novas chaves no ONTAP antes de excluir os valores antigos do StorageGRID. Caso contrário, o ONTAP poderá perder temporariamente o seu acesso ao StorageGRID.
Nome do contentor	Digite o nome do bucket do StorageGRID que você criou para uso com este nível do ONTAP.

2. Conclua a configuração final do FabricPool no ONTAP.
   a. Anexar um ou mais agregados à camada de nuvem.
   b. Como opção, crie uma política de disposição em categorias de volume.

Configure o servidor DNS

Depois de configurar grupos de alta disponibilidade, pontos de extremidade do balanceador de carga e nomes de domínio de endpoint S3, você deve garantir que o

DNS inclua as entradas necessárias para o StorageGRID. Você deve incluir uma entrada DNS para cada nome no certificado de segurança e para cada endereço IP que você possa usar.

"Considerações para balanceamento de carga"Consulte .

Entradas DNS para o nome do servidor StorageGRID

Adicione entradas de DNS para associar o nome do servidor StorageGRID (nome de domínio totalmente qualificado) a cada endereço IP do StorageGRID que você usará. Os endereços IP inseridos no DNS dependem se você está usando um grupo de HA de nós de balanceamento de carga:

- Se você tiver configurado um grupo de HA, o ONTAP se conetará aos endereços IP virtuais desse grupo de HA.
- Se você não estiver usando um grupo de HA, o ONTAP poderá se conetar ao serviço do balanceador de carga do StorageGRID usando o endereço IP de qualquer nó de gateway ou nó de administrador.
- Se o nome do servidor resolver para mais de um endereço IP, o ONTAP estabelece conexões de cliente com todos os endereços IP (até um máximo de 16 endereços IP). Os endereços IP são coletados em um método round-robin quando as conexões são estabelecidas.

Entradas DNS para solicitações virtuais de estilo hospedado

Se você definiu "S3 nomes de domínio de endpoint" e usará solicitações virtuais de estilo hospedado, adicione entradas DNS para todos os nomes de domínio de endpoint S3 necessários, incluindo nomes de curinga.

Práticas recomendadas da StorageGRID para FabricPool

Práticas recomendadas para grupos de alta disponibilidade (HA)

Antes de conectar o StorageGRID como uma categoria de nuvem do FabricPool, conheça os grupos de alta disponibilidade (HA) do StorageGRID e analise as práticas recomendadas para uso de grupos de HA com o FabricPool.

O que é um grupo HA?

Um grupo de alta disponibilidade (HA) é um conjunto de interfaces de vários nós de gateway StorageGRID, nós de administração ou ambos. Um grupo HA ajuda a manter as conexões de dados do cliente disponíveis. Se a interface ativa no grupo de HA falhar, uma interface de backup poderá gerenciar o workload com pouco impacto nas operações do FabricPool.

Cada grupo de HA fornece acesso altamente disponível aos serviços compartilhados nos nós associados. Por exemplo, um grupo de HA que consiste em interfaces somente em nós de Gateway ou em nós de Admin e nós de Gateway fornece acesso altamente disponível ao serviço de balanceador de carga compartilhado.

Para saber mais sobre grupos de alta disponibilidade, "Gerenciar grupos de alta disponibilidade (HA)"consulte .

Usando grupos de HA

As práticas recomendadas para a criação de um grupo de HA do StorageGRID para FabricPool dependem do workload.

- Se você planeja usar o FabricPool com dados de workload primário, precisa criar um grupo de HA que inclua pelo menos dois nós de balanceamento de carga para evitar a interrupção da recuperação de dados.
- Se você planeja usar a política de disposição em camadas de volume somente snapshot do FabricPool ou camadas de performance locais não principais (por exemplo, locais de recuperação de desastres ou destinos do NetApp SnapMirror), é possível configurar um grupo de HA com apenas um nó.

Essas instruções descrevem a configuração de um grupo de HA para o ative-Backup HA (um nó está ativo e um nó é backup). No entanto, você pode preferir usar DNS Round Robin ou ative-ative HA. Para saber os benefícios dessas outras configurações de HA, "Opções de configuração para grupos de HA"consulte .

Práticas recomendadas para balanceamento de carga para FabricPool

Antes de conectar o StorageGRID como uma camada de nuvem do FabricPool, verifique as práticas recomendadas para o uso de balanceadores de carga com o FabricPool.

Para obter informações gerais sobre o balanceador de carga StorageGRID e o certificado do balanceador de carga, "Considerações para balanceamento de carga"consulte .

Práticas recomendadas para o acesso do locatário ao ponto de extremidade do balanceador de carga usado para o FabricPool

Você pode controlar quais locatários podem usar um endpoint de balanceador de carga específico para acessar seus buckets. Você pode permitir todos os inquilinos, permitir alguns inquilinos ou bloquear alguns inquilinos. Ao criar um ponto de extremidade de balanceamento de carga para uso do FabricPool, selecione **permitir todos os locatários**. O ONTAP criptografa os dados que são colocados nos buckets do StorageGRID, portanto, pouca segurança adicional seria fornecida por essa camada de segurança extra.

Práticas recomendadas para o certificado de segurança

Quando você cria um ponto de extremidade do balanceador de carga do StorageGRID para uso do FabricPool, você fornece o certificado de segurança que permitirá que o ONTAP se autentique com o StorageGRID.

Na maioria dos casos, a conexão entre o ONTAP e o StorageGRID deve usar criptografia TLS (Transport Layer Security). O uso do FabricPool sem criptografia TLS é suportado, mas não é recomendado. Ao selecionar o protocolo de rede para o ponto de extremidade do balanceador de carga do StorageGRID, selecione **HTTPS**. Em seguida, forneça o certificado de segurança que permitirá que o ONTAP se autentique com o StorageGRID.

Para saber mais sobre o certificado do servidor para um endpoint de balanceamento de carga:

- "Gerenciar certificados de segurança"
- "Considerações para balanceamento de carga"
- "Diretrizes de fortalecimento para certificados de servidor"

Adicionar certificado ao ONTAP

Quando você adiciona o StorageGRID como um nível de nuvem do FabricPool, você deve instalar o mesmo certificado no cluster do ONTAP, incluindo o certificado raiz e quaisquer certificados de autoridade de certificação subordinada (CA).

Gerenciar a expiração do certificado

> Se o certificado usado para proteger a conexão entre o ONTAP e o StorageGRID expirar, o FabricPool deixará temporariamente de funcionar e o ONTAP perderá temporariamente o acesso aos dados dispostos em camadas no StorageGRID.

Para evitar problemas de expiração de certificado, siga estas práticas recomendadas:

- Monitore cuidadosamente quaisquer alertas que avisem sobre datas de expiração de certificado que estejam se aproximando, como **validade do certificado de endpoint do balanceador de carga** e **expiração do certificado de servidor global para alertas da API S3**.
- Mantenha sempre as versões StorageGRID e ONTAP do certificado em sincronia. Se você substituir ou renovar o certificado usado para um ponto de extremidade do balanceador de carga, deverá substituir ou renovar o certificado equivalente usado pelo ONTAP para a camada de nuvem.
- Use um certificado de CA assinado publicamente. Se você usar um certificado assinado por uma CA, poderá usar a API de Gerenciamento de Grade para automatizar a rotação de certificados. Isso permite que você substitua certificados que expiram em breve sem interrupções.
- Se você tiver gerado um certificado StorageGRID autoassinado e esse certificado estiver prestes a expirar, será necessário substituir manualmente o certificado no StorageGRID e no ONTAP antes que o certificado existente expire. Se um certificado autoassinado já expirou, desative a validação de certificado no ONTAP para evitar a perda de acesso.

```
https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_configure_a_new_StorageGRID_self-signed_server_certificate_on_an_existing_ONTAP_FabricPool_deployment["Base de dados de Conhecimento da NetApp: Como configurar um novo certificado de servidor auto-assinado do StorageGRID numa implementação do ONTAP FabricPool existente"^]Consulte para obter instruções.
```

Práticas recomendadas para usar o ILM com dados do FabricPool

Se você estiver usando o FabricPool para categorizar dados no StorageGRID, entenda os requisitos para usar o gerenciamento do ciclo de vida das informações (ILM) do StorageGRID com dados do FabricPool.

> A FabricPool não tem conhecimento das regras ou políticas do StorageGRID ILM. A perda de dados pode ocorrer se a política ILM do StorageGRID estiver mal configurada. Para obter informações detalhadas, "Use regras ILM para gerenciar objetos"consulte e "Criar políticas ILM".

Diretrizes para o uso de ILM com FabricPool

Quando você usa o assistente de configuração do FabricPool, o assistente cria automaticamente uma nova regra ILM para cada bucket do S3 criado e adiciona essa regra a uma política inativa. Você é solicitado a ativar a política. A regra criada automaticamente segue as práticas recomendadas: Ela usa codificação de apagamento 2-1 em um único site.

Se você estiver configurando o StorageGRID manualmente em vez de usar o assistente de configuração do FabricPool, revise essas diretrizes para garantir que suas regras de ILM e política de ILM sejam adequadas

para dados do FabricPool e seus requisitos de negócios. Talvez seja necessário criar novas regras e atualizar suas políticas ILM ativas para atender a essas diretrizes.

- Você pode usar qualquer combinação de regras de replicação e codificação de apagamento para proteger os dados de categorias de nuvem.

  A prática recomendada é usar a codificação de apagamento 2-1 em um site para proteção de dados econômica. A codificação de apagamento usa mais CPU, mas oferece significativamente menos capacidade de storage do que a replicação. Os esquemas 4-1 e 6-1 utilizam menos capacidade do que o esquema 2-1. No entanto, os esquemas 4-1 e 6-1 são menos flexíveis se você precisar adicionar nós de storage durante a expansão da grade. Para obter detalhes, "Adicionar capacidade de storage para objetos codificados por apagamento"consulte .

- Cada regra aplicada a dados do FabricPool deve usar codificação de apagamento ou criar pelo menos duas cópias replicadas.

  > 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 for "Remova os dados do FabricPool do StorageGRID"necessário , use o ONTAP para recuperar todos os dados do volume FabricPool e promovê-los para o nível de desempenho.

  > Para evitar a perda de dados, não use uma regra de ILM que expirará ou excluirá os dados da camada de nuvem do FabricPool. Defina o período de retenção em cada regra ILM como **Forever** para garantir que os objetos FabricPool não sejam excluídos pelo StorageGRID ILM.

- Não crie regras que movam os dados da camada de nuvem do FabricPool do bucket para outro local. Não é possível usar um pool de armazenamento em nuvem para mover dados do FabricPool para outro armazenamento de objetos.

  > O uso de pools de armazenamento em nuvem com FabricPool não é suportado devido à latência adicional para recuperar um objeto do destino de pool de armazenamento em nuvem.

- A partir do ONTAP 9.8, você pode, opcionalmente, criar tags de objeto para ajudar a classificar e classificar dados em camadas para facilitar o gerenciamento. Por exemplo, você pode definir tags apenas em volumes FabricPool anexados ao StorageGRID. Em seguida, quando você cria regras ILM no StorageGRID, você pode usar o filtro avançado Etiqueta de Objeto para selecionar e colocar esses dados.

Outras práticas recomendadas para StorageGRID e FabricPool

Ao configurar um sistema StorageGRID para uso com o FabricPool, talvez seja necessário alterar outras opções do StorageGRID. Antes de alterar uma configuração global, considere como a alteração afetará outras aplicações S3D.

Auditoria de mensagens e destinos de log

As cargas de trabalho do FabricPool geralmente têm uma alta taxa de operações de leitura, o que pode gerar um alto volume de mensagens de auditoria.

- Se você não precisar de um Registro de operações de leitura de cliente para o FabricPool ou qualquer outro aplicativo S3, opcionalmente vá para **CONFIGURATION** > **Monitoring** > **servidor de auditoria e syslog**. Altere a configuração **leitura do cliente** para **erro** para diminuir o número de mensagens de auditoria registradas no log de auditoria. "Configurar mensagens de auditoria e destinos de log"Consulte para obter detalhes.
- Se você tiver uma grade grande, use vários tipos de aplicativos S3 ou deseja reter todos os dados de auditoria, configure um servidor syslog externo e salve as informações de auditoria remotamente. O uso de um servidor externo minimiza o impactos no desempenho do Registro de mensagens de auditoria sem reduzir a integridade dos dados de auditoria. "Considerações para servidor syslog externo"Consulte para obter detalhes.

Criptografia de objetos

Ao configurar o StorageGRID, você pode opcionalmente ativar a "opção global para criptografia de objeto armazenado"criptografia de dados se for necessária para outros clientes StorageGRID. Os dados dispostos em camadas de FabricPool para StorageGRID já estão criptografados, portanto, a ativação da configuração StorageGRID não é necessária. As chaves de criptografia do lado do cliente são propriedade da ONTAP.

Compactação de objetos

Ao configurar o StorageGRID, não ative o "opção global para comprimir objetos armazenados". Os dados dispostos em camadas de FabricPool para StorageGRID já estão compatados. Usar a opção StorageGRID não reduzirá ainda mais o tamanho de um objeto.

Consistência do balde

Para buckets do FabricPool, a consistência de bucket recomendada é **leitura após nova gravação**, que é a consistência padrão para um novo bucket. Não edite buckets do FabricPool para usar **Available** ou **strong-site**.

Disposição em camadas do FabricPool

Se um nó do 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. Por exemplo, se um nó StorageGRID estiver sendo executado em um host VMware, verifique se o volume que faz o backup do armazenamento de dados para o nó StorageGRID 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.

Remova os dados do FabricPool do StorageGRID

Se você precisar remover os dados do FabricPool que estão armazenados no StorageGRID atualmente, use o ONTAP para recuperar todos os dados do volume FabricPool e promovê-los para o nível de desempenho.

Antes de começar

- Você revisou as instruções e considerações em "Promover dados para o nível de desempenho".
- Você está usando o ONTAP 9.8 ou posterior.

- Você está usando um "navegador da web suportado".
- Você pertence a um grupo de usuários do StorageGRID para a conta de locatário do FabricPool que tem o "Gerencie todos os buckets ou permissão de acesso root".

Sobre esta tarefa

Estas instruções explicam como mover dados do StorageGRID de volta para o FabricPool. Você executa este procedimento usando o ONTAP e o Gerenciador do Locatário do StorageGRID.

Passos

1. No ONTAP, emita o `volume modify` comando.

   Defina `tiering-policy` como `none` para interromper a nova disposição em categorias e defina `cloud-retrieval-policy` como `promote` para retornar todos os dados que foram dispostos anteriormente no StorageGRID.

   ```
   https://docs.netapp.com/us-en/ontap/fabricpool/promote-all-data-performance-tier-task.html["Promover todos os dados de um volume FabricPool para o nível de performance"^]Consulte .
   ```

2. Aguarde até que a operação seja concluída.

   Pode utilizar o `volume object-store` comando com a `tiering` opção para "verifique o status da promoção do nível de desempenho".

3. Quando a operação de promoção estiver concluída, faça login no Gerenciador do Locatário do StorageGRID para a conta de locatário do FabricPool.
4. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
5. Confirme se o balde FabricPool está vazio.
6. Se o balde estiver vazio"elimine o balde", .

Depois de terminar

Quando você exclui o bucket, a disposição em camadas do FabricPool para o StorageGRID não pode mais continuar. No entanto, como o nível local ainda está anexado ao nível de nuvem do StorageGRID, o Gerenciador de sistema do ONTAP retornará mensagens de erro indicando que o bucket está inacessível.

Para evitar essas mensagens de erro, siga um destes procedimentos:

- Use o espelhamento do FabricPool para anexar uma camada de nuvem diferente ao agregado.
- Mova os dados do agregado FabricPool para um agregado que não seja FabricPool e exclua o agregado não utilizado.

Consulte "Documentação do ONTAP para FabricPool" para obter instruções.

Use locatários e clientes do StorageGRID

Use uma conta de locatário

Use uma conta de locatário

Uma conta de locatário permite que você use a API REST do Simple Storage Service (S3) ou a API REST Swift para armazenar e recuperar objetos em um sistema StorageGRID.

O que é uma conta de locatário?

Cada conta de locatário tem seus próprios grupos federados ou locais, usuários, buckets do S3 ou contentores Swift e objetos.

As contas de inquilino podem ser usadas para segregar objetos armazenados por diferentes entidades. Por exemplo, várias contas de inquilino podem ser usadas para qualquer um desses casos de uso:

- **Caso de uso corporativo:** se o sistema StorageGRID estiver sendo usado dentro de uma empresa, o armazenamento de objetos da grade pode ser segregado pelos diferentes departamentos da organização. Por exemplo, pode haver contas de inquilino para o departamento de marketing, o departamento de suporte ao cliente, o departamento de recursos humanos e assim por diante.

  > Se você usar o protocolo cliente S3, também poderá usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa criar contas de locatário separadas. Consulte as instruções de implementação "Buckets e políticas de buckets do S3" para obter mais informações.

- * Caso de uso do provedor de serviços:* se o sistema StorageGRID estiver sendo usado por um provedor de serviços, o armazenamento de objetos da grade pode ser segregado pelas diferentes entidades que alugam o armazenamento. Por exemplo, pode haver contas de inquilino para a empresa A, empresa B, empresa C e assim por diante.

Como criar uma conta de locatário

As contas de inquilino são criadas por um "Administrador de grade do StorageGRID usando o Gerenciador de grade". Ao criar uma conta de locatário, o administrador da grade especifica o seguinte:

- Informações básicas, incluindo o nome do locatário, o tipo de cliente (S3) e a cota de armazenamento opcional.
- Permissões para a conta de locatário, como se a conta de locatário pode usar os serviços da plataforma S3, configurar sua própria origem de identidade, usar S3 Select ou usar uma conexão de federação de grade.
- O acesso raiz inicial para o locatário, com base se o sistema StorageGRID usa grupos e usuários locais, federação de identidade ou logon único (SSO).

Além disso, os administradores de grade podem ativar a configuração bloqueio de objeto S3 para o sistema StorageGRID se as contas de locatário S3 precisarem cumprir os requisitos regulamentares. Quando o bloqueio de objeto S3 está ativado, todas as contas de locatário do S3 podem criar e gerenciar buckets compatíveis.

Configurar locatários do S3

Depois de um "S3 conta de locatário é criada", você pode acessar o Gerenciador do Locatário para executar tarefas como as seguintes:

- Configurar federação de identidade (a menos que a origem de identidade seja compartilhada com a grade)
- Gerenciar grupos e usuários
- Use a federação de grade para clone de conta e replicação entre grade
- Gerenciar S3 chaves de acesso
- Crie e gerencie buckets do S3
- Use os serviços da plataforma S3
- Utilize S3 Select (Selecionar)
- Monitorar o uso do storage

Embora você possa criar e gerenciar buckets do S3 com o Gerenciador do locatário, use um "Cliente S3" ou "S3 Console" para obter e gerenciar objetos.

Como entrar e sair

Inicie sessão no Tenant Manager

Você acessa o Gerenciador do Locatário inserindo o URL do locatário na barra de endereços de um "navegador da web suportado".

Antes de começar

- Você tem suas credenciais de login.
- Você tem um URL para acessar o Gerenciador do Locatário, conforme fornecido pelo administrador da grade. O URL será parecido com um destes exemplos:

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

  https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
  ```

  O URL sempre inclui um nome de domínio totalmente qualificado (FQDN), o endereço IP de um nó de administração ou o endereço IP virtual de um grupo de HA de nós de administração. Ele também pode incluir um número de porta, o ID da conta de locatário de 20 dígitos ou ambos.

- Se o URL não incluir o ID de conta de 20 dígitos do locatário, você terá esse ID de conta.
- Você está usando um "navegador da web suportado".
- Os cookies são ativados no seu navegador.
- Você pertence a um grupo de usuários que "permissões de acesso específicas"tem .

Passos

1. Inicie um "navegador da web suportado".

2. Na barra de endereços do navegador, insira o URL para acessar o Gerenciador de locatários.
3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Inicie sessão no Gestor do Locatário.

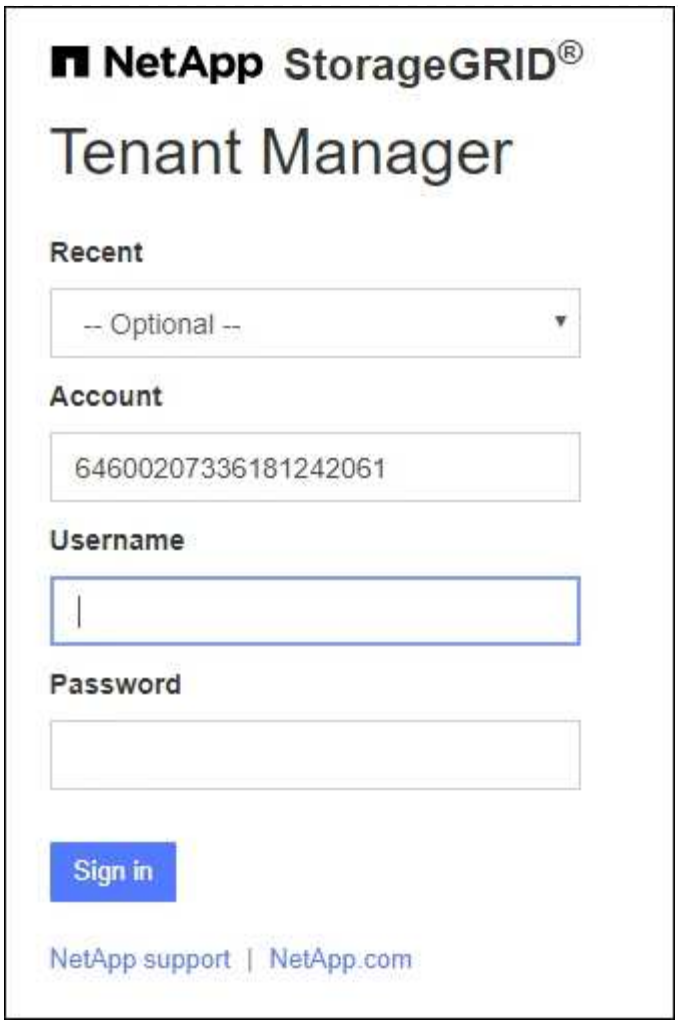
   A tela de login exibida depende do URL digitado e se o SSO (logon único) foi configurado para o StorageGRID.

Não está a utilizar SSO

Se o StorageGRID não estiver usando SSO, uma das seguintes telas será exibida:

- A página de login do Gerenciador de Grade. Selecione o link **Logon** do locatário.

- A página de início de sessão do Tenant Manager. O campo **Account** pode já estar concluído, como mostrado abaixo.



i. Se o ID da conta de 20 dígitos do locatário não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.

ii. Introduza o seu nome de utilizador e palavra-passe.

iii. Selecione **entrar**.

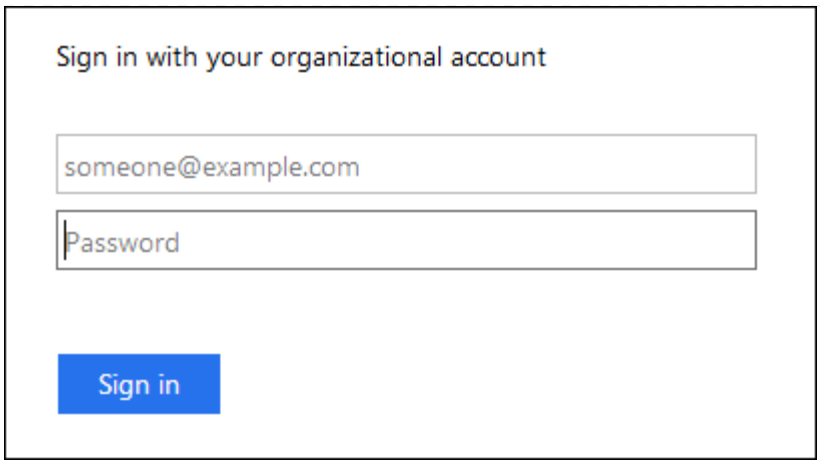
É apresentado o painel do Tenant Manager.

iv. Se você recebeu uma senha inicial de outra pessoa, selecione ***username*** > **alterar senha** para proteger sua conta.

Usando SSO

Se o StorageGRID estiver usando SSO, uma das seguintes telas será exibida:

◦ Página SSO da sua organização. Por exemplo:



Insira suas credenciais SSO padrão e selecione **entrar**.

- A página de login SSO do Tenant Manager.

i. Se o ID da conta de 20 dígitos do locatário não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.

ii. Selecione **entrar**.

iii. Inicie sessão com as suas credenciais SSO padrão na página de início de sessão SSO da sua organização.

É apresentado o painel do Tenant Manager.

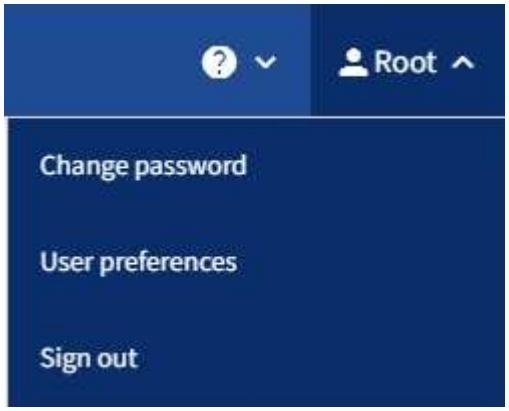
Sair do Tenant Manager

Quando terminar de trabalhar com o Gestor de Locatário, tem de terminar sessão para

garantir que os utilizadores não autorizados não possam aceder ao sistema StorageGRID. Fechar seu navegador pode não sair do sistema, com base nas configurações de cookies do navegador.

Passos

1. Localize o nome de usuário suspenso no canto superior direito da interface do usuário.



2. Selecione o nome de usuário e, em seguida, selecione **Sair**.

   - Se o SSO não estiver em uso:

     Você está desconetado do Admin Node. É apresentada a página de início de sessão do Gestor do Locatário.

     Se você tiver feito login em mais de um nó de administrador, será necessário sair de cada nó.

   - Se o SSO estiver ativado:

     Você está desconetado de todos os nós de administrador que estava acessando. É apresentada a página de início de sessão do StorageGRID. O nome da conta de locatário que você acabou de acessar é listado como padrão na lista suspensa **Recent Accounts** (Contas recentes) e o **Account ID** do locatário é mostrado.

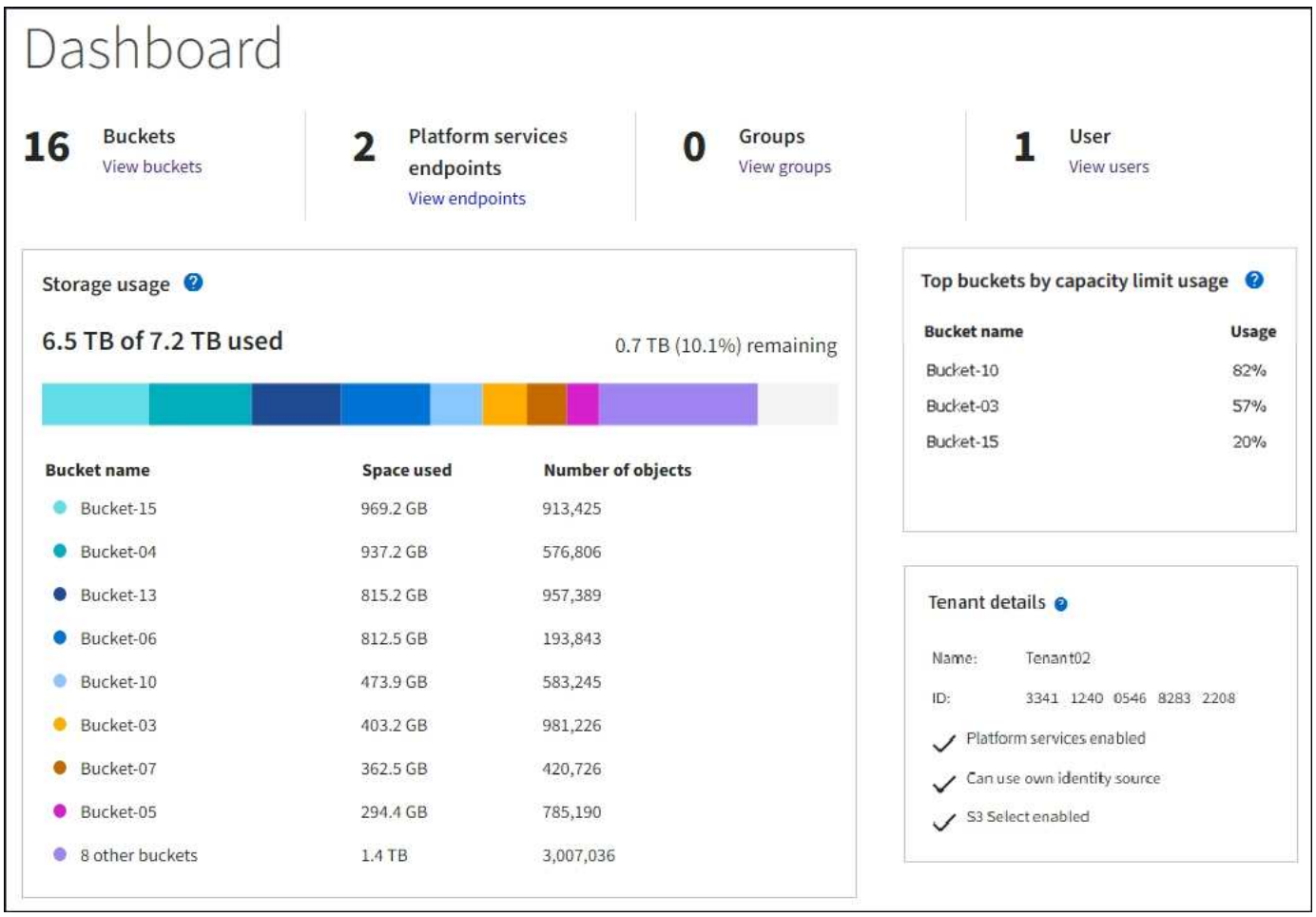
     Se o SSO estiver ativado e você também estiver conetado ao Gerenciador de Grade, você também deverá sair do Gerenciador de Grade para sair do SSO.

Entenda o painel do Tenant Manager

O painel do Tenant Manager fornece uma visão geral da configuração de uma conta de locatário e da quantidade de espaço usada por objetos nos buckets do locatário (S3) ou contentores (Swift). Se o locatário tiver uma cota, o painel mostrará quanto da cota é usada e quanto resta. Se houver algum erro relacionado à conta do locatário, os erros serão exibidos no painel.

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

Quando os objetos tiverem sido carregados, o painel se parece com o seguinte exemplo:



Informações da conta do locatário

A parte superior do painel exibe o número de buckets ou contentores configurados, grupos e usuários. Ele também exibe o número de endpoints de serviços de plataforma, se algum tiver sido configurado. Selecione as ligações para ver os detalhes.

Dependendo do "permissões de gerenciamento do locatário" que você tiver e das opções configuradas, o restante do painel exibe várias combinações de diretrizes, uso do armazenamento, informações de objetos e detalhes do locatário.

Uso de storage e cota

O painel uso do armazenamento contém as seguintes informações:

- A quantidade de dados de objeto para o locatário.

  Esse valor indica a quantidade total de dados de objeto carregados e não representa o espaço usado para armazenar cópias desses objetos e seus metadados.

- Se uma cota for definida, a quantidade total de espaço disponível para os dados do objeto e a quantidade e porcentagem de espaço restante. A cota limita a quantidade de dados de objetos que podem ser ingeridos.

O uso da cota é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita 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 o uso da cota seja recalculado. Os cálculos de uso de cotas podem levar 10 minutos ou mais.

- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou contentores.

  Você pode colocar o cursor sobre qualquer um dos segmentos do gráfico para visualizar o espaço total consumido por esse intervalo ou contentor.

- Para corresponder ao gráfico de barras, uma lista dos maiores buckets ou contentores, incluindo a quantidade total de dados do objeto e o número de objetos para cada bucket ou contentor.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

  Se o locatário tiver mais de nove buckets ou contêineres, todos os outros buckets ou contêineres serão combinados em uma única entrada na parte inferior da lista.

Para alterar as unidades para os valores de armazenamento exibidos no Gerenciador do locatário, selecione a lista suspensa usuário no canto superior direito do Gerenciador do locatário e selecione **Preferências do usuário**.

Alertas de uso de cota

Se os alertas de uso de cota tiverem sido ativados no Gerenciador de Grade, esses alertas aparecerão no Gerenciador de Locatário quando a cota for baixa ou excedida, da seguinte forma:

- Se 90% ou mais da cota de um locatário tiver sido usada, o alerta **uso de cota de locatário alto** será acionado.

  Considere pedir ao administrador da grade para aumentar a cota.

- Se você exceder sua cota, uma notificação informa que você não pode carregar novos objetos.

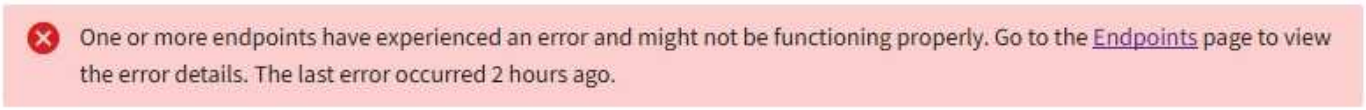
uso do limite de capacidade

Se você definiu um limite de capacidade para seus buckets, o painel do Gerenciador do locatário exibirá uma lista dos buckets principais por uso do limite de capacidade.

Se nenhum limite for definido para um bucket, sua capacidade será ilimitada. No entanto, se sua conta de locatário tiver uma cota total de armazenamento e essa cota for atingida, você não poderá ingerir mais objetos independentemente do limite de capacidade restante em um bucket.

Erros de endpoint

Se você usou o Gerenciador de Grade para configurar um ou mais endpoints para uso com serviços de plataforma, o painel do Gerenciador do locatário exibirá um alerta se algum erro de endpoint tiver ocorrido nos últimos sete dias.



Para ver detalhes sobre "erros de endpoint dos serviços da plataforma"o , selecione **Endpoints** para exibir a página Endpoints.

API de gerenciamento do locatário

Entenda a API de gerenciamento do locatário

Você pode executar tarefas de gerenciamento do sistema usando a API REST do Gerenciamento do locatário em vez da interface de usuário do Gerenciador do locatário. Por exemplo, você pode querer usar a API para automatizar operações ou criar várias entidades, como usuários, mais rapidamente.

A API de gerenciamento do locatário:

- Usa a plataforma de API Swagger de código aberto. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores interajam com a API. A interface do usuário Swagger fornece detalhes completos e documentação para cada operação da API.
- Utiliza "controle de versão para dar suporte a atualizações sem interrupções".

Para acessar a documentação do Swagger para a API de gerenciamento do locatário:

1. Inicie sessão no Gestor do Locatário.
2. Na parte superior do Gerenciador do Locatário, selecione o ícone de ajuda e selecione **Documentação da API**.

Operações da API

A API de Gerenciamento do Tenant organiza as operações de API disponíveis nas seguintes seções:

- * Conta*: Operações na conta de locatário atual, incluindo obter informações de uso do armazenamento.
- **Auth**: Operações para realizar autenticação de sessão do usuário.

  A API de gerenciamento do locatário suporta o esquema de autenticação de token do portador. Para um login de locatário, você fornece um nome de usuário, senha e AccountID no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com êxito, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("autorização: Token portador").

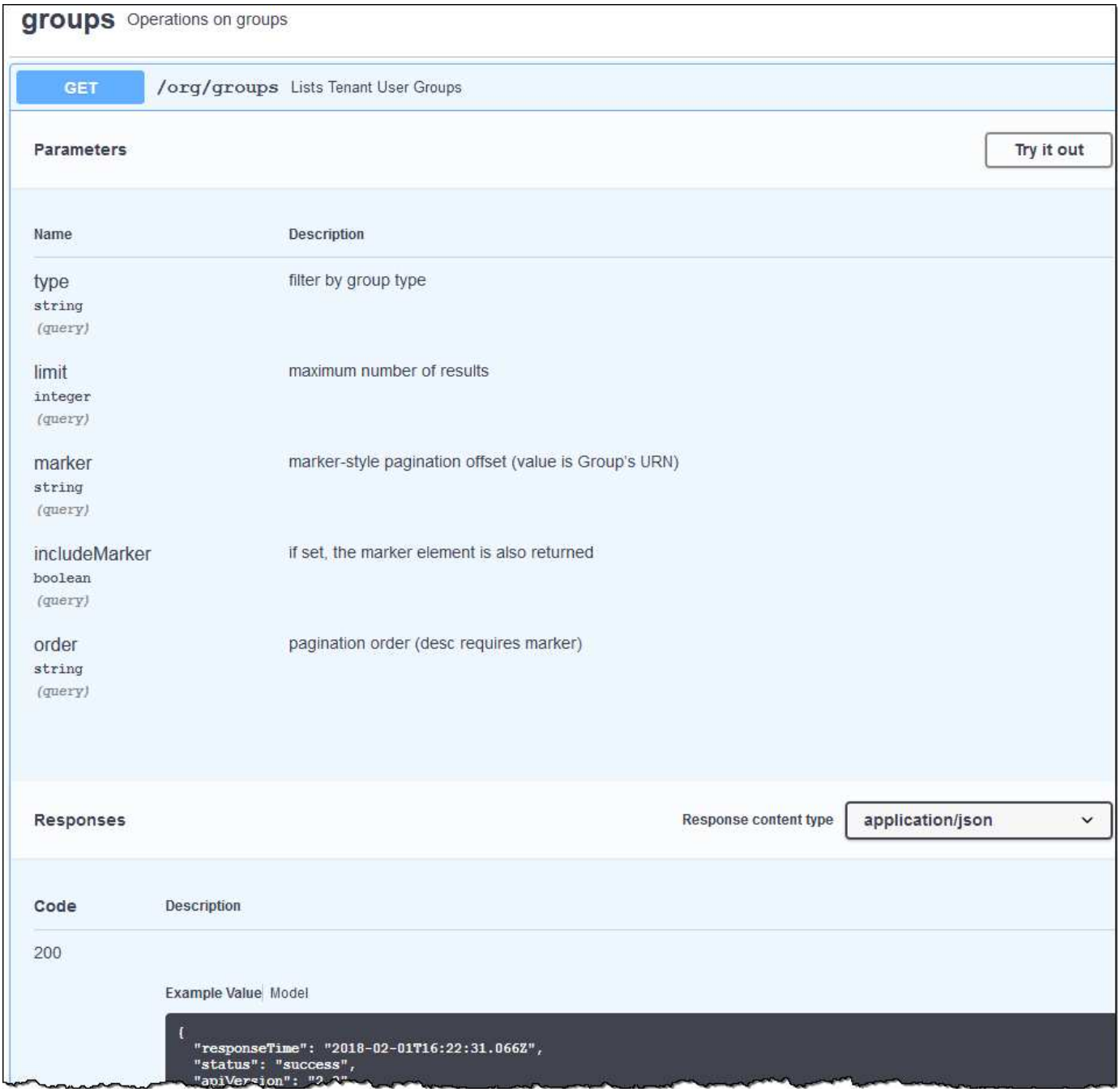
  Para obter informações sobre como melhorar a segurança de autenticação, "Proteger contra falsificação de pedidos entre sites"consulte .

  > ⓘ Se o logon único (SSO) estiver ativado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte "Instruções para usar a API Grid Management".

- **Config**: Operações relacionadas à versão do produto e versões da API de Gerenciamento do Tenant. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **Containers**: Operações em baldes S3 ou contentores Swift.
- **Disabled-features**: Operações para visualizar recursos que podem ter sido desativados.
- **Endpoints**: Operações para gerenciar um endpoint. Os endpoints permitem que um bucket do S3 use um serviço externo para replicação, notificações ou integração de pesquisa do StorageGRID CloudMirror.
- * Grid-federação-conexões*: Operações em conexões de federação de grade e replicação entre grade.
- **Groups**: Operações para gerenciar grupos de locatários locais e recuperar grupos de locatários federados de uma fonte de identidade externa.
- **Identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **ilm**: Operações nas configurações de gerenciamento do ciclo de vida da informação (ILM).
- **Regions**: Operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **S3**: Operações para gerenciar S3 chaves de acesso para usuários arrendatários.
- **S3-object-lock**: Operações em configurações globais de bloqueio de objetos S3D, usadas para suportar a conformidade regulamentar.
- **Usuários**: Operações para visualizar e gerenciar usuários de inquilinos.

Detalhes da operação

Quando você expande cada operação da API, você pode ver sua ação HTTP, URL do endpoint, uma lista de todos os parâmetros necessários ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.



Emitir solicitações de API

> Todas as operações de API executadas usando a página da Documentação da API são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. Selecione a ação HTTP para ver os detalhes da solicitação.
2. Determine se a solicitação requer parâmetros adicionais, como um grupo ou ID de usuário. Em seguida, obtenha esses valores. Talvez você precise emitir uma solicitação de API diferente primeiro para obter as informações de que precisa.
3. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode selecionar **modelo** para aprender os requisitos para cada campo.

4. Selecione **Experimente**.
5. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
6. Selecione **Executar**.
7. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Controle de versão da API de gerenciamento de locatário

A API de gerenciamento do locatário usa o controle de versão para oferecer suporte a atualizações sem interrupções.

Por exemplo, este URL de solicitação especifica a versão 4 da API.

`https://hostname_or_ip_address/api/v4/authorize`

A versão principal da API é quebrada quando alterações são feitas que são *não compatíveis* com versões mais antigas. A versão menor da API é quebrada quando alterações são feitas que *são compatíveis* com versões mais antigas. As alterações compatíveis incluem a adição de novos endpoints ou novas propriedades.

O exemplo a seguir ilustra como a versão da API é carregada com base no tipo de alterações feitas.

Tipo de alteração para API	Versão antiga	Nova versão
Compatível com versões mais antigas	2,1	2,2
Não compatível com versões mais antigas	2,1	3,0

Quando você instala o software StorageGRID pela primeira vez, apenas a versão mais recente da API é ativada. No entanto, quando você atualiza para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.

> Pode configurar as versões suportadas. Consulte a seção **config** da documentação da API Swagger para "API de gerenciamento de grade"obter mais informações. Você deve desativar o suporte para a versão mais antiga depois de atualizar todos os clientes de API para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Deprecated: True"
- O corpo de resposta JSON inclui "obsoleto": True
- Um aviso obsoleto é adicionado ao nms.log. Por exemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determine quais versões de API são suportadas na versão atual

Use a `GET /versions` solicitação de API para retornar uma lista das principais versões da API suportada. Esta solicitação está localizada na seção **config** da documentação da API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especifique uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v4`) ou um cabeçalho (`Api-Version: 4`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Proteger contra falsificação de solicitação entre locais (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra StorageGRID usando tokens CSRF para melhorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes de API podem optar por ativá-lo quando fizerem login.

Um invasor que pode acionar uma solicitação para um site diferente (como um POST de formulário HTTP) pode fazer com que certas solicitações sejam feitas usando os cookies do usuário conetado.

O StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro específico DO corpo DO POST.

Para ativar a funcionalidade, defina o `csrfToken` parâmetro para `true` durante a autenticação. A predefinição é `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando verdadeiro, um `GridCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Grade, e o `AccountCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Tenant.

Se o cookie estiver presente, todas as solicitações que podem modificar o estado do sistema (POST, PUT, PATCH, DELETE) devem incluir um dos seguintes itens:

- O `X-Csrf-Token` cabeçalho, com o valor do cabeçalho definido para o valor do cookie de token CSRF.
- Para endpoints que aceitam um corpo codificado por formulário: Um `csrfToken` parâmetro corpo de solicitação codificado por formulário.

Para configurar a proteção CSRF, use o "API de gerenciamento de grade" ou "API de gerenciamento do locatário".

> As solicitações que têm um conjunto de cookies de token CSRF também irão aplicar o cabeçalho "Content-Type: Application/json" para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

Use conexões de federação de grade

Clonar grupos de locatários e usuários

Se um locatário foi criado ou editado para usar uma conexão de federação de grade, esse locatário é replicado de um sistema StorageGRID (o locatário de origem) para outro sistema StorageGRID (o locatário de réplica). Depois que o locatário tiver sido replicado, todos os grupos e usuários adicionados ao locatário de origem serão clonados para o locatário de réplica.

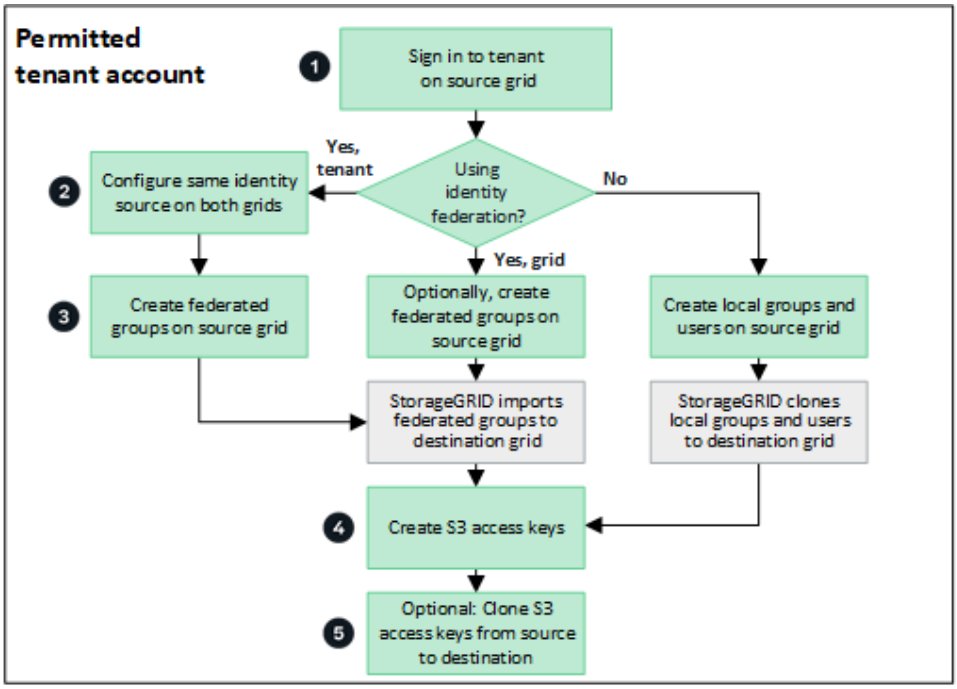
O sistema StorageGRID onde o locatário é originalmente criado é a *grade de origem* do locatário. O sistema StorageGRID onde o locatário é replicado é a *grade de destino* do locatário. Ambas as contas de inquilino têm o mesmo ID de conta, nome, descrição, cota de armazenamento e permissões atribuídas, mas o locatário de destino não tem inicialmente uma senha de usuário raiz. Para obter detalhes, "O que é o clone de conta"consulte e "Gerenciar locatários permitidos".

A clonagem de informações de conta de locatário é necessária para "replicação entre grade"objetos bucket. Ter os mesmos grupos de inquilinos e usuários em ambas as grades garante que você possa acessar os buckets e objetos correspondentes em qualquer grade.

Fluxo de trabalho do locatário para clone de conta

Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, revise o diagrama do fluxo

de trabalho para ver as etapas que você executará para clonar grupos, usuários e chaves de acesso S3.



Estas são as etapas principais no fluxo de trabalho:

1 Inicie sessão no inquilino

Faça login na conta de locatário na grade de origem (a grade onde o locatário foi criado inicialmente.)

2 Opcionalmente, configure a federação de identidade

Se sua conta de locatário tiver a permissão **Use own Identity source** para usar grupos federados e usuários, configure a mesma fonte de identidade (com as mesmas configurações) para as contas de locatário de origem e destino. Grupos federados e usuários não podem ser clonados a menos que ambas as grades estejam usando a mesma fonte de identidade. Para obter instruções, "Use a federação de identidade"consulte .

3 Crie grupos e usuários

Ao criar grupos e usuários, sempre comece a partir da grade de origem do locatário. Quando você adiciona um novo grupo, o StorageGRID o clona automaticamente à grade de destino.

- Se a federação de identidade estiver configurada para todo o sistema StorageGRID ou para sua conta de locatário, "criar novos grupos de inquilinos"importando grupos federados da origem da identidade.
- Se você não estiver usando a federação de identidade "crie novos grupos locais"e, em seguida"crie usuários locais", .

4 Crie S3 chaves de acesso

Você pode "crie suas próprias chaves de acesso" ou fazer "crie chaves de acesso de outro usuário" na grade de origem ou na grade de destino para acessar buckets nessa grade.

5 **Opcionalmente, clonar chaves de acesso S3**

Se você precisar acessar buckets com as mesmas chaves de acesso em ambas as grades, crie as chaves de acesso na grade de origem e use a API do Gerenciador do locatário para cloná-las manualmente na grade de destino. Para obter instruções, "Clonar chaves de acesso S3 usando a API"consulte .

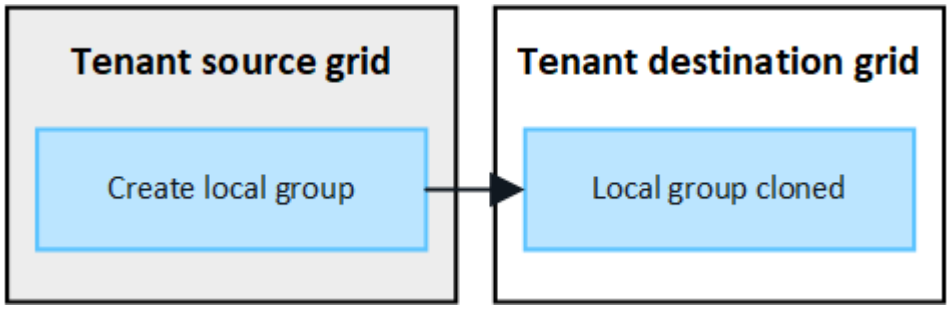
Como grupos, usuários e chaves de acesso S3 são clonadas?

Revise esta seção para entender como grupos, usuários e chaves de acesso S3 são clonados entre a grade de origem do locatário e a grade de destino do locatário.

Os grupos locais criados na grade de origem são clonados

Depois que uma conta de locatário é criada e replicada na grade de destino, o StorageGRID clonará automaticamente todos os grupos locais adicionados à grade de origem do locatário à grade de destino do locatário.

Tanto o grupo original quanto seu clone têm o mesmo modo de acesso, permissões de grupo e política de grupo S3. Para obter instruções, "Criar grupos para S3 inquilino"consulte .

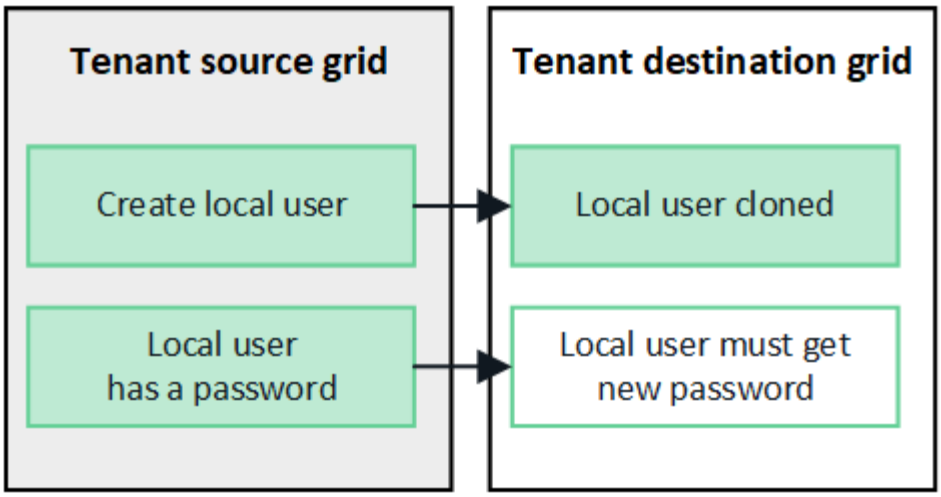


Os usuários selecionados quando você cria um grupo local na grade de origem não são incluídos quando o grupo é clonado para a grade de destino. Por esse motivo, não selecione usuários quando você criar o grupo. Em vez disso, selecione o grupo quando você criar os usuários.

Os usuários locais criados na grade de origem são clonados

Quando você cria um novo usuário local na grade de origem, o StorageGRID automaticamente clona esse usuário na grade de destino. Tanto o usuário original quanto seu clone têm o mesmo nome completo, nome de usuário e configuração **Negar acesso**. Ambos os usuários também pertencem aos mesmos grupos. Para obter instruções, "Gerenciar usuários locais"consulte .

Por motivos de segurança, as senhas de usuário local não são clonadas para a grade de destino. Se um usuário local precisar acessar o Gerenciador do Locatário na grade de destino, o usuário raiz da conta do locatário deve adicionar uma senha para esse usuário na grade de destino. Para obter instruções, "Gerenciar usuários locais"consulte .

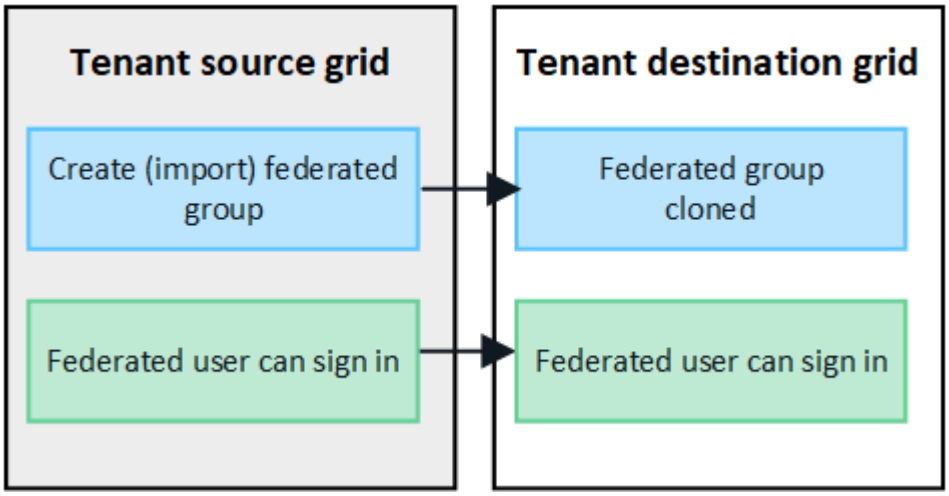


Os grupos federados criados na grade de origem são clonados

Supondo que os requisitos para usar o clone de conta com "logon único" e "federação de identidade" tenham sido atendidos, os grupos federados que você criar (importar) para o locatário na grade de origem são clonados automaticamente para o locatário na grade de destino.

Ambos os grupos têm o mesmo modo de acesso, permissões de grupo e política de grupo S3.

Depois que os grupos federados forem criados para o locatário de origem e clonados para o locatário de destino, os usuários federados poderão fazer login no locatário em qualquer grade.

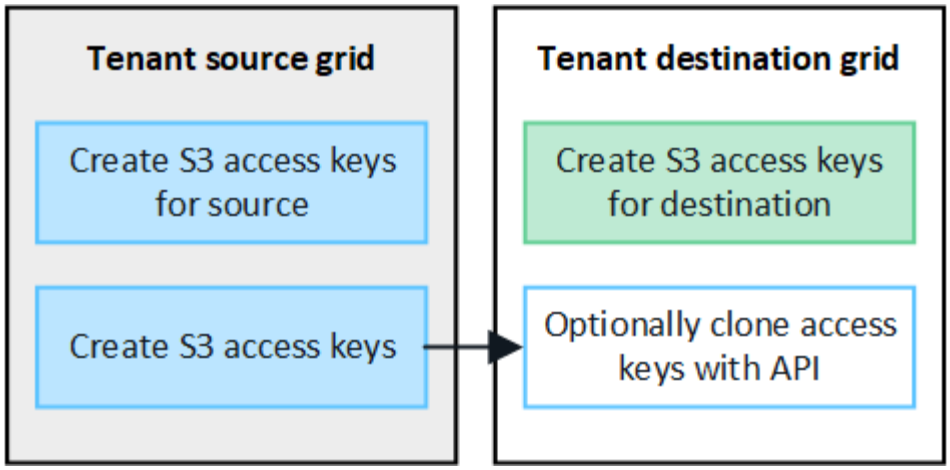


S3 teclas de acesso podem ser clonadas manualmente

O StorageGRID não clonar automaticamente as chaves de acesso S3 porque a segurança é melhorada por ter chaves diferentes em cada grade.

Para gerenciar chaves de acesso nas duas grades, você pode fazer um dos seguintes procedimentos:

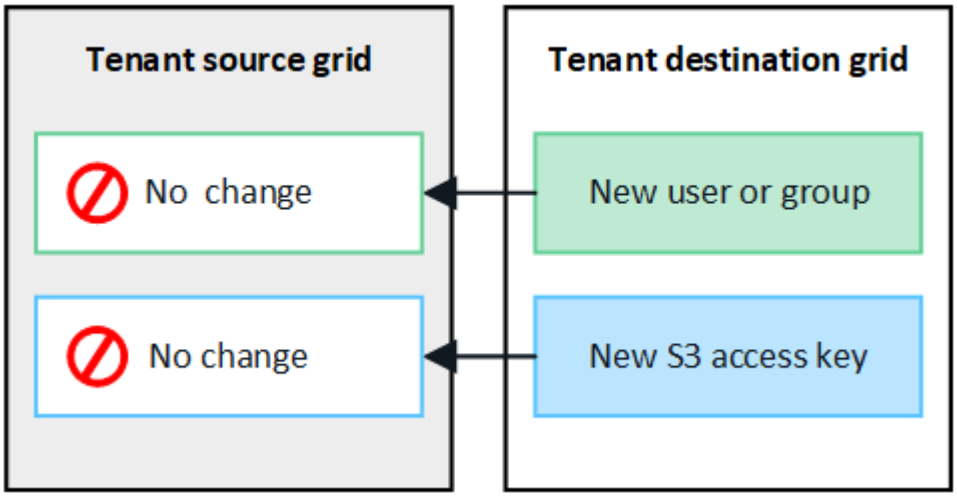
- Se você não precisa usar as mesmas teclas para cada grade, você pode "crie suas próprias chaves de acesso" ou "crie chaves de acesso de outro usuário" em cada grade.
- Se você precisar usar as mesmas chaves em ambas as grades, você pode criar chaves na grade de origem e usar a API do Gerenciador do locatário para manualmente "clone as chaves" para a grade de destino.



Quando você clonar chaves de acesso S3 para um usuário federado, tanto o usuário quanto as chaves de acesso S3 são clonadas para o locatário de destino.

Os grupos e usuários adicionados à grade de destino não são clonados

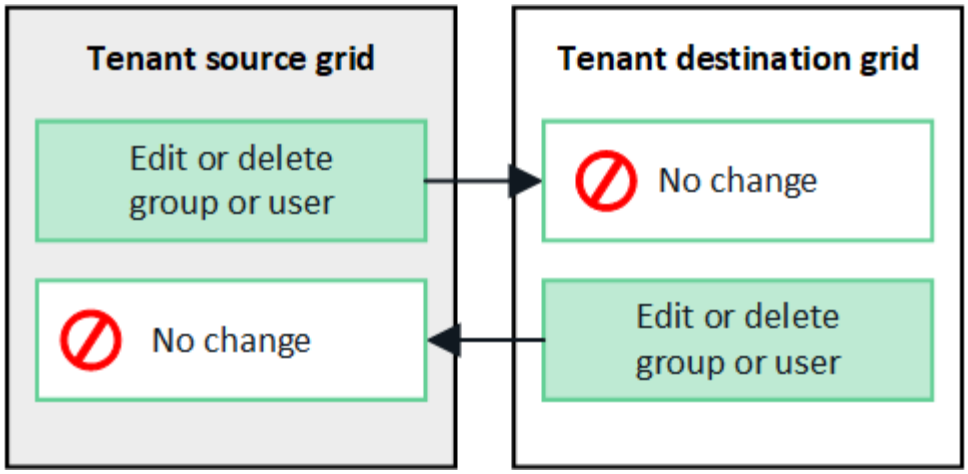
A clonagem ocorre somente da grade de origem do locatário para a grade de destino do locatário. Se você criar ou importar grupos e usuários na grade de destino do locatário, o StorageGRID não clonará esses itens de volta à grade de origem do locatário.



Grupos, usuários e chaves de acesso editados ou excluídos não são clonados

A clonagem ocorre somente quando você cria novos grupos e usuários.

Se você editar ou excluir grupos, usuários ou chaves de acesso em qualquer grade, suas alterações não serão clonadas para a outra grade.



Clonar chaves de acesso S3 usando a API

Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, você poderá usar a API de Gerenciamento do locatário para clonar manualmente as chaves de acesso S3 do locatário na grade de origem para o locatário na grade de destino.

Antes de começar

- A conta de locatário tem a permissão **Use Grid Federation Connection**.
- A conexão de federação de grade tem um **status de conexão** de **conectado**.
- Você está conetado ao Gerenciador do Locatário na grade de origem do locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie suas próprias credenciais S3 ou permissão de acesso root".
- Se você estiver clonando chaves de acesso para um usuário local, o usuário já existe em ambas as grades.

> Quando você clonar chaves de acesso S3 para um usuário federado, tanto o usuário quanto as chaves de acesso S3 são adicionadas ao locatário de destino.

Clone suas próprias chaves de acesso

Você pode clonar suas próprias chaves de acesso se precisar acessar os mesmos buckets em ambas as grades.

Passos

1. Usando o Gerenciador do Tenant na grade de origem e "crie suas próprias chaves de acesso"baixe o `.csv` arquivo.
2. Na parte superior do Gerenciador do Locatário, selecione o ícone de ajuda e selecione **Documentação da API**.
3. Na seção **S3**, selecione o seguinte ponto final:

```
POST /org/users/current-user/replicate-s3-access-key
```

4. Selecione **Experimente**.
5. Na caixa de texto **body**, substitua as entradas de exemplo para **accessKey** e **secretAccessKey** pelos valores do arquivo **.csv** que você baixou.

   Certifique-se de manter as aspas duplas em torno de cada string.

6. Se a chave expirar, substitua a entrada de exemplo para **Expires** pela data e hora de expiração como uma string no formato de data-hora ISO 8601 (por exemplo, `2024-02-28T22:46:33-08:00`). Se a chave não expirar, digite **null** como o valor da entrada **expira** (ou remova a linha **expira** e a vírgula anterior).
7. Selecione **Executar**.
8. Confirme se o código de resposta do servidor é **204**, indicando que a chave foi clonada com sucesso para a grade de destino.

Clonar chaves de acesso de outro usuário

Você pode clonar as chaves de acesso de outro usuário se ele precisar acessar os mesmos buckets em ambas as grades.

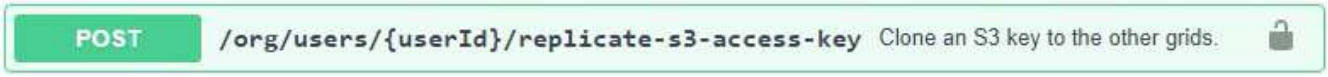
Passos

1. Usando o Gerenciador do Tenant na grade de origem e "Crie as chaves de acesso S3 do outro usuário"baixe o `.csv` arquivo.
2. Na parte superior do Gerenciador do Locatário, selecione o ícone de ajuda e selecione **Documentação da API**.
3. Obtenha a ID do utilizador. Você precisará desse valor para clonar as chaves de acesso do outro usuário.
   a. Na seção **usuários**, selecione o seguinte ponto final:

      `GET /org/users`

   b. Selecione **Experimente**.
   c. Especifique quaisquer parâmetros que você deseja usar ao procurar usuários.
   d. Selecione **Executar**.
   e. Encontre o usuário cujas chaves você deseja clonar e copie o número no campo **id**.
4. Na seção **S3**, selecione o seguinte ponto final:

   `POST /org/users/{userId}/replicate-s3-access-key`



5. Selecione **Experimente**.
6. Na caixa de texto **UserId**, cole o ID de usuário que você copiou.
7. Na caixa de texto **body**, substitua as entradas de exemplo para **example access key** e **secret access key** pelos valores do arquivo **.csv** para esse usuário.

   Certifique-se de manter as aspas duplas ao redor da string.

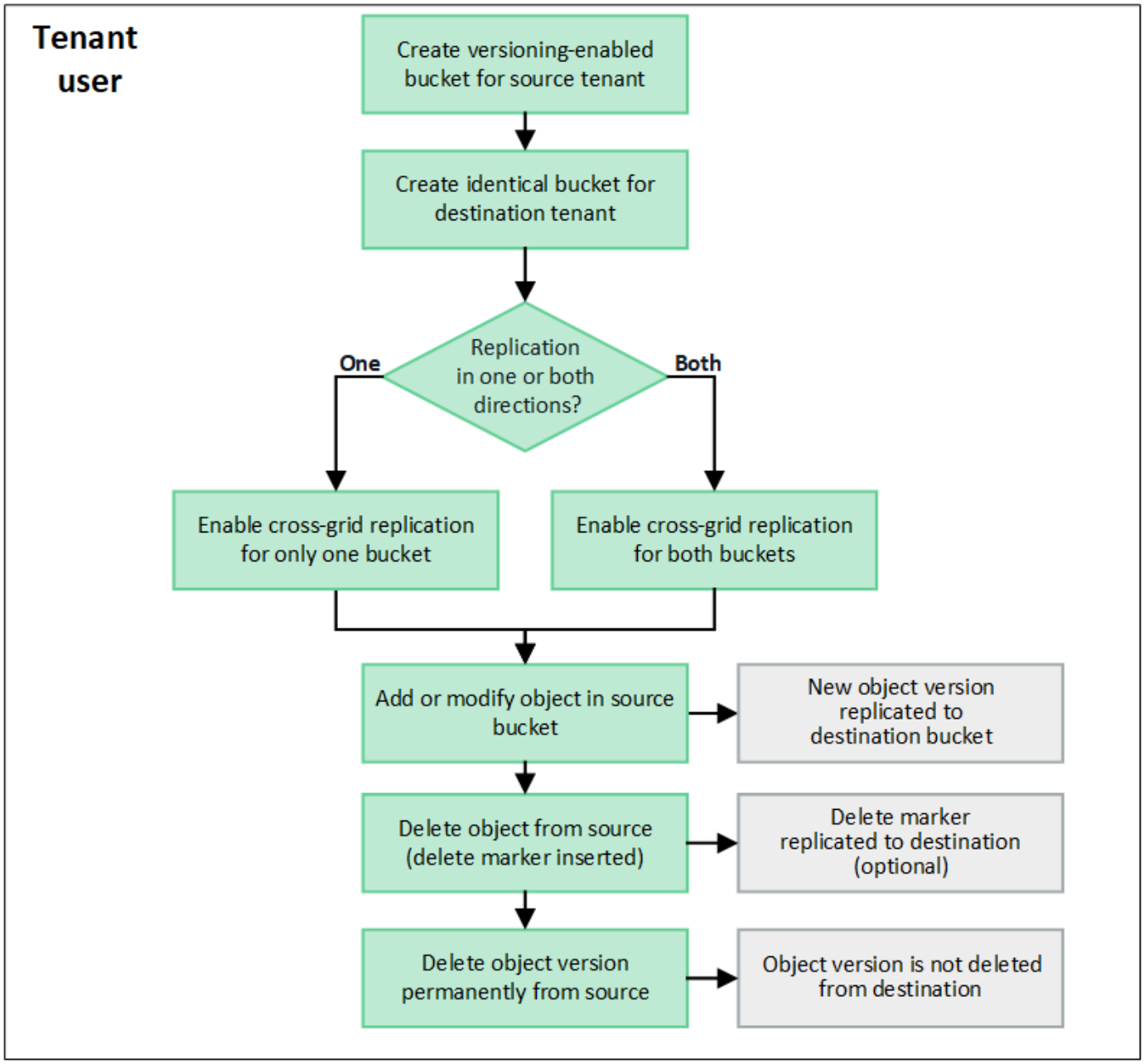
8. Se a chave expirar, substitua a entrada de exemplo para **Expires** pela data e hora de expiração como uma string no formato de data-hora ISO 8601 (por exemplo, `2023-02-28T22:46:33-08:00`). Se a chave não expirar, digite **null** como o valor da entrada **expira** (ou remova a linha **expira** e a vírgula anterior).
9. Selecione **Executar**.
10. Confirme se o código de resposta do servidor é **204**, indicando que a chave foi clonada com sucesso para a grade de destino.

Gerenciar a replicação entre grades

Se a sua conta de locatário tiver sido atribuída a permissão **usar conexão de federação de grade** quando ela foi criada, você poderá usar a replicação entre grade para replicar automaticamente objetos entre buckets na grade de origem do locatário e buckets na grade de destino do locatário. A replicação entre grades pode ocorrer em uma ou ambas as direções.

Fluxo de trabalho para replicação entre grades

O diagrama do fluxo de trabalho resume as etapas que você executará para configurar a replicação entre grades entre intervalos em duas grades. Estas etapas são descritas em mais detalhes abaixo.



Configurar a replicação entre redes

Antes de usar a replicação entre grade, você deve fazer login nas contas de locatário correspondentes em cada grade e criar buckets idênticos. Em seguida, é possível habilitar a replicação entre grade em um ou em ambos os buckets.

Antes de começar

- Você revisou os requisitos para replicação entre grade. "O que é replicação entre grades"Consulte .
- Você está usando um "navegador da web suportado".
- A conta de locatário tem a permissão **usar conexão de federação de grade** e contas de locatário idênticas existem em ambas as grades. "Gerenciar os locatários permitidos para conexão de federação de grade"Consulte .
- O usuário de locatário que você fará login como já existe em ambas as grades e pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

- Se você estiver entrando na grade de destino do locatário como usuário local, o usuário raiz da conta do locatário definiu uma senha para sua conta de usuário nessa grade.

Crie dois baldes idênticos

Como primeira etapa, faça login nas contas de locatário correspondentes em cada grade e crie buckets idênticos.

Passos

1. A partir de qualquer grade na conexão de federação de grade, crie um novo intervalo:
   a. Faça login na conta de locatário usando as credenciais de um usuário de locatário que existe em ambas as grades.

      Se você não conseguir entrar na grade de destino do locatário como um usuário local, confirme se o usuário raiz da conta de locatário definiu uma senha para sua conta de usuário.

   b. Siga as instruções "Crie um bucket do S3"para .
   c. Na guia **Manage Object settings** (Gerenciar configurações de objeto), selecione **Enable Object versioning** (Ativar controle de versão de objeto).
   d. Se o bloqueio de objeto S3 estiver ativado para o seu sistema StorageGRID, não ative o bloqueio de objeto S3 para o bucket.
   e. Selecione **criar bucket**.
   f. Selecione **Finish**.
2. Repita essas etapas para criar um intervalo idêntico para a mesma conta de locatário na outra grade na conexão de federação de grade.

   Conforme necessário, cada balde pode usar uma região diferente.

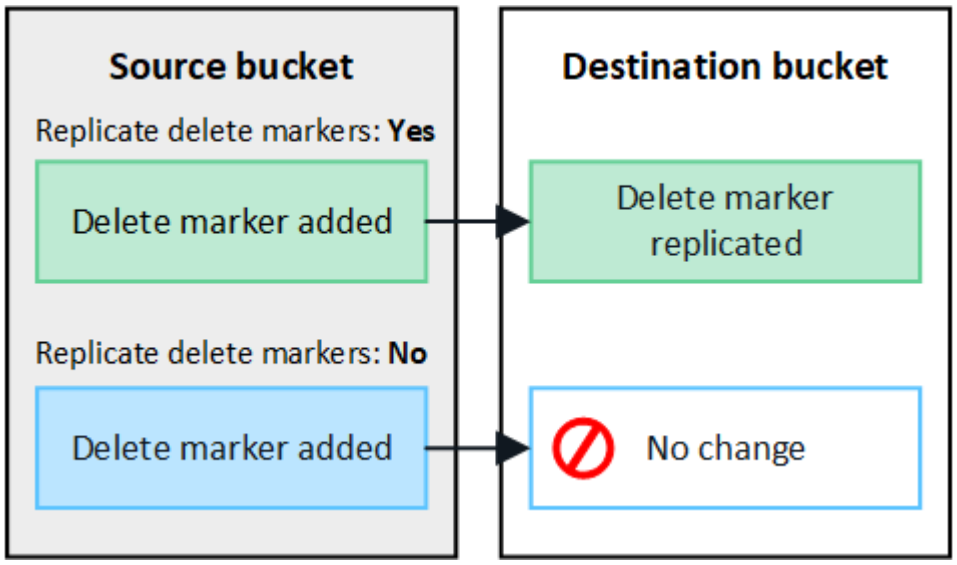
Ative a replicação entre redes

Você deve executar estas etapas antes de adicionar quaisquer objetos a qualquer bucket.

Passos

1. A partir de uma grade cujos objetos você deseja replicar, habilite "replicação entre grade em uma direção":
   a. Faça login na conta do locatário do bucket.
   b. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
   c. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
   d. Selecione a guia **replicação entre grades**.
   e. Selecione **Ativar** e reveja a lista de requisitos.
   f. Se todos os requisitos tiverem sido atendidos, selecione a conexão de federação de grade que deseja usar.
   g. Opcionalmente, altere a configuração de **Replicate DELETE markers** para determinar o que acontece na grade de destino se um cliente S3 emitir uma solicitação de exclusão para a grade de origem que não inclui um ID de versão:

- **Sim** (padrão): Um marcador de exclusão é adicionado ao intervalo de origem e replicado ao intervalo de destino.
- **Não**: Um marcador de exclusão é adicionado ao intervalo de origem, mas não é replicado para o intervalo de destino.



> Se a solicitação de exclusão incluir um ID de versão, essa versão do objeto será removida permanentemente do intervalo de origem. O StorageGRID não replica solicitações de exclusão que incluem um ID de versão, portanto, a mesma versão do objeto não é excluída do destino.

"O que é replicação entre grades"Consulte para obter detalhes.

a. Opcionalmente, altere a configuração da categoria de auditoria **replicação entre redes** para gerenciar o volume de mensagens de auditoria:
   - **Erro** (padrão): Somente solicitações de replicação entre grade com falha são incluídas na saída da auditoria.
   - **Normal**: Todas as solicitações de replicação entre redes estão incluídas, o que aumenta significativamente o volume da saída da auditoria.
b. Reveja as suas seleções. Você não pode alterar essas configurações a menos que ambos os buckets estejam vazios.
c. Selecione **Ativar e testar**.

   Depois de alguns momentos, uma mensagem de sucesso aparece. Os objetos adicionados a esse bucket serão replicados automaticamente para a outra grade. **A replicação entre grades** é mostrada como um recurso habilitado na página de detalhes do bucket.

2. Opcionalmente, vá para o balde correspondente na outra grade e "ative a replicação entre grades em ambas as direções".

Teste a replicação entre grades

Se a replicação entre grades estiver habilitada para um bucket, talvez seja necessário verificar se a conexão e a replicação entre grades estão funcionando corretamente e se os buckets de origem e destino ainda atendem a todos os requisitos (por exemplo, o controle de versão ainda está habilitado).

Antes de começar

- Você está usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

Passos

1. Faça login na conta do locatário do bucket.
2. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
4. Selecione a guia **replicação entre grades**.
5. Selecione **Test Connection**.

   Se a conexão estiver saudável, um banner de sucesso será exibido. Caso contrário, uma mensagem de erro é exibida, que você e o administrador da grade podem usar para resolver o problema. Para obter detalhes, "Solucionar erros de federação de grade"consulte .

6. Se a replicação entre grades estiver configurada para ocorrer em ambas as direções, vá para o intervalo correspondente na outra grade e selecione **conexão de teste** para verificar se a replicação entre grades está funcionando na outra direção.

Desative a replicação entre redes

Você pode parar permanentemente a replicação entre grade se não quiser mais copiar objetos para a outra grade.

Antes de desativar a replicação entre grades, observe o seguinte:

- A desativação da replicação entre grades não remove nenhum objeto que já tenha sido copiado entre grades. Por exemplo, os objetos no `my-bucket` na Grade 1 que foram copiados `my-bucket` no Grid 2 não serão removidos se você desativar a replicação entre grades para esse bucket. Se você quiser excluir esses objetos, você deve removê-los manualmente.
- Se a replicação entre grade foi ativada para cada um dos buckets (ou seja, se a replicação ocorrer em ambas as direções), você pode desativar a replicação entre grade para um ou ambos os buckets. Por exemplo, você pode querer desativar a replicação de objetos `my-bucket` de na Grade 1 para na Grade `my-bucket` 2, enquanto continua a replicar objetos `my-bucket` de na Grade 2 para na Grade `my-bucket` 1.
- Você deve desativar a replicação entre grade antes de remover a permissão de um locatário para usar a conexão de federação de grade. "Gerenciar locatários permitidos"Consulte .
- Se você desabilitar a replicação entre grade para um bucket que contém objetos, não será possível reativar a replicação entre grade a menos que você exclua todos os objetos dos buckets de origem e destino.

  Não é possível reativar a replicação a menos que ambos os buckets estejam vazios.

Antes de começar

- Você está usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

Passos

1. A partir da grade cujos objetos você não deseja mais replicar, pare a replicação entre grade para o bucket:
   a. Faça login na conta do locatário do bucket.
   b. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
   c. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
   d. Selecione a guia **replicação entre grades**.
   e. Selecione **Desativar replicação**.
   f. Se tiver certeza de que deseja desativar a replicação entre grades para esse intervalo, digite **Yes** na caixa de texto e selecione **Disable**.

      Depois de alguns momentos, uma mensagem de sucesso aparece. Novos objetos adicionados a esse bucket não podem mais ser replicados automaticamente para a outra grade. **A replicação entre grades** não é mais mostrada como um recurso habilitado na página Buckets.
2. Se a replicação entre grade foi configurada para ocorrer em ambas as direções, vá para o intervalo correspondente na outra grade e pare a replicação entre grade na outra direção.

Exibir conexões de federação de grade

Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, você poderá visualizar as conexões permitidas.

Antes de começar

- A conta de locatário tem a permissão **Use Grid Federation Connection**.
- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

Passos

1. Selecione **STORAGE (S3)** > **conexões de federação de grade**.

   A página de conexão de federação de grade é exibida e inclui uma tabela que resume as seguintes informações:

Coluna	Descrição
Nome da ligação	As conexões de federação de grade que este locatário tem permissão para usar.
Buckets com replicação entre grade	Para cada conexão de federação de grade, os buckets do locatário que têm replicação entre grade habilitada. Os objetos adicionados a esses buckets serão replicados para a outra grade na conexão.
Último erro	Para cada conexão de federação de grade, o erro mais recente ocorre, se houver, quando os dados estavam sendo replicados para a outra grade. Apague o último erroConsulte .

2. Opcionalmente, selecione um nome de bucket para "veja os detalhes do balde".

limpe o último erro

Um erro pode aparecer na coluna **último erro** por um destes motivos:

- A versão do objeto fonte não foi encontrada.
- O balde de origem não foi encontrado.
- O intervalo de destino foi eliminado.
- O intervalo de destino foi recriado por uma conta diferente.
- O bucket de destino tem controle de versão suspenso.
- O intervalo de destino foi recriado pela mesma conta, mas agora não foi versionado.

> Esta coluna mostra apenas o último erro de replicação entre grelha a ocorrer; os erros anteriores que possam ter ocorrido não serão apresentados.

Passos

1. Se uma mensagem for exibida na coluna **último erro**, exiba o texto da mensagem.

   Por exemplo, esse erro indica que o intervalo de destino para replicação entre grades estava em um estado inválido, possivelmente porque o controle de versão foi suspenso ou o bloqueio de objeto S3 foi ativado.

2. Execute quaisquer ações recomendadas. Por exemplo, se o controle de versão foi suspenso no bucket de destino para replicação entre grades, reative o controle de versão desse bucket.
3. Selecione a ligação na tabela.
4. Selecione **Clear error**.
5. Selecione **Sim** para limpar a mensagem e atualizar o estado do sistema.
6. Aguarde 5-6 minutos e, em seguida, insira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

   > Para garantir que a mensagem de erro seja limpa, aguarde pelo menos 5 minutos após o carimbo de data/hora na mensagem antes de inserir um novo objeto.

7. Para determinar se algum objeto não pôde ser replicado devido ao erro de bucket, "Identificar e tentar novamente operações de replicação com falha"consulte .

Gerenciar grupos e usuários

Use a federação de identidade

O uso da federação de identidade torna a configuração de grupos de locatários e usuários mais rápida e permite que os usuários do locatário façam login na conta do locatário usando credenciais familiares.

Configure a federação de identidade para o Gerenciador do Locatário

Você pode configurar a federação de identidade para o Gerenciador do locatário se quiser que grupos de locatários e usuários sejam gerenciados em outro sistema, como o ative Directory, o Azure ative Directory (Azure AD), o OpenLDAP ou o Oracle Directory Server.

Antes de começar

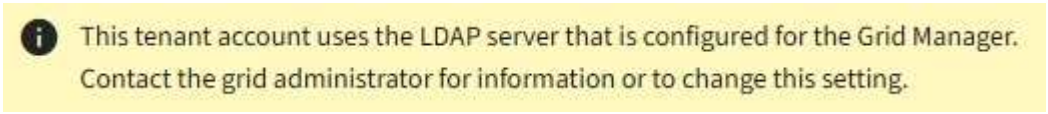
- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Você está usando o ative Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.

  Se pretender utilizar um serviço LDAP v3 que não esteja listado, contacte o suporte técnico.

- Se você pretende usar o OpenLDAP, você deve configurar o servidor OpenLDAP. Diretrizes para configurar o servidor OpenLDAPConsulte .
- Se você pretende usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade deve estar usando TLS 1,2 ou 1,3. "Cifras suportadas para conexões TLS de saída"Consulte .

Sobre esta tarefa

Se você pode configurar um serviço de federação de identidade para seu locatário depende de como sua conta de locatário foi configurada. Seu locatário pode compartilhar o serviço de federação de identidade configurado para o Gerenciador de Grade. Se você vir essa mensagem ao acessar a página Federação de identidade, não será possível configurar uma origem de identidade federada separada para esse locatário.

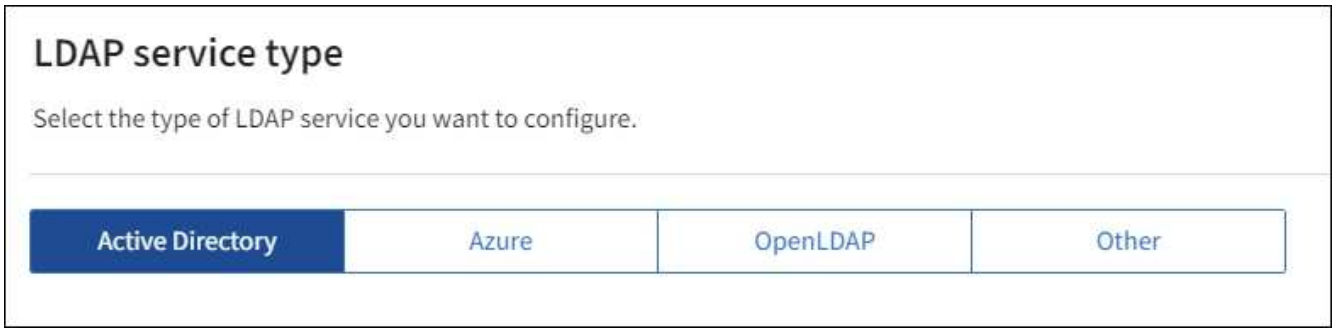


Introduza a configuração

Ao configurar a federação de identificação, você fornece os valores que o StorageGRID precisa para se conetar a um serviço LDAP.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **federação de identidade**.
2. Selecione **Ativar federação de identidade**.
3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.



Selecione **Other** para configurar valores para um servidor LDAP que use o Oracle Directory Server.

4. Se você selecionou **Other**, preencha os campos na seção atributos LDAP. Caso contrário, vá para a próxima etapa.
   - **Nome exclusivo do usuário**: O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `uid` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `uid`.
   - **UUID de usuário**: O nome do atributo que contém o identificador exclusivo permanente de um usuário LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
   - **Group Unique Name**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `cn` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `cn`.
   - **Group UUID**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
5. Para todos os tipos de serviço LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias na secção Configurar servidor LDAP.
   - **Nome de host**: O nome de domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
   - **Port**: A porta usada para se conetar ao servidor LDAP.

     A porta padrão para STARTTLS é 389 e a porta padrão para LDAPS é 636. No entanto, você pode usar qualquer porta desde que seu firewall esteja configurado corretamente.

   - **Nome de usuário**: O caminho completo do nome distinto (DN) para o usuário que se conetará ao servidor LDAP.

     No ative Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

     O usuário especificado deve ter permissão para listar grupos e usuários e para acessar os seguintes atributos:

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`

- `cn`
- `memberOf` ou `isMemberOf`
- **Ative Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, E `userPrincipalName`
- **Azure**: `accountEnabled` E. `userPrincipalName`

◦ **Senha**: A senha associada ao nome de usuário.

> Se você alterar a senha no futuro, você deve atualizá-la nesta página.

◦ **Group base DN**: O caminho completo do nome distinto (DN) para uma subárvore LDAP que você deseja pesquisar grupos. No exemplo do ative Directory (abaixo), todos os grupos cujo Nome distinto é relativo ao DN base (DC-StorageGRID,DC-com) podem ser usados como grupos federados.

> Os valores **Group unique name** devem ser exclusivos dentro do **Group base DN** a que pertencem.

◦ **DN da base do usuário**: O caminho completo do nome distinto (DN) de uma subárvore LDAP que você deseja pesquisar por usuários.

> Os valores **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN da base de usuários** a que pertencem.

◦ **Bind username format** (opcional): O padrão de username padrão StorageGRID deve ser usado se o padrão não puder ser determinado automaticamente.

É recomendado fornecer **Bind username format** porque pode permitir que os usuários façam login se o StorageGRID não conseguir vincular-se à conta de serviço.

Introduza um destes padrões:

- **Padrão UserPrincipalName (ative Directory e Azure)**: `[USERNAME]@*example*.com`
- * Padrão de nome de logon de nível inferior (ative Directory e Azure)*: `*example*\[USERNAME]`
- * Padrão de nome distinto *: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

Inclua **[USERNAME]** exatamente como escrito.

6. Na seção Transport Layer Security (TLS), selecione uma configuração de segurança.
◦ **Use STARTTLS**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para ative Directory, OpenLDAP ou outro, mas esta opção não é suportada para o Azure.
◦ **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar essa opção para o Azure.
◦ **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido. Esta opção não é suportada para o Azure.

> O uso da opção **não usar TLS** não é suportado se o servidor do ative Directory forçar a assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

7. Se você selecionou STARTTLS ou LDAPS, escolha o certificado usado para proteger a conexão.
   - **Use o certificado CA do sistema operacional**: Use o certificado CA de grade padrão instalado no sistema operacional para proteger conexões.
   - **Use certificado CA personalizado**: Use um certificado de segurança personalizado.

     Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

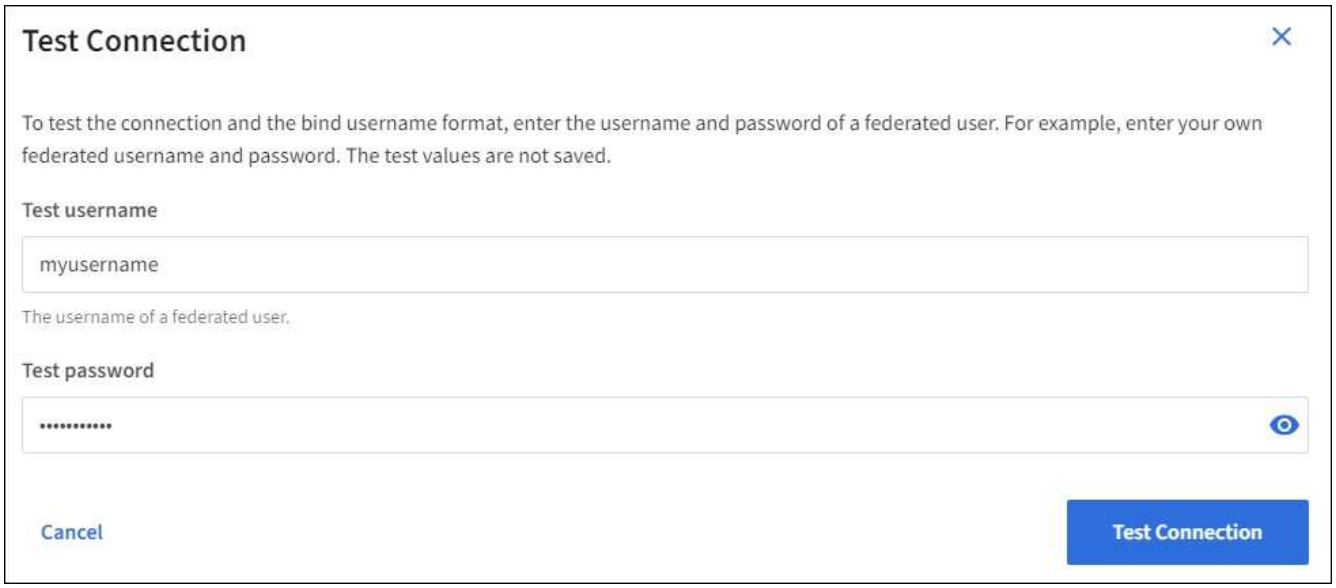
Teste a conexão e salve a configuração

Depois de introduzir todos os valores, tem de testar a ligação antes de poder guardar a configuração. O StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato de nome de usuário de vinculação, se você tiver fornecido uma.

Passos

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
   - É apresentada uma mensagem "Test Connection successful" (testar ligação bem-sucedida) se as definições de ligação forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - É apresentada uma mensagem "não foi possível estabelecer ligação de teste" se as definições da ligação forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você tiver fornecido um formato de nome de usuário do BIND, insira o nome de usuário e a senha de um usuário federado válido.

   Por exemplo, insira seu próprio nome de usuário e senha. Não inclua carateres especiais no nome de usuário, como em ou /.



   - É apresentada uma mensagem "Test Connection successful" (testar ligação bem-sucedida) se as definições de ligação forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem de erro é exibida se as configurações de conexão, o formato de nome de usuário de ligação ou o nome de usuário de teste e a senha forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar a sincronização com a fonte de identidade

O sistema StorageGRID sincroniza periodicamente grupos federados e usuários da origem da identidade. Você pode forçar o início da sincronização se quiser ativar ou restringir as permissões de usuário o mais rápido possível.

Passos

1. Vá para a página de federação de identidade.
2. Selecione **servidor de sincronização** na parte superior da página.

   O processo de sincronização pode demorar algum tempo, dependendo do ambiente.

   O alerta **Falha na sincronização da federação de identidade** é acionado se houver um problema na sincronização de grupos federados e usuários da origem da identidade.

Desativar a federação de identidade

Você pode desativar temporariamente ou permanentemente a federação de identidade para grupos e usuários. Quando a federação de identidade está desativada, não há comunicação entre o StorageGRID e a fonte de identidade. No entanto, todas as configurações que você configurou são mantidas, permitindo que você reative facilmente a federação de identidade no futuro.

Sobre esta tarefa

Antes de desativar a federação de identidade, você deve estar ciente do seguinte:

- Os utilizadores federados não poderão iniciar sessão.
- Os usuários federados que estiverem conetados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a origem da identidade não ocorrerá e os alertas não serão gerados para contas que não tenham sido sincronizadas.
- A caixa de seleção **Ativar federação de identidade** será desativada se o logon único (SSO) estiver definido como **ativado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. "Desative o logon único"Consulte .

Passos

1. Vá para a página de federação de identidade.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.

Diretrizes para configurar o servidor OpenLDAP

Se você quiser usar um servidor OpenLDAP para federação de identidade, você deve configurar configurações específicas no servidor OpenLDAP.

Para fontes de identidade que não são ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso S3 aos usuários que estão desativados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 para o usuário ou remova o usuário de todos os grupos.

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para a manutenção da associação de grupo reverso no "Documentação do OpenLDAP: Guia do administrador da versão 2,4".

Indexação

Você deve configurar os seguintes atributos OpenLDAP com as palavras-chave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Além disso, certifique-se de que os campos mencionados na ajuda do Nome de usuário sejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção da associação de grupo reverso no "Documentação do OpenLDAP: Guia do administrador da versão 2,4".

Gerenciar grupos de locatários

Crie grupos para um locatário do S3

Você pode gerenciar permissões para S3 grupos de usuários importando grupos federados ou criando grupos locais.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se você pretende importar um grupo federado, o "federação de identidade configurada", e o grupo federado já existe na origem de identidade configurada.
- Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para "clonar grupos de locatários e usuários", e você estará conetado à grade de origem do locatário.

Acesse o assistente criar grupo

Como primeira etapa, acesse o assistente criar grupo.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Se sua conta de locatário tiver a permissão **Use Grid Federation Connection**, confirme se um banner azul aparece, indicando que novos grupos criados nessa grade serão clonados para o mesmo locatário na outra grade na conexão. Se este banner não aparecer, você pode estar conetado à grade de destino do locatário.

3. Selecione **criar grupo**.

Escolha um tipo de grupo

Você pode criar um grupo local ou importar um grupo federado.

Passos

1. Selecione a guia **local group** para criar um grupo local ou selecione a guia **Federated group** para importar um grupo da origem de identidade configurada anteriormente.

   Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários pertencentes a grupos locais não poderão fazer login no Gerenciador de locatários, embora possam usar aplicativos clientes para gerenciar os recursos do locatário, com base nas permissões de grupo.

2. Introduza o nome do grupo.
   - **Local group**: Insira um nome de exibição e um nome exclusivo. Pode editar o nome de apresentação mais tarde.

     Se sua conta de locatário tiver a permissão **Use Grid Federation Connection**, ocorrerá um erro de clonagem se o mesmo **nome exclusivo** já existir para o locatário na grade de destino.

   - **Federated group**: Insira o nome exclusivo. Para o ative Directory, o nome exclusivo é o nome associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.
3. Selecione **continuar**.

Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Gerenciador de inquilinos e na API de gerenciamento de inquilinos.

Passos

1. Para **modo de acesso**, selecione uma das seguintes opções:
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do locatário e gerenciar a configuração do locatário.

- **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar nenhuma operação no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. Os usuários locais só de leitura podem alterar suas próprias senhas.

> Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como somente leitura, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

2. Selecione uma ou mais permissões para este grupo.

   "Permissões de gerenciamento do locatário"Consulte .

3. Selecione **continuar**.

Defina a política de grupo S3

A política de grupo determina quais permissões de acesso S3 os usuários terão.

Passos

1. Selecione a política que pretende utilizar para este grupo.

Política de grupo	Descrição
Sem acesso S3	Padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
Acesso somente leitura	Os usuários deste grupo têm acesso somente leitura a recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
Acesso total	Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
Mitigação de ransomware	Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários deste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que têm o controle de versão de objeto habilitado. Os usuários do Gerenciador de locatários que têm a permissão **Gerenciar todos os buckets** podem substituir essa política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação multifator (MFA), onde disponível.

Política de grupo	Descrição
Personalizado	Os usuários do grupo recebem as permissões especificadas na caixa de texto.

2. Se você selecionou **Personalizado**, digite a política de grupo. Cada política de grupo tem um limite de tamanho de 5.120 bytes. Você deve inserir uma string formatada JSON válida.

   Para obter informações detalhadas sobre políticas de grupo, incluindo sintaxe de idioma e exemplos, "Exemplo de políticas de grupo"consulte .

3. Se estiver criando um grupo local, selecione **continuar**. Se você estiver criando um grupo federado, selecione **criar grupo** e **concluir**.

Adicionar utilizadores (apenas grupos locais)

Você pode salvar o grupo sem adicionar usuários ou, opcionalmente, adicionar usuários locais que já existem.

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, os usuários selecionados ao criar um grupo local na grade de origem não serão incluídos quando o grupo for clonado para a grade de destino. Por esse motivo, não selecione usuários quando você criar o grupo. Em vez disso, selecione o grupo quando você criar os usuários.

Passos

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.
2. Selecione **criar grupo** e **concluir**.

   O grupo criado aparece na lista de grupos.

   Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver na grade de origem do locatário, o novo grupo será clonado para a grade de destino do locatário. **Success** aparece como **status de clonagem** na seção Visão geral da página de detalhes do grupo.

Crie grupos para um locatário Swift

Você pode gerenciar permissões de acesso para uma conta de locatário Swift importando grupos federados ou criando grupos locais. Pelo menos um grupo deve ter a permissão Swift Administrator, que é necessária para gerenciar os contentores e objetos para uma conta Swift.

> O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se você pretende importar um grupo federado, o "federação de identidade configurada", e o grupo federado já existe na origem de identidade configurada.

Acesse o assistente criar grupo

Passos

Como primeira etapa, acesse o assistente criar grupo.

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Selecione **criar grupo**.

Escolha um tipo de grupo

Você pode criar um grupo local ou importar um grupo federado.

Passos

1. Selecione a guia **local group** para criar um grupo local ou selecione a guia **Federated group** para importar um grupo da origem de identidade configurada anteriormente.

   Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários pertencentes a grupos locais não poderão fazer login no Gerenciador de locatários, embora possam usar aplicativos clientes para gerenciar os recursos do locatário, com base nas permissões de grupo.

2. Introduza o nome do grupo.
   - **Local group**: Insira um nome de exibição e um nome exclusivo. Pode editar o nome de apresentação mais tarde.
   - **Federated group**: Insira o nome exclusivo. Para o ative Directory, o nome exclusivo é o nome associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.
3. Selecione **continuar**.

Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Gerenciador de inquilinos e na API de gerenciamento de inquilinos.

Passos

1. Para **modo de acesso**, selecione uma das seguintes opções:
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do locatário e gerenciar a configuração do locatário.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar nenhuma operação no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. Os usuários locais só de leitura podem alterar suas próprias senhas.

     > Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como somente leitura, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

2. Marque a caixa de seleção **Root Access** se os usuários do grupo precisarem fazer login na API de Gerenciamento de Locatário ou Gerenciamento de Locatário.
3. Selecione **continuar**.

Defina a política de grupo Swift

Os usuários Swift precisam de permissão de administrador para se autenticar na API REST do Swift para criar contentores e ingerir objetos.

1. Marque a caixa de seleção **Swift administrator** se os usuários do grupo precisarem usar a Swift REST API para gerenciar contentores e objetos.
2. Se estiver criando um grupo local, selecione **continuar**. Se você estiver criando um grupo federado, selecione **criar grupo** e **concluir**.

Adicionar utilizadores (apenas grupos locais)

Você pode salvar o grupo sem adicionar usuários ou, opcionalmente, adicionar usuários locais que já existem.

Passos

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.

   Se ainda não tiver criado utilizadores locais, pode adicionar este grupo ao utilizador na página utilizadores. "Gerenciar usuários locais"Consulte .

2. Selecione **criar grupo** e **concluir**.

   O grupo criado aparece na lista de grupos.

Permissões de gerenciamento do locatário

Antes de criar um grupo de inquilinos, considere quais permissões você deseja atribuir a esse grupo. As permissões de gerenciamento do locatário determinam quais tarefas os usuários podem executar usando o Gerenciador do locatário ou a API de gerenciamento do locatário. Um usuário pode pertencer a um ou mais grupos. As permissões são cumulativas se um usuário pertencer a vários grupos.

Para fazer login no Gerenciador do Locatário ou usar a API de Gerenciamento do Locatário, os usuários devem pertencer a um grupo que tenha pelo menos uma permissão. Todos os usuários que podem entrar podem executar as seguintes tarefas:

- Visualizar o painel de instrumentos
- Alterar sua própria senha (para usuários locais)

Para todas as permissões, a configuração do modo de acesso do grupo determina se os usuários podem alterar configurações e executar operações ou se eles podem exibir somente as configurações e recursos relacionados.

> Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como somente leitura, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

Pode atribuir as seguintes permissões a um grupo. Observe que S3 locatários e locatários Swift têm permissões de grupo diferentes.

Permissão	Descrição	Detalhes
Acesso à raiz	Fornece acesso total ao Gerenciador do Locatário e à API de Gerenciamento do Locatário.	Os usuários Swift devem ter permissão de acesso root para entrar na conta do locatário.
Administrador	Apenas inquilinos Swift. Fornece acesso total aos contentores e objetos Swift para essa conta de locatário	Os usuários Swift devem ter a permissão Swift Administrator para executar qualquer operação com a SWIFT REST API.
Gerencie suas próprias credenciais S3	Permite que os usuários criem e removam suas próprias chaves de acesso S3.	Os utilizadores que não têm esta permissão não veem a opção de menu **STORAGE (S3)** > **My S3 Access Keys**.
Veja todos os baldes	**S3 locatários**: Permite que os usuários visualizem todos os buckets e configurações de bucket. **Swift tenants**: Permite que os usuários do Swift visualizem todos os contentores e configurações de contentores usando a API de Gerenciamento do locatário.	Os usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu **Buckets**. Essa permissão é substituída pela permissão Gerenciar todos os buckets. Não afeta as políticas de grupo ou bucket S3 usadas por clientes S3 ou console S3. Você só pode atribuir essa permissão aos grupos Swift a partir da API de Gerenciamento de Tenant. Não é possível atribuir essa permissão a grupos Swift usando o Gerenciador de Locações.
Gerenciar todos os buckets	**S3 inquilinos**: Permite que os usuários usem o Gerenciador do locatário e a API de gerenciamento do locatário para criar e excluir buckets do S3 e gerenciar as configurações de todos os buckets do S3 na conta do locatário, independentemente das políticas de bucket ou grupo do S3. **Swift tenants**: Permite que usuários Swift controlem a consistência para contentores Swift usando a API de Gerenciamento de inquilinos.	Os usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu **Buckets**. Esta permissão substitui a permissão Exibir todos os buckets. Não afeta as políticas de grupo ou bucket S3 usadas por clientes S3 ou console S3. Você só pode atribuir essa permissão aos grupos Swift a partir da API de Gerenciamento de Tenant. Não é possível atribuir essa permissão a grupos Swift usando o Gerenciador de Locações.

Permissão	Descrição	Detalhes
Gerenciar endpoints	Permite que os usuários usem o Gerenciador do Locatário ou a API de Gerenciamento do Locatário para criar ou editar endpoints de serviço da plataforma, que são usados como o destino dos serviços da plataforma StorageGRID.	Os usuários que não têm essa permissão não veem a opção de menu **endpoints de serviços da plataforma**.
Use a guia Console do S3	Quando combinada com a permissão Exibir todos os buckets ou Gerenciar todos os buckets, permite que os usuários visualizem e gerenciem objetos na guia Console do S3 na página de detalhes de um bucket.	

Gerenciar grupos

Gerencie seus grupos de locatários conforme necessário para exibir, editar ou duplicar um grupo e muito mais.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

Ver ou editar grupo

Você pode exibir e editar as informações básicas e os detalhes de cada grupo.

Passos

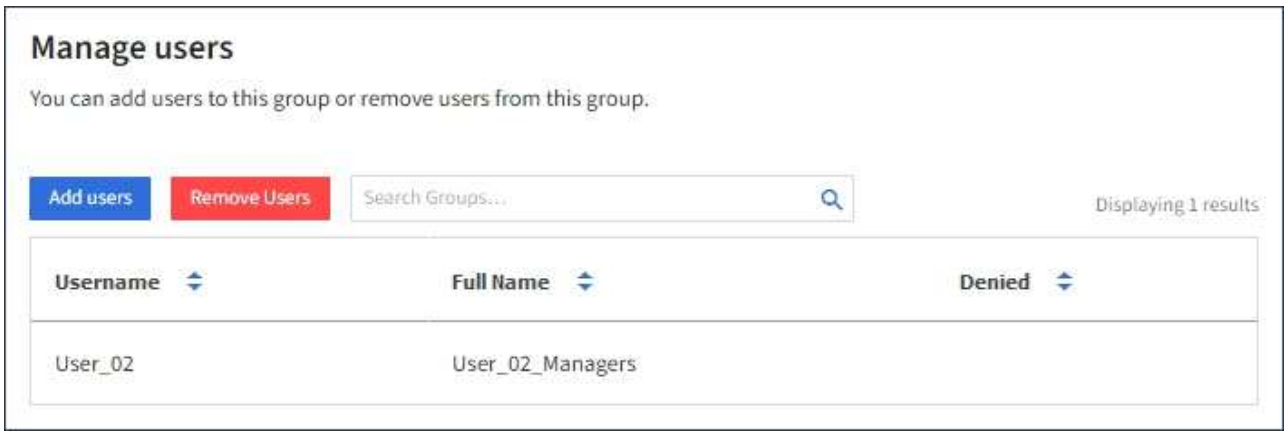
1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Revise as informações fornecidas na página grupos, que lista informações básicas para todos os grupos locais e federados dessa conta de locatário.

   Se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando grupos na grade de origem do locatário:

   - Uma mensagem de banner indica que, se você editar ou remover um grupo, suas alterações não serão sincronizadas com a outra grade.
   - Conforme necessário, uma mensagem de banner indica se os grupos não foram clonados ao locatário na grade de destino. Você pode tente novamente um clone de grupo que falhou.
3. Se quiser alterar o nome do grupo:
   a. Selecione a caixa de verificação para o grupo.
   b. Selecione **ações** > **Editar nome do grupo**.
   c. Introduza o novo nome.
   d. Selecione **Salvar alterações.**
4. Se você quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes procedimentos:
   - Selecione o nome do grupo.

- Marque a caixa de seleção para o grupo e selecione **ações** > **Exibir detalhes do grupo**.

5. Revise a seção Visão geral, que mostra as seguintes informações para cada grupo:
   - Nome do visor
   - Nome único
   - Tipo
   - Modo de acesso
   - Permissões
   - S3 Política
   - Número de usuários neste grupo
   - Campos adicionais se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando o grupo na grade de origem do locatário:
     - Status da clonagem, **sucesso** ou **falha**
     - Um banner azul indicando que, se você editar ou excluir esse grupo, suas alterações não serão sincronizadas com a outra grade.
6. Edite as definições do grupo conforme necessário. "Crie grupos para um locatário do S3"Consulte e "Crie grupos para um locatário Swift" para obter detalhes sobre o que introduzir.
   a. Na seção Visão geral , altere o nome de exibição selecionando o nome ou o ícone de edição .
   b. Na guia **permissões de grupo**, atualize as permissões e selecione **Salvar alterações**.
   c. Na guia **Política de grupo**, faça quaisquer alterações e selecione **Salvar alterações**.
      - Se você estiver editando um grupo S3, opcionalmente, selecione uma política de grupo S3 diferente ou insira a string JSON para uma política personalizada, conforme necessário.
      - Se você estiver editando um grupo Swift, opcionalmente selecione ou desmarque a caixa de seleção **Administrador Swift**.
7. Para adicionar um ou mais usuários locais existentes ao grupo:
   a. Selecione a guia usuários.



   b. Selecione **Adicionar usuários**.
   c. Selecione os usuários existentes que você deseja adicionar e selecione **Adicionar usuários**.

      Uma mensagem de sucesso aparece no canto superior direito.

8. Para remover usuários locais do grupo:

a. Selecione a guia usuários.
b. Selecione **Remover usuários**.
c. Selecione os usuários que deseja remover e selecione **Remover usuários**.

   Uma mensagem de sucesso aparece no canto superior direito.

9. Confirme se selecionou **Guardar alterações** para cada secção alterada.

Grupo duplicado

Você pode duplicar um grupo existente para criar novos grupos mais rapidamente.

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você duplicar um grupo da grade de origem do locatário, o grupo duplicado será clonado para a grade de destino do locatário.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Marque a caixa de seleção do grupo que deseja duplicar.
3. Selecione **ações** > **grupo duplicado**.
4. "Crie grupos para um locatário do S3"Consulte ou "Crie grupos para um locatário Swift" para obter detalhes sobre o que introduzir.
5. Selecione **criar grupo**.

Repetir o clone do grupo

Para tentar novamente um clone que falhou:

1. Selecione cada grupo que indica *(Falha na clonagem)* abaixo do nome do grupo.
2. Selecione **ações** > **Clone groups**.
3. Veja o status da operação de clone na página de detalhes de cada grupo que você está clonando.

Para obter informações adicionais, "Clonar grupos de locatários e usuários"consulte .

Exclua um ou mais grupos

Pode eliminar um ou mais grupos. Quaisquer usuários que pertençam apenas a um grupo que seja excluído não poderão mais entrar no Gerenciador do locatário ou usar a conta do locatário.

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você excluir um grupo, o StorageGRID não excluirá o grupo correspondente na outra grade. Se você precisar manter essas informações em sincronia, exclua o mesmo grupo de ambas as grades.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Selecione a caixa de verificação para cada grupo que pretende eliminar.
3. Selecione **ações** > **Excluir grupo** ou **ações** > **Excluir grupos**.

   É apresentada uma caixa de diálogo de confirmação.

4. Selecione **Excluir grupo** ou **Excluir grupos**.

Gerenciar usuários locais

Você pode criar usuários locais e atribuí-los a grupos locais para determinar quais recursos esses usuários podem acessar. O Gerenciador do Tenant inclui um usuário local predefinido, chamado "root". Embora você possa adicionar e remover usuários locais, você não pode remover o usuário raiz.

> Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários locais não poderão fazer login no Gerenciador do Locatário ou na API de Gerenciamento do Locatário, embora possam usar aplicativos cliente para acessar os recursos do locatário, com base nas permissões de grupo.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para "clonar grupos de locatários e usuários", e você estará conetado à grade de origem do locatário.

Crie um usuário local

Você pode criar um usuário local e atribuí-lo a um ou mais grupos locais para controlar suas permissões de acesso.

S3 os usuários que não pertencem a nenhum grupo não têm permissões de gerenciamento ou políticas de grupo S3 aplicadas a eles. Esses usuários podem ter acesso ao bucket do S3 concedido por meio de uma política de bucket.

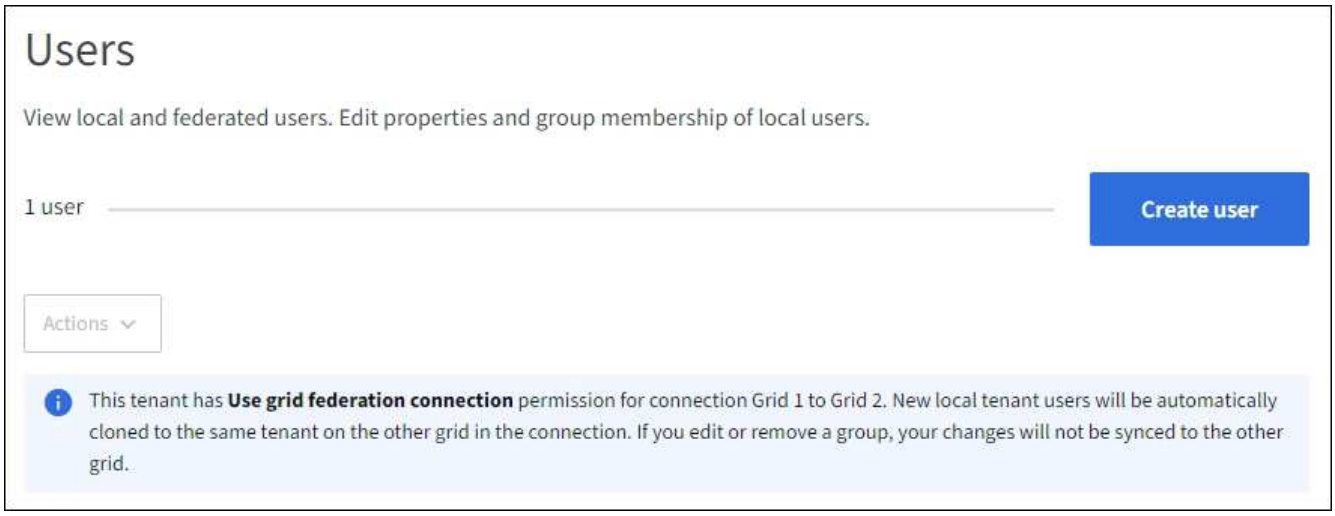
Os usuários Swift que não pertencem a nenhum grupo não têm permissões de gerenciamento ou acesso ao contentor Swift.

Acesse o assistente criar usuário

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.

   Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, um banner azul indica que essa é a grade de origem do locatário. Todos os usuários locais que você criar nesta grade serão clonados para a outra grade na conexão.



2. Selecione **criar usuário**.

Introduza as credenciais

Passos

1. Para a etapa **Insira as credenciais do usuário**, preencha os campos a seguir.

Campo	Descrição
Nome completo	O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo.
Nome de utilizador	O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados. **Nota**: Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, ocorrerá um erro de clonagem se o mesmo **Username** já existir para o locatário na grade de destino.
Senha e confirmar senha	A senha que o usuário usará inicialmente ao fazer login.
Negar acesso	Selecione **Sim** para impedir que esse usuário faça login na conta de locatário, mesmo que ele ainda possa pertencer a um ou mais grupos. Por exemplo, selecione **Sim** para suspender temporariamente a capacidade de um usuário fazer login.

2. Selecione **continuar**.

Atribuir a grupos

Passos

1. Atribua o usuário a um ou mais grupos locais para determinar quais tarefas podem ser executadas.

   Atribuir um usuário a grupos é opcional. Se preferir, você pode selecionar usuários ao criar ou editar grupos.

Os usuários que não pertencem a nenhum grupo não terão permissões de gerenciamento. As permissões são cumulativas. Os usuários terão todas as permissões para todos os grupos aos quais pertencem. "Permissões de gerenciamento do locatário"Consulte .

2. Selecione **criar usuário**.

   Se sua conta de locatário tiver a permissão **Use Grid Federation Connection** e você estiver na grade de origem do locatário, o novo usuário local será clonado para a grade de destino do locatário. **Success** aparece como **status de clonagem** na seção Visão geral da página de detalhes do usuário.

3. Selecione **Finish** para retornar à página usuários.

Ver ou editar utilizador local

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Revise as informações fornecidas na página usuários, que lista informações básicas para todos os usuários locais e federados dessa conta de locatário.

   Se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando o usuário na grade de origem do locatário:

   - Uma mensagem de banner indica que, se você editar ou remover um usuário, suas alterações não serão sincronizadas com a outra grade.
   - Conforme necessário, uma mensagem de banner indica se os usuários não foram clonados para o locatário na grade de destino. Você pode tente novamente um clone de usuário que falhou.
3. Se pretender alterar o nome completo do utilizador:
   a. Selecione a caixa de verificação para o utilizador.
   b. Selecione **ações** > **Editar nome completo**.
   c. Introduza o novo nome.
   d. Selecione **Salvar alterações.**
4. Se você quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes procedimentos:
   - Selecione o nome de utilizador.
   - Marque a caixa de seleção para o usuário e selecione **ações** > **Exibir detalhes do usuário**.
5. Revise a seção Visão geral, que mostra as seguintes informações para cada usuário:
   - Nome completo
   - Nome de utilizador
   - Tipo de utilizador
   - Acesso negado
   - Modo de acesso
   - Associação ao grupo
   - Campos adicionais se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando o usuário na grade de origem do locatário:
     - Status da clonagem, **sucesso** ou **falha**
     - Um banner azul indicando que, se você editar este usuário, suas alterações não serão

sincronizadas com a outra grade.

6. Edite as definições do utilizador conforme necessário. Consulte Criar utilizador local para obter detalhes sobre o que introduzir.
   a. Na seção Visão geral , altere o nome completo selecionando o nome ou o ícone de edição .

      Você não pode alterar o nome de usuário.

   b. Na guia **Senha**, altere a senha do usuário e selecione **Salvar alterações**.
   c. Na guia **Access**, selecione **não** para permitir que o usuário faça login ou selecione **Sim** para impedir que o usuário faça login. Em seguida, selecione **Salvar alterações**.
   d. Na guia **teclas de acesso**, selecione **criar chave** e siga as instruções para "Criando as chaves de acesso S3 de outro usuário".
   e. Na guia **grupos**, selecione **Editar grupos** para adicionar o usuário aos grupos ou remover o usuário dos grupos. Em seguida, selecione **Salvar alterações**.
7. Confirme se selecionou **Guardar alterações** para cada secção alterada.

Duplicar utilizador local

Você pode duplicar um usuário local para criar um novo usuário mais rapidamente.

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você duplicar um usuário da grade de origem do locatário, o usuário duplicado será clonado para a grade de destino do locatário.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Selecione a caixa de verificação para o utilizador que pretende duplicar.
3. Selecione **ações** > **usuário duplicado**.
4. Consulte Criar utilizador local para obter detalhes sobre o que introduzir.
5. Selecione **criar usuário**.

Repetir o clone do usuário

Para tentar novamente um clone que falhou:

1. Selecione cada usuário que indica *(Falha na clonagem)* abaixo do nome de usuário.
2. Selecione **ações** > **Clone usuários**.
3. Veja o status da operação de clone na página de detalhes de cada usuário que você está clonando.

Para obter informações adicionais, "Clonar grupos de locatários e usuários"consulte .

Exclua um ou mais usuários locais

Você pode excluir permanentemente um ou mais usuários locais que não precisam mais acessar a conta de locatário do StorageGRID.

Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você excluir um usuário local, o StorageGRID não excluirá o usuário correspondente na outra grade. Se você precisar manter essas informações em sincronia, você deve excluir o mesmo usuário de ambas as grades.

Você deve usar a origem de identidade federada para excluir usuários federados.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Selecione a caixa de verificação para cada utilizador que pretende eliminar.
3. Selecione **ações** > **Excluir usuário** ou **ações** > **Excluir usuários**.

   É apresentada uma caixa de diálogo de confirmação.

4. Selecione **Excluir usuário** ou **Excluir usuários**.

Gerenciar S3 chaves de acesso

Gerenciar S3 chaves de acesso

Cada usuário de uma conta de locatário do S3 deve ter uma chave de acesso para armazenar e recuperar objetos no sistema StorageGRID. Uma chave de acesso consiste em um ID de chave de acesso e uma chave de acesso secreta.

As chaves de acesso S3 podem ser gerenciadas da seguinte forma:

- Os usuários que têm a permissão **Gerenciar suas próprias credenciais S3** podem criar ou remover suas próprias chaves de acesso S3.
- Os usuários que têm a permissão **Root Access** podem gerenciar as chaves de acesso para a conta raiz do S3 e todos os outros usuários. As chaves de acesso root fornecem acesso total a todos os buckets e objetos para o locatário, a menos que explicitamente desabilitado por uma política de bucket.

O StorageGRID suporta a autenticação Signature versão 2 e Signature versão 4. O acesso entre contas não é permitido, a menos que explicitamente habilitado por uma política de bucket.

Crie suas próprias chaves de acesso S3

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, você poderá criar suas próprias chaves de acesso do S3. Você precisa ter uma chave de acesso para acessar seus buckets e objetos.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie suas próprias credenciais S3 ou permissão de acesso root".

Sobre esta tarefa

Você pode criar uma ou mais chaves de acesso S3 que permitem criar e gerenciar buckets para sua conta de locatário. Depois de criar uma nova chave de acesso, atualize a aplicação com a sua nova ID de chave de

acesso e chave de acesso secreta. Para segurança, não crie mais chaves do que você precisa e exclua as chaves que você não está usando. Se você tiver apenas uma chave e ela estiver prestes a expirar, crie uma nova chave antes que a antiga expire e, em seguida, exclua a antiga.

Cada chave pode ter um tempo de expiração específico ou nenhuma expiração. Siga estas diretrizes para o tempo de expiração:

- Defina um tempo de expiração para que suas chaves limitem seu acesso a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a chave de acesso secreta forem acidentalmente expostos. As chaves expiradas são removidas automaticamente.
- Se o risco de segurança em seu ambiente for baixo e você não precisar criar periodicamente novas chaves, você não precisa definir um tempo de expiração para suas chaves. Se você decidir mais tarde criar novas chaves, exclua as chaves antigas manualmente.

> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **ARMAZENAMENTO (S3)** > **as minhas chaves de acesso**.

   A página Minhas chaves de acesso é exibida e lista todas as chaves de acesso existentes.

2. Selecione **criar chave**.
3. Execute um dos seguintes procedimentos:
   - Selecione **não defina um tempo de expiração** para criar uma chave que não expirará. (Predefinição)
   - Selecione **defina um tempo de expiração** e defina a data e a hora de expiração.

     > A data de validade pode ser um máximo de cinco anos a partir da data atual. O tempo de expiração pode ser um mínimo de um minuto a partir do tempo atual.

4. Selecione **criar chave de acesso**.

   A caixa de diálogo Download Access Key (Transferir chave de acesso) é exibida, listando o ID da chave de acesso e a chave de acesso secreta.

5. Copie o ID da chave de acesso e a chave de acesso secreta para um local seguro ou selecione **Transferir .csv** para guardar um ficheiro de folha de cálculo que contenha a ID da chave de acesso e a chave de acesso secreta.

   > Não feche esta caixa de diálogo até que você tenha copiado ou baixado essas informações. Não é possível copiar ou transferir chaves depois de a caixa de diálogo ter sido fechada.

6. Selecione **Finish**.

   A nova chave está listada na página Minhas chaves de acesso.

7. Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, opcionalmente use a API de Gerenciamento do locatário para clonar manualmente as chaves de acesso S3 do locatário na grade

de origem para o locatário na grade de destino. "Clonar chaves de acesso S3 usando a API"Consulte .

Veja as suas teclas de acesso S3

Se você estiver usando um locatário do S3 e tiver o "permissão apropriada", você poderá exibir uma lista das chaves de acesso do S3. Você pode classificar a lista por tempo de expiração, para que você possa determinar quais chaves expirarão em breve. Conforme necessário, você pode "crie novas chaves" ou "eliminar chaves"não está mais usando.

> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem as credenciais Gerenciar suas próprias credenciais S3 "permissão".

Passos

1. Selecione **ARMAZENAMENTO (S3)** > **as minhas chaves de acesso**.
2. Na página Minhas chaves de acesso, classifique todas as chaves de acesso existentes por **tempo de expiração** ou **ID da chave de acesso**.
3. Conforme necessário, crie novas chaves ou exclua quaisquer chaves que você não esteja mais usando.

   Se você criar novas chaves antes que as chaves existentes expirem, você pode começar a usar as novas chaves sem perder temporariamente o acesso aos objetos na conta.

   As chaves expiradas são removidas automaticamente.

Elimine as suas próprias chaves de acesso S3

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, você poderá excluir suas próprias chaves de acesso do S3. Depois que uma chave de acesso for excluída, ela não poderá mais ser usada para acessar os objetos e buckets na conta do locatário.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você tem o "Gerencie sua própria permissão de credenciais S3".

> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **ARMAZENAMENTO (S3)** > **as minhas chaves de acesso**.
2. Na página Minhas chaves de acesso, marque a caixa de seleção para cada chave de acesso que deseja remover.
3. Selecione **Delete key**.
4. Na caixa de diálogo de confirmação, selecione **Delete key**.

   Uma mensagem de confirmação aparece no canto superior direito da página.

Crie as chaves de acesso S3 de outro usuário

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, poderá criar chaves de acesso do S3 para outros usuários, como aplicativos que precisam de acesso a buckets e objetos.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

Sobre esta tarefa

Você pode criar uma ou mais chaves de acesso S3 para outros usuários para que eles possam criar e gerenciar buckets para sua conta de locatário. Depois de criar uma nova chave de acesso, atualize a aplicação com a nova ID da chave de acesso e chave de acesso secreta. Para segurança, não crie mais chaves do que o usuário precisa e exclua as chaves que não estão sendo usadas. Se você tiver apenas uma chave e ela estiver prestes a expirar, crie uma nova chave antes que a antiga expire e, em seguida, exclua a antiga.

Cada chave pode ter um tempo de expiração específico ou nenhuma expiração. Siga estas diretrizes para o tempo de expiração:

- Defina um tempo de expiração para as teclas para limitar o acesso do usuário a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a chave de acesso secreta forem acidentalmente expostos. As chaves expiradas são removidas automaticamente.
- Se o risco de segurança em seu ambiente for baixo e você não precisar criar periodicamente novas chaves, você não precisa definir um tempo de expiração para as chaves. Se você decidir mais tarde criar novas chaves, exclua as chaves antigas manualmente.

> Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para esse usuário no Gerenciador do locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Selecione o usuário cujas chaves de acesso S3 você deseja gerenciar.

   É apresentada a página de detalhes do utilizador.

3. Selecione **teclas de acesso** e, em seguida, selecione **criar chave**.
4. Execute um dos seguintes procedimentos:
   - Selecione **não defina um tempo de expiração** para criar uma chave que não expire. (Predefinição)
   - Selecione **defina um tempo de expiração** e defina a data e a hora de expiração.

   > A data de validade pode ser um máximo de cinco anos a partir da data atual. O tempo de expiração pode ser um mínimo de um minuto a partir do tempo atual.

5. Selecione **criar chave de acesso**.

   A caixa de diálogo Download Access Key (Transferir chave de acesso) é exibida, listando o ID da chave de acesso e a chave de acesso secreta.

6. Copie o ID da chave de acesso e a chave de acesso secreta para um local seguro ou selecione **Transferir .csv** para guardar um ficheiro de folha de cálculo que contenha a ID da chave de acesso e a chave de acesso secreta.

   > Não feche esta caixa de diálogo até que você tenha copiado ou baixado essas informações. Não é possível copiar ou transferir chaves depois de a caixa de diálogo ter sido fechada.

7. Selecione **Finish**.

   A nova chave está listada na guia teclas de acesso da página de detalhes do usuário.

8. Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, opcionalmente use a API de Gerenciamento do locatário para clonar manualmente as chaves de acesso S3 do locatário na grade de origem para o locatário na grade de destino. "Clonar chaves de acesso S3 usando a API"Consulte .

Veja as S3 chaves de acesso de outro usuário

Se você estiver usando um locatário do S3 e tiver permissões apropriadas, poderá visualizar as chaves de acesso do S3 de outro usuário. Você pode classificar a lista por tempo de expiração para determinar quais chaves expirarão em breve. Conforme necessário, você pode criar novas chaves e excluir chaves que não estão mais em uso.

Antes de começar

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

> Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para esse usuário no Gerenciador do locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Na página usuários, selecione o usuário cujas teclas de acesso S3 você deseja exibir.
3. Na página Detalhes do usuário, selecione **teclas de acesso**.

4. Classifique as chaves por **tempo de expiração** ou **ID da chave de acesso**.
5. Conforme necessário, crie novas chaves e exclua manualmente as chaves que não estiverem mais em uso.

   Se você criar novas chaves antes que as chaves existentes expirem, o usuário pode começar a usar as novas chaves sem perder temporariamente o acesso aos objetos na conta.

   As chaves expiradas são removidas automaticamente.

Informações relacionadas

- "Crie as chaves de acesso S3 de outro usuário"
- "Eliminar as S3 chaves de acesso de outro utilizador"

Exclua as S3 chaves de acesso de outro usuário

Se você estiver usando um locatário S3 e tiver permissões apropriadas, você poderá excluir as chaves de acesso S3 de outro usuário. Depois que uma chave de acesso for excluída, ela não poderá mais ser usada para acessar os objetos e buckets na conta do locatário.

Antes de começar

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

> Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para esse usuário no Gerenciador do locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Na página usuários, selecione o usuário cujas chaves de acesso S3 você deseja gerenciar.
3. Na página Detalhes do usuário, selecione **teclas de acesso** e, em seguida, marque a caixa de seleção para cada chave de acesso que deseja excluir.
4. Selecione **ações** > **Excluir tecla selecionada**.
5. Na caixa de diálogo de confirmação, selecione **Delete key**.

   Uma mensagem de confirmação aparece no canto superior direito da página.

Gerenciar buckets do S3

Crie um bucket do S3

Você pode usar o Gerenciador do locatário para criar buckets do S3 para dados de objetos.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o acesso raiz ou Gerenciar todos os buckets "permissão". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

> As permissões para definir ou modificar as propriedades de bloqueio de objetos S3D de buckets ou objetos podem ser concedidas pelo "política de bucket ou política de grupo".

- Se você planeja habilitar o bloqueio de objeto S3 para um bucket, um administrador de grade ativou a configuração global de bloqueio de objeto S3 para o sistema StorageGRID e revisou os requisitos para buckets e objetos do bloqueio de objeto S3.
- Se cada locatário tiver 5.000 buckets, cada nó de armazenamento na grade tem um mínimo de 64 GB de RAM.

> Cada grade pode ter um máximo de 100.000 baldes.

Acesse o assistente

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione **criar bucket**.

Introduza os detalhes

Passos

1. Introduza os detalhes do balde.

Campo	Descrição
Nome do intervalo	Um nome para o bucket que está em conformidade com estas regras: • Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). • Deve ser compatível com DNS. • Deve conter pelo menos 3 e não mais de 63 carateres. • Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens. • Não deve conter períodos em solicitações de estilo hospedadas virtuais. Os períodos causarão problemas com a verificação do certificado curinga do servidor. Para obter mais informações, consulte "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de bucket" . **Nota**: Não é possível alterar o nome do bucket depois de criar o bucket.

Campo	Descrição
Região	A região do balde. O administrador do StorageGRID gerencia as regiões disponíveis. A região de um bucket pode afetar a política de proteção de dados aplicada a objetos. Por padrão, todos os buckets são criados na `us-east-1` região. **Nota**: Não é possível alterar a região depois de criar o intervalo.

2. Selecione **continuar**.

Gerir definições

Passos

1. Opcionalmente, habilite o controle de versão de objetos para o bucket.

   Ative o controle de versão de objetos se você quiser armazenar todas as versões de cada objeto neste intervalo. Em seguida, você pode recuperar versões anteriores de um objeto, conforme necessário. Você deve habilitar o controle de versão de objetos se o bucket for usado para replicação entre grades.

2. Se a configuração global S3 Object Lock estiver ativada, ative opcionalmente o S3 Object Lock para o bucket armazenar objetos usando um modelo WORM (write-once-read-many).

   Ative o bloqueio de objetos S3D para um bucket somente se você precisar manter objetos por um período de tempo fixo, por exemplo, para atender a certos requisitos regulatórios. S3 Object Lock é uma configuração permanente que ajuda a evitar que objetos sejam excluídos ou substituídos por um período fixo de tempo ou indefinidamente.

   > Depois que a configuração S3 Object Lock estiver ativada para um bucket, ele não poderá ser desativado. Qualquer pessoa com as permissões corretas pode adicionar objetos a esse intervalo que não podem ser alterados. Você pode não ser capaz de excluir esses objetos ou o próprio bucket.

   Se você ativar o bloqueio de objeto S3 para um bucket, o controle de versão do bucket será ativado automaticamente.

3. Se você selecionou **Enable Object Lock** (Ativar bloqueio de objetos S3), opcionalmente, ative **Default retension** (retenção padrão) para este intervalo.

   > O administrador da grade deve dar permissão "Use recursos específicos do S3 Object Lock"ao .

   Quando **retenção padrão** estiver ativada, novos objetos adicionados ao bucket serão automaticamente protegidos contra exclusão ou substituição. A configuração **retenção padrão** não se aplica a objetos que tenham seus próprios períodos de retenção.

   a. Se **retenção padrão** estiver ativada, especifique um **modo de retenção padrão** para o intervalo.

Modo de retenção predefinido	Descrição
Governança	• Os usuários com `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as configurações de retenção. • Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada. • Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto.
Conformidade	• O objeto não pode ser excluído até que sua data de retenção seja alcançada. • O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído. • A data de retenção do objeto não pode ser removida até que essa data seja atingida. **Nota**: O administrador da grade deve permitir que você use o modo de conformidade.

b. Se **retenção padrão** estiver ativada, especifique o **período de retenção padrão** para o intervalo.

   O **período de retenção padrão** indica quanto tempo novos objetos adicionados a esse intervalo devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor menor ou igual ao período máximo de retenção para o locatário, conforme definido pelo administrador da grade.

Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador da grade cria o locatário. Quando você define um período de retenção *default*, ele não pode exceder o valor definido para o período de retenção máximo. Se necessário, peça ao administrador da grade para aumentar ou diminuir o período máximo de retenção.

4. opcionalmente, selecione **Enable Capacity Limit**.

   O limite de capacidade é a capacidade máxima disponível para os objetos deste bucket. Este valor representa uma quantidade lógica (tamanho do objeto), não uma quantidade física (tamanho no disco).

   Se nenhum limite for definido, a capacidade para este intervalo é ilimitada. "Uso do limite de capacidade"Consulte para obter mais informações.

5. Selecione **criar bucket**.

   O bucket é criado e adicionado à tabela na página Buckets.

6. Opcionalmente, selecione **ir para a página de detalhes do bucket** "veja os detalhes do balde"e execute configurações adicionais.

Veja os detalhes do balde

Você pode visualizar os buckets em sua conta de locatário.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Acesso root, Gerenciar todos os buckets ou permissão Ver todos os buckets". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket.

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.

   A página baldes é exibida.

2. Reveja a tabela de resumo de cada balde.

   Conforme necessário, você pode classificar as informações por qualquer coluna, ou pode encaminhar e voltar a página através da lista.

   > Os valores contagem de objetos, espaço utilizado e utilização apresentados são estimativas. Essas estimativas são afetadas pelo timing de inests, conetividade de rede e status de nó. Se os buckets tiverem o controle de versão habilitado, as versões de objetos excluídos serão incluídas na contagem de objetos.

   Nome
   O nome exclusivo do bucket, que não pode ser alterado.

   Recursos ativados
   A lista de recursos que estão ativados para o bucket.

   S3 bloqueio de objetos
   Se o bloqueio de objeto S3 está ativado para o balde.

   Esta coluna só aparece se o bloqueio de objeto S3 estiver ativado para a grade. Esta coluna também mostra informações para quaisquer buckets em conformidade com o legado.

   Região
   A região do balde, que não pode ser alterada. Esta coluna está oculta por padrão.

   Contagem de objetos
   O número de objetos neste intervalo. Se os buckets tiverem o controle de versão ativado, versões de objetos não atuais serão incluídas neste valor.

   Quando objetos são adicionados ou excluídos, esse valor pode não ser atualizado imediatamente.

   Espaço utilizado
   O tamanho lógico de todos os objetos no intervalo. O tamanho lógico não inclui o espaço real necessário para cópias replicadas ou codificadas para apagamento ou metadados de objetos.

   Esse valor pode levar até 10 minutos para ser atualizado.

   Utilização
   A percentagem utilizada do limite de capacidade do balde, se tiver sido definida.

   O valor de uso é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, o StorageGRID verifica o limite de capacidade (se definido) quando um locatário inicia o upload de objetos e rejeita novos ingerências para esse bucket se o locatário tiver excedido o limite de

capacidade. No entanto, o StorageGRID não leva em conta o tamanho do carregamento atual ao determinar se o limite de capacidade foi excedido. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos para este bucket até que o uso do limite de capacidade seja recalculado. Os cálculos podem levar 10 minutos ou mais.

Esse valor indica o tamanho lógico, não o tamanho físico necessário para armazenar os objetos e seus metadados.

Capacidade

Se definido, o limite de capacidade do balde.

Data de criação

A data e a hora em que o intervalo foi criado. Esta coluna está oculta por padrão.

3. Para ver detalhes de um intervalo específico, selecione o nome do intervalo na tabela.
   a. Veja as informações de resumo na parte superior da página da Web para confirmar os detalhes do intervalo, como contagem de região e Objeto.
   b. Veja a barra de uso do limite de capacidade. Se o uso for 100% ou próximo a 100%, considere aumentar o limite ou excluir alguns objetos.
   c. Conforme necessário, selecione **Excluir objetos no bucket** e **Excluir bucket**.

Preste muita atenção às precauções que aparecem quando você seleciona cada uma dessas opções. Para obter mais informações, consulte:

- "Exclua todos os objetos em um bucket"
- "Eliminar um balde" (o balde deve estar vazio)

   d. Visualize ou altere as definições do balde em cada uma das patilhas, conforme necessário.
      - **S3 Console**: Visualize os objetos do bucket. Para obter mais informações, "Use o Console S3"consulte .
      - **Opções de balde**: Veja ou altere as configurações de opção. Algumas configurações, como o bloqueio de objetos S3, não podem ser alteradas após a criação do bucket.
        - "Gerenciar a consistência do balde"
        - "Últimas atualizações de tempo de acesso"
        - "Limite de capacidade"
        - "Controle de versão de objetos"
        - "S3 bloqueio de objetos"
        - "Retenção padrão do balde"
        - "Gerenciar a replicação entre grades" (se permitido para o inquilino)
      - **Serviços de plataforma**: "Gerenciar serviços de plataforma"(Se permitido para o inquilino)
      - **Bucket Access**: Veja ou altere as configurações de opção. Você deve ter permissões de acesso específicas.
        - Configure "Compartilhamento de recursos entre origens (CORS)" para que o bucket e os objetos no bucket fiquem acessíveis a aplicativos da Web em outros domínios.
        - "Controle o acesso do usuário" Para um balde S3 e objetos nesse balde.

Aplique uma etiqueta de política ILM a um bucket

Escolha uma etiqueta de política ILM para aplicar a um bucket com base nos requisitos de armazenamento de objetos.

A política ILM controla onde os dados do objeto são armazenados e se eles são excluídos após um determinado período de tempo. O administrador da grade cria políticas ILM e as atribui a tags de política ILM ao usar várias políticas ativas.

> Evite reatribuir frequentemente a etiqueta de política de um bucket. Caso contrário, podem ocorrer problemas de desempenho.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Acesso root, Gerenciar todos os buckets ou permissão Ver todos os buckets". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket.

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.

   A página baldes é exibida. Conforme necessário, você pode classificar as informações por qualquer coluna, ou pode encaminhar e voltar a página através da lista.

2. Selecione o nome do intervalo ao qual deseja atribuir uma etiqueta de política ILM.

   Você também pode alterar a atribuição de tag de política ILM para um bucket que já tenha uma tag atribuída.

   > Os valores contagem de objetos e espaço utilizados apresentados são estimativas. Essas estimativas são afetadas pelo timing de inests, conetividade de rede e status de nó. Se os buckets tiverem o controle de versão habilitado, as versões de objetos excluídos serão incluídas na contagem de objetos.

3. Na guia Opções de balde, expanda o acordeão da etiqueta de política ILM. Esse acordeão só aparece se o administrador da grade tiver habilitado o uso de tags de política personalizadas.
4. Leia a descrição de cada tag de política para determinar qual tag deve ser aplicada ao bucket.

   > Alterar a etiqueta de política ILM para um bucket acionará a reavaliação ILM de todos os objetos no bucket. Se a nova política reter objetos por um tempo limitado, os objetos mais antigos serão excluídos.

5. Selecione o botão de opção para a etiqueta que pretende atribuir ao balde.
6. Selecione **Salvar alterações**. Uma nova tag de bucket S3 será definida no bucket com a chave `NTAP-SG-ILM-BUCKET-TAG` e o valor do nome da tag de política ILM.

   > Certifique-se de que as aplicações do S3 não anulam acidentalmente ou excluem a nova etiqueta de bucket. Se essa tag for omitida ao aplicar um novo TagSet ao bucket, os objetos no bucket reverterão para serem avaliados em relação à política padrão do ILM.

Defina e modifique as tags de política ILM usando apenas o Gerenciador do locatário ou a API do Gerenciador do locatário onde a tag de política ILM é validada. Não modifique a `NTAP-SG-ILM-BUCKET-TAG` tag de política ILM usando a API PutBucketTagging S3 ou a API DeleteBucketTagging S3.

A alteração da etiqueta de política atribuída a um bucket tem um impactos temporário no desempenho enquanto os objetos estão sendo reavaliados usando a nova política ILM.

Gerenciar política de bucket

Você pode controlar o acesso do usuário para um bucket do S3 e os objetos nesse bucket.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz". As permissões Exibir todos os buckets e Gerenciar todos os buckets só permitem a visualização.
- Você verificou que o número necessário de nós e sites de storage estão disponíveis. Se dois ou mais nós de storage não estiverem disponíveis em nenhum local ou se um site não estiver disponível, as alterações nessas configurações poderão não estar disponíveis.

Passos

1. Selecione **Buckets** e, em seguida, selecione o bucket que pretende gerir.
2. Na página de detalhes do balde, selecione **Bucket Access** > **Bucket policy**.
3. Execute um dos seguintes procedimentos:
   - Insira uma política de intervalo selecionando a caixa de seleção **Ativar política**. Em seguida, insira uma string formatada JSON válida.

     Cada política de bucket tem um limite de tamanho de 20.480 bytes.
   - Modifique uma política existente editando a cadeia de carateres.
   - Desative uma política desmarcando **Ativar política**.

Para obter informações detalhadas sobre políticas de bucket, incluindo sintaxe de idioma e exemplos, "Exemplo de políticas de bucket"consulte .

Gerenciar a consistência do balde

Valores de consistência podem ser usados para especificar a disponibilidade de alterações de configuração de bucket, bem como para fornecer um equilíbrio entre a disponibilidade dos objetos dentro de um bucket e a consistência desses objetos em diferentes nós de storage e locais. Você pode alterar os valores de consistência para serem diferentes dos valores padrão para que os aplicativos clientes possam atender às suas necessidades operacionais.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".

- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Diretrizes de consistência do balde

A consistência do bucket é usada para determinar a consistência dos aplicativos clientes que afetam objetos dentro desse bucket do S3. Em geral, você deve usar a consistência **Read-after-novo-write** para seus buckets.

altere a consistência do balde

Se a consistência **Read-after-new-write** não atender aos requisitos do aplicativo cliente, você pode alterar a consistência definindo a consistência do bucket ou usando o `Consistency-Control` cabeçalho. O `Consistency-Control` colhedor substitui a consistência do balde.

> Quando você altera a consistência de um balde, apenas os objetos que são ingeridos após a alteração têm a garantia de atender à configuração revisada.

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na tabela.

   É apresentada a página de detalhes do balde.
3. Na guia **Opções de balde**, selecione o acordeão **.
4. Selecione uma consistência para as operações realizadas nos objetos neste intervalo.
   - **Todos**: Fornece o mais alto nível de consistência. Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
   - **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
   - * Strong-site*: Garante consistência de leitura-após-gravação para todas as solicitações de clientes dentro de um site.
   - **Read-after-novo-write** (padrão): Fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
   - **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.
5. Selecione **Salvar alterações**.

O que acontece quando você altera as configurações do balde

Os buckets têm várias configurações que afetam o comportamento dos buckets e dos objetos dentro desses buckets.

As seguintes configurações de bucket usam a consistência **strong** por padrão. Se dois ou mais nós de storage não estiverem disponíveis em nenhum local, ou se um site não estiver disponível, quaisquer alterações nessas configurações poderão não estar disponíveis.

- "Eliminação do balde vazio em segundo plano"
- "Último tempo de acesso"
- "Ciclo de vida do balde"
- "Política de balde"
- "Identificação do balde"
- "Controle de versão do bucket"
- "S3 bloqueio de objetos"
- "Criptografia do bucket"

> O valor de consistência para controle de versão de bucket, bloqueio de objeto S3 e criptografia de bucket não pode ser definido para um valor que não é fortemente consistente.

As seguintes configurações de bucket não usam consistência forte e têm maior disponibilidade para alterações. As alterações a essas configurações podem levar algum tempo antes de ter um efeito.

- "Configuração de serviços de plataforma: Integração de notificação, replicação ou pesquisa"
- "Configuração CORS"
- Altere a consistência do balde

> Se a consistência padrão usada ao alterar as configurações do bucket não atender aos requisitos do aplicativo cliente, você poderá alterar a consistência usando o `Consistency-Control` cabeçalho para "S3 API REST"ou usando `reducedConsistency` as opções ou `force` no "API de gerenciamento do locatário".

Ative ou desative as atualizações da última hora de acesso

Quando os administradores de grade criam as regras de gerenciamento do ciclo de vida das informações (ILM) para um sistema StorageGRID, opcionalmente, eles podem especificar que o último tempo de acesso de um objeto seja usado para determinar se deseja mover esse objeto para um local de armazenamento diferente. Se você estiver usando um locatário do S3, poderá aproveitar essas regras habilitando as atualizações da última hora de acesso para os objetos em um bucket do S3.

Estas instruções aplicam-se apenas a sistemas StorageGRID que incluam pelo menos uma regra ILM que utilize a opção **último tempo de acesso** como um filtro avançado ou como um tempo de referência. Você pode ignorar essas instruções se o seu sistema StorageGRID não incluir essa regra. "Use o último tempo de acesso nas regras do ILM"Consulte para obter detalhes.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Sobre esta tarefa

Último tempo de acesso é uma das opções disponíveis para a instrução de colocação **tempo de referência** para uma regra ILM. Definir o tempo de referência para uma regra como tempo de acesso último permite que os administradores de grade especifiquem que os objetos sejam colocados em determinados locais de

armazenamento com base em quando esses objetos foram recuperados pela última vez (lidos ou visualizados).

Por exemplo, para garantir que os objetos visualizados recentemente permaneçam em armazenamento mais rápido, um administrador de grade pode criar uma regra ILM especificando o seguinte:

- Os objetos recuperados no mês passado devem permanecer nos nós de storage locais.
- Os objetos que não foram recuperados no mês passado devem ser movidos para um local externo.

Por padrão, as atualizações para a última hora de acesso são desativadas. Se o seu sistema StorageGRID incluir uma regra ILM que use a opção **último tempo de acesso** e você quiser que essa opção se aplique a objetos neste intervalo, você deverá habilitar as atualizações para o último tempo de acesso para os buckets do S3 especificados nessa regra.

> Atualizar o último tempo de acesso quando um objeto é recuperado pode reduzir o desempenho do StorageGRID, especialmente para objetos pequenos.

Um impactos no desempenho ocorre com as últimas atualizações de tempo de acesso porque o StorageGRID deve executar essas etapas adicionais sempre que os objetos são recuperados:

- Atualize os objetos com novos carimbos de data/hora
- Adicione os objetos à fila ILM para que possam ser reavaliados em relação às regras e políticas atuais do ILM

A tabela resume o comportamento aplicado a todos os objetos no intervalo quando o último tempo de acesso é desativado ou ativado.

Tipo de solicitação	Comportamento se a última hora de acesso estiver desativada (predefinição)		Comportamento se a última hora de acesso estiver ativada	
	Último tempo de acesso atualizado?	Objeto adicionado à fila de avaliação ILM?	Último tempo de acesso atualizado?	Objeto adicionado à fila de avaliação ILM?
Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados	Não	Não	Sim	Sim
Solicitação para atualizar os metadados de um objeto	Sim	Sim	Sim	Sim
Solicitação para listar objetos ou versões de objetos	Não	Não	Não	Não

Solicitação para copiar um objeto de um bucket para outro	• Não, para a cópia de origem • Sim, para a cópia de destino	• Não, para a cópia de origem • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino
Pedido para concluir um carregamento multipart	Sim, para o objeto montado	Sim, para o objeto montado	Sim, para o objeto montado	Sim, para o objeto montado

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na tabela.

   É apresentada a página de detalhes do balde.

3. Na guia **Opções do balde**, selecione o acordeão **atualizações do último tempo de acesso**.
4. Ative ou desative as atualizações da última hora de acesso.
5. Selecione **Salvar alterações**.

Alterar o controle de versão de objetos para um bucket

Se você estiver usando um locatário S3, poderá alterar o estado de controle de versão para buckets do S3.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Você verificou que o número necessário de nós e sites de storage estão disponíveis. Se dois ou mais nós de storage não estiverem disponíveis em nenhum local ou se um site não estiver disponível, as alterações nessas configurações poderão não estar disponíveis.

Sobre esta tarefa

Você pode ativar ou suspender o controle de versão de objetos para um bucket. Depois de ativar o controle de versão para um bucket, ele não pode retornar a um estado não versionado. No entanto, você pode suspender o controle de versão para o bucket.

- Desativado: O controle de versão nunca foi habilitado
- Habilitado: O controle de versão está habilitado
- Suspenso: O controle de versão foi ativado anteriormente e está suspenso

Para obter mais informações, consulte o seguinte:

- "Controle de versão de objetos"
- "Regras e políticas do ILM para objetos com versão S3 (exemplo 4)"
- "Como os objetos são excluídos"

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na tabela.

   É apresentada a página de detalhes do balde.

3. Na guia **Opções de balde**, selecione o acordeão **versão de objeto**.
4. Selecione um estado de controle de versão para os objetos neste intervalo.

   O controle de versão do objeto deve permanecer habilitado para um bucket usado para replicação entre grades. Se o bloqueio de objeto S3 ou a conformidade legada estiver ativada, as opções **versão de objeto** serão desativadas.

Opção	Descrição
Habilite o controle de versão	Ative o controle de versão de objetos se você quiser armazenar todas as versões de cada objeto neste intervalo. Em seguida, você pode recuperar versões anteriores de um objeto, conforme necessário. Os objetos que já estavam no bucket serão versionados quando forem modificados por um usuário.
Suspenda o controle de versão	Suspenda o controle de versão do objeto se você não quiser mais criar novas versões de objeto. Você ainda pode recuperar quaisquer versões de objetos existentes.

5. Selecione **Salvar alterações**.

Use o bloqueio de objetos S3D para reter objetos

Você pode usar o bloqueio de objetos S3 se os buckets e os objetos precisarem cumprir os requisitos regulamentares para retenção.

O administrador da grade deve dar permissão para usar recursos específicos do S3 Object Lock.

O que é S3 Object Lock?

O recurso bloqueio de objetos do StorageGRID S3 é uma solução de proteção de objetos equivalente ao bloqueio de objetos do S3 no Amazon Simple Storage Service (Amazon S3).

Quando a configuração de bloqueio de objeto S3 global está ativada para um sistema StorageGRID, uma conta de locatário S3 pode criar buckets com ou sem bloqueio de objeto S3 ativado. Se um bucket tiver o bloqueio de objetos S3 ativado, o controle de versão do bucket é necessário e é ativado automaticamente.

Um bucket sem S3 Object Lock só pode ter objetos sem as configurações de retenção especificadas. Nenhum objeto ingerido terá configurações de retenção.

- Um bucket com S3 Object Lock* pode ter objetos com e sem configurações de retenção especificadas por aplicativos clientes S3. Alguns objetos ingeridos terão definições de retenção.

Um bucket com o bloqueio de objeto S3 e a retenção padrão configurada pode ter carregado objetos com

configurações de retenção especificadas e novos objetos sem configurações de retenção. Os novos objetos usam a configuração padrão, porque a configuração de retenção não foi configurada no nível do objeto.

Efetivamente, todos os objetos recém-ingeridos têm configurações de retenção quando a retenção padrão é configurada. Os objetos existentes sem configurações de retenção de objetos permanecem inalterados.

Modos de retenção

O recurso bloqueio de objetos do StorageGRID S3 suporta dois modos de retenção para aplicar diferentes níveis de proteção aos objetos. Esses modos são equivalentes aos modos de retenção do Amazon S3.

- No modo de conformidade:
  - O objeto não pode ser excluído até que sua data de retenção seja alcançada.
  - O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- No modo de governança:
  - Os usuários com permissão especial podem usar um cabeçalho de desvio em solicitações para modificar determinadas configurações de retenção.
  - Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada.
  - Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto.

Configurações de retenção para versões de objetos

Se um bucket for criado com o bloqueio de objeto S3 ativado, os usuários poderão usar o aplicativo cliente S3 para especificar opcionalmente as seguintes configurações de retenção para cada objeto adicionado ao bucket:

- **Modo de retenção**: Conformidade ou governança.
- **Retent-until-date**: Se a data de retent-until de uma versão de objeto estiver no futuro, o objeto pode ser recuperado, mas não pode ser excluído.
- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar colocar uma retenção legal em um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até que seja explicitamente removida. As obrigações legais são independentes da retenção até à data.

  > Se um objeto estiver sob uma retenção legal, ninguém poderá excluir o objeto, independentemente de seu modo de retenção.

  Para obter detalhes sobre as configurações do objeto, "Use a API REST do S3 para configurar o bloqueio de objetos do S3"consulte .

Configuração de retenção padrão para buckets

Se um bucket for criado com o bloqueio de objetos S3 ativado, os usuários podem especificar opcionalmente as seguintes configurações padrão para o bucket:

- **Modo de retenção padrão**: Conformidade ou governança.
- **Período de retenção padrão**: Quanto tempo as novas versões de objetos adicionadas a este intervalo devem ser mantidas, a partir do dia em que são adicionadas.

As configurações padrão de bucket se aplicam somente a novos objetos que não têm suas próprias configurações de retenção. Os objetos de bucket existentes não são afetados quando você adiciona ou altera essas configurações padrão.

"Crie um bucket do S3"Consulte e "Atualização S3 retenção padrão bloqueio Objeto".

S3 tarefas de bloqueio de objetos

As listas a seguir para administradores de grade e usuários de locatário contêm as tarefas de alto nível para usar o recurso bloqueio de objeto S3.

Administrador de grade

- Ative a configuração global de bloqueio de objetos S3D para todo o sistema StorageGRID.
- Certifique-se de que as políticas de gerenciamento do ciclo de vida das informações (ILM) sejam *compatíveis*; ou seja, elas atendem "Requisitos de buckets com bloqueio de objeto S3 ativado"ao .
- Conforme necessário, permita que um locatário use a conformidade como modo de retenção. Caso contrário, somente o modo Governança é permitido.
- Conforme necessário, defina um período máximo de retenção para um locatário.

Utilizador inquilino

- Considerações de revisão para buckets e objetos com o S3 Object Lock.
- Conforme necessário, entre em Contato com o administrador de grade para habilitar a configuração global de bloqueio de objetos S3D e definir permissões.
- Crie buckets com o S3 Object Lock ativado.
- Opcionalmente, configure as configurações de retenção padrão para um bucket:
  - Modo de retenção padrão: Governança ou conformidade, se permitido pelo administrador da grade.
  - Período de retenção padrão: Deve ser menor ou igual ao período de retenção máximo definido pelo administrador da grade.
- Use o aplicativo cliente S3 para adicionar objetos e, opcionalmente, definir retenção específica de objeto:
  - Modo de retenção. Governança ou conformidade, se permitido pelo administrador da grade.
  - Reter Data até: Deve ser menor ou igual ao permitido pelo período de retenção máximo definido pelo administrador da grade.

Requisitos para buckets com bloqueio de objeto S3 ativado

- Se a configuração global de bloqueio de objeto S3 estiver ativada para o sistema StorageGRID, você poderá usar o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3 para criar buckets com o bloqueio de objeto S3 ativado.
- Se você planeja usar o bloqueio de objetos S3D, você deve ativar o bloqueio de objetos S3D ao criar o bucket. Não é possível ativar o bloqueio de objetos S3 para um bucket existente.
- Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket. Não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão para o bucket.
- Opcionalmente, você pode especificar um modo de retenção padrão e um período de retenção para cada bucket usando o Gerenciador de locatários, a API de gerenciamento do locatário ou a API REST do S3. As configurações de retenção padrão do bucket se aplicam somente a novos objetos adicionados ao bucket que não têm suas próprias configurações de retenção. Você pode substituir essas configurações

padrão especificando um modo de retenção e manter-até-data para cada versão do objeto quando ele é carregado.

- A configuração do ciclo de vida do bucket é compatível com buckets com o S3 Object Lock ativado.
- A replicação do CloudMirror não é compatível com buckets com o S3 Object Lock ativado.

Requisitos para objetos em buckets com o bloqueio de objetos S3 ativado

- Para proteger uma versão de objeto, você pode especificar configurações de retenção padrão para o bucket ou especificar configurações de retenção para cada versão do objeto. As configurações de retenção no nível do objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST S3.
- As configurações de retenção se aplicam a versões de objetos individuais. Uma versão de objeto pode ter uma configuração de retenção de data e de retenção legal, uma mas não a outra, ou nenhuma. Especificar uma configuração reter-até-data ou retenção legal para um objeto protege apenas a versão especificada na solicitação. Você pode criar novas versões do objeto, enquanto a versão anterior do objeto permanece bloqueada.

Ciclo de vida dos objetos em buckets com o bloqueio de objetos S3 ativado

Cada objeto que é salvo em um bucket com o S3 Object Lock ativado passa por estes estágios:

1. * Ingestão de objetos*

   Quando uma versão de objeto é adicionada ao bucket que tem o bloqueio de objeto S3 ativado, as configurações de retenção são aplicadas da seguinte forma:

   - Se as configurações de retenção forem especificadas para o objeto, as configurações de nível do objeto serão aplicadas. Todas as configurações padrão do bucket são ignoradas.
   - Se não forem especificadas configurações de retenção para o objeto, as configurações padrão de bucket serão aplicadas, se existirem.
   - Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não será protegido pelo bloqueio de objeto S3.

   Se as configurações de retenção forem aplicadas, o objeto e quaisquer metadados definidos pelo usuário do S3 serão protegidos.

2. * Retenção e exclusão de objetos*

   Várias cópias de cada objeto protegido são armazenadas pelo StorageGRID durante o período de retenção especificado. O número exato e o tipo de cópias de objetos e os locais de storage são determinados pelas regras em conformidade nas políticas ativas de ILM. Se um objeto protegido pode ser excluído antes de sua data de retenção ser alcançada depende de seu modo de retenção.

   - Se um objeto estiver sob uma retenção legal, ninguém poderá excluir o objeto, independentemente de seu modo de retenção.

Ainda posso gerenciar buckets em conformidade com o legado?

O recurso bloqueio de objetos S3 substitui o recurso de conformidade que estava disponível nas versões anteriores do StorageGRID. Se você criou buckets compatíveis usando uma versão anterior do StorageGRID, poderá continuar gerenciando as configurações desses buckets. No entanto, não será mais possível criar novos buckets compatíveis. Para obter instruções, "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"consulte .

Atualização S3 retenção padrão bloqueio Objeto

Se você ativou o bloqueio de objeto S3 quando criou o bucket, poderá editar o bucket para alterar as configurações de retenção padrão. Você pode ativar (ou desativar) a retenção padrão e definir um modo de retenção e um período de retenção padrão.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- O bloqueio de objetos S3D é ativado globalmente para o seu sistema StorageGRID e você ativou o bloqueio de objetos S3D quando criou o bucket. "Use o bloqueio de objetos S3D para reter objetos"Consulte .

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na tabela.

   É apresentada a página de detalhes do balde.

3. Na guia **Opções de balde**, selecione o acordeão **S3 Object Lock**.
4. Opcionalmente, ative ou desative **retenção padrão** para este bucket.

   As alterações a essa configuração não se aplicam a objetos que já estejam no bucket ou a quaisquer objetos que possam ter seus próprios períodos de retenção.

5. Se **retenção padrão** estiver ativada, especifique um **modo de retenção padrão** para o intervalo.

Modo de retenção predefinido	Descrição
Governança	• Os usuários com `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as configurações de retenção. • Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada. • Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto.
Conformidade	• O objeto não pode ser excluído até que sua data de retenção seja alcançada. • O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído. • A data de retenção do objeto não pode ser removida até que essa data seja atingida. **Nota**: O administrador da grade deve permitir que você use o modo de conformidade.

6. Se **retenção padrão** estiver ativada, especifique o **período de retenção padrão** para o intervalo.

   O **período de retenção padrão** indica quanto tempo novos objetos adicionados a esse intervalo devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor menor ou igual ao período máximo de retenção para o locatário, conforme definido pelo administrador da grade.

   Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador da grade cria o locatário. Quando você define um período de retenção *default*, ele não pode exceder o valor definido para o período de retenção máximo. Se necessário, peça ao administrador da grade para aumentar ou diminuir o período máximo de retenção.

7. Selecione **Salvar alterações**.

Configurar o compartilhamento de recursos entre origens (CORS)

Você pode configurar o compartilhamento de recursos entre origens (CORS) para um bucket do S3 se quiser que esse bucket e objetos nesse bucket estejam acessíveis a aplicativos da Web em outros domínios.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Para OBTER solicitações de configuração do CORS, você pertence a um grupo de usuários que tenha o "Gerencie todos os buckets ou visualize todos os buckets". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Para SOLICITAÇÕES de configuração put CORS, você pertence a um grupo de usuários que tem o "Gerenciar todas as permissões de buckets". Essa permissão substitui as configurações de permissões em políticas de grupo ou bucket.
- O "Permissão de acesso à raiz" fornece acesso a todas as solicitações de configuração do CORS.

Sobre esta tarefa

O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos da Web do cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado `Images` para armazenar gráficos. Ao configurar o CORS para o `Images` bucket, você pode permitir que as imagens nesse bucket sejam exibidas no site `http://www.example.com`.

Ativar CORS para um balde

Passos

1. Use um editor de texto para criar o XML necessário. Este exemplo mostra o XML usado para ativar o CORS para um bucket S3. Especificamente:
   - Permite que qualquer domínio envie SOLICITAÇÕES GET para o bucket
   - Só permite que o `http://www.example.com` domínio envie SOLICITAÇÕES GET, POST e DELETE
   - Todos os cabeçalhos de solicitação são permitidos

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

Para obter mais informações sobre o XML de configuração do CORS, "Documentação do Amazon Web Services (AWS): Guia do usuário do Amazon Simple Storage Service" consulte .

2. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do intervalo na tabela.

   É apresentada a página de detalhes do balde.

4. Na guia **Bucket Access**, selecione o acordeão **Cross-Origin Resource Sharing (CORS)**.
5. Marque a caixa de seleção **Enable CORS** (Ativar CORS*).
6. Cole o XML de configuração do CORS na caixa de texto.
7. Selecione **Salvar alterações**.

Modificar a definição CORS

Passos

1. Atualize o XML de configuração do CORS na caixa de texto ou selecione **Limpar** para recomeçar.
2. Selecione **Salvar alterações**.

Desativar a definição CORS

Passos

1. Desmarque a caixa de seleção **Enable CORS** (Ativar CORS*).
2. Selecione **Salvar alterações**.

Excluir objetos no bucket

Você pode usar o Gerenciador do locatário para excluir os objetos em um ou mais buckets.

Considerações e requisitos

Antes de executar estas etapas, observe o seguinte:

- Quando você exclui os objetos em um bucket, o StorageGRID remove permanentemente todos os objetos e todas as versões de objetos em cada bucket selecionado de todos os nós e sites do seu sistema StorageGRID. O StorageGRID também remove quaisquer metadados de objetos relacionados. Você não será capaz de recuperar essas informações.
- A exclusão de todos os objetos em um bucket pode levar minutos, dias ou até semanas, com base no número de objetos, cópias de objetos e operações simultâneas.
- Se um bucket tiver "S3 bloqueio de objetos ativado", ele poderá permanecer no estado **Deletando objetos: Somente leitura** por *anos*.

Um bucket que usa o bloqueio de objeto S3 permanecerá no estado **excluindo objetos: Somente leitura** até que a data de retenção seja alcançada para todos os objetos e quaisquer retenções legais sejam removidas.

- Enquanto os objetos estão sendo excluídos, o estado do bucket é **excluindo objetos: Somente leitura**. Neste estado, não é possível adicionar novos objetos ao intervalo.
- Quando todos os objetos tiverem sido excluídos, o bucket permanece no estado somente leitura. Você pode fazer um dos seguintes procedimentos:
  - Retorne o bucket ao modo de gravação e reutilize-o para novos objetos
  - Elimine o balde
  - Mantenha o intervalo no modo somente leitura para reservar seu nome para uso futuro
- Se um bucket tiver o controle de versão de objetos ativado, excluir marcadores criados no StorageGRID 11,8 ou posterior poderá ser removido usando o recurso Excluir objetos em operações de bucket.
- Se um bucket tiver o controle de versão de objeto ativado, a operação excluir objetos não removerá marcadores de exclusão criados no StorageGRID 11,7 ou anterior. Consulte informações sobre como excluir objetos em um bucket no "Como objetos com versão S3 são excluídos".
- Se utilizar "replicação entre grade"o , tenha em atenção o seguinte:
  - Usar essa opção não exclui nenhum objeto do bucket na outra grade.
  - Se você selecionar essa opção para o intervalo de origem, o alerta **Falha na replicação entre grades** será acionado se você adicionar objetos ao intervalo de destino na outra grade. Se você não puder garantir que ninguém adicionará objetos ao bucket na outra grade, "desative a replicação entre redes" para esse bucket antes de excluir todos os objetos do bucket.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz". Essa permissão substitui as configurações de permissões em políticas de grupo ou bucket.

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.

   A página baldes é exibida e mostra todos os baldes S3 existentes.

2. Use o menu **ações** ou a página de detalhes de um intervalo específico.

Menu ações

a. Marque a caixa de seleção para cada bucket do qual você deseja excluir objetos.

b. Selecione **ações** > **Excluir objetos no bucket**.

Página de detalhes

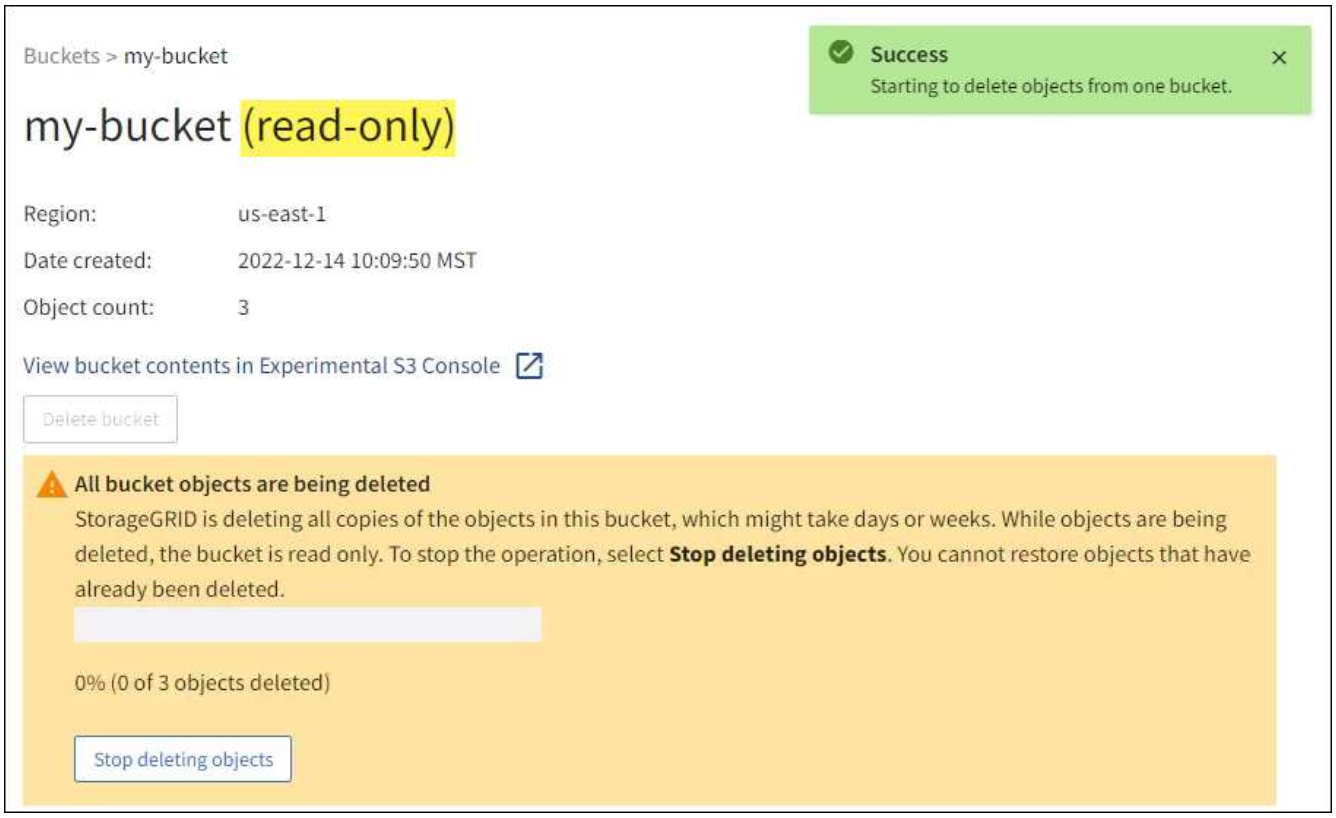
a. Selecione um nome de bucket para exibir seus detalhes.

b. Selecione **Excluir objetos no bucket**.

3. Quando a caixa de diálogo de confirmação for exibida, revise os detalhes, digite **Sim** e selecione **OK**.
4. Aguarde o início da operação de eliminação.

   Após alguns minutos:

   - É apresentado um banner de estado amarelo na página de detalhes do balde. A barra de progresso representa a porcentagem de objetos que foram excluídos.
   - **(somente leitura)** aparece após o nome do bucket na página de detalhes do bucket.
   - **(excluindo objetos: Somente leitura)** aparece ao lado do nome do bucket na página Buckets.

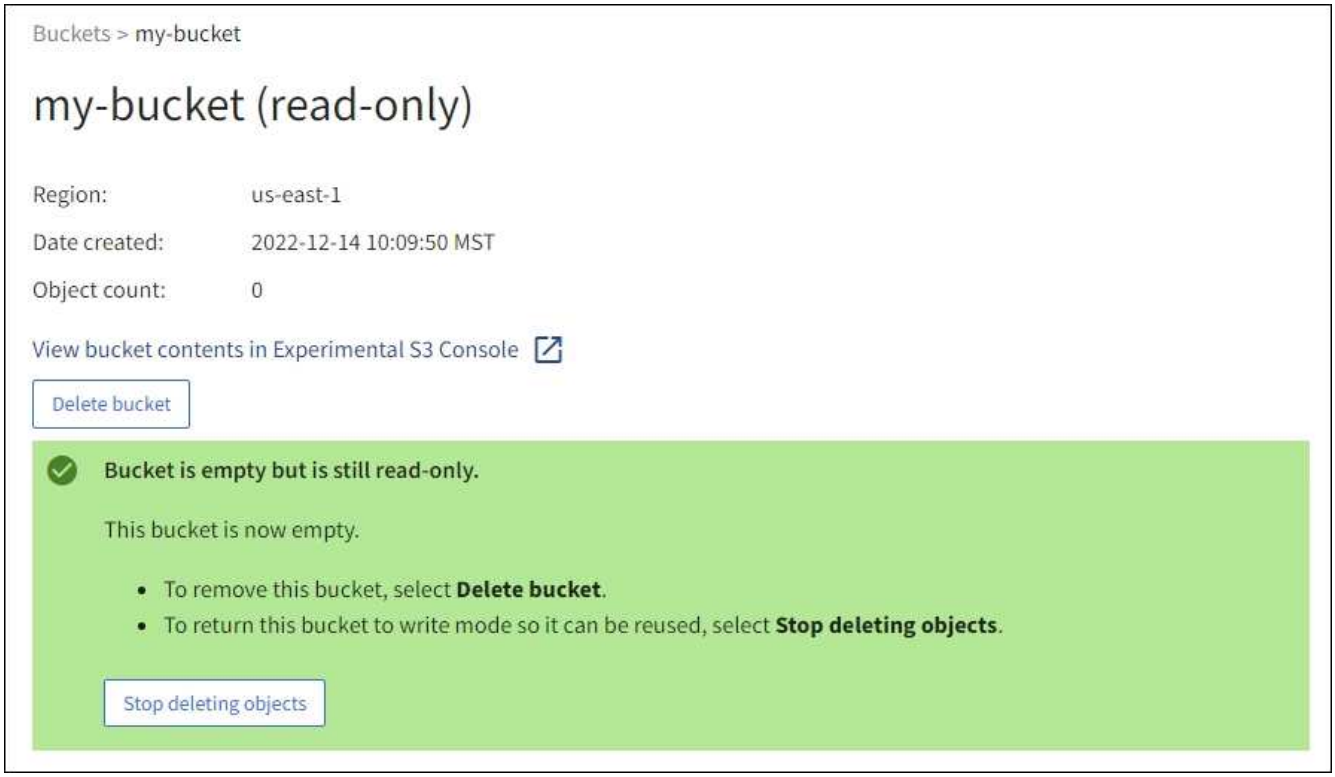


5. Conforme necessário enquanto a operação estiver em execução, selecione **Parar de excluir objetos** para interromper o processo. Em seguida, opcionalmente, selecione **Excluir objetos no bucket** para retomar o processo.

   Quando você seleciona **Parar de excluir objetos**, o bucket é retornado ao modo de gravação; no entanto, você não pode acessar ou restaurar quaisquer objetos que tenham sido excluídos.

6. Aguarde até que a operação seja concluída.

Quando o intervalo está vazio, o banner de status é atualizado, mas o intervalo permanece somente leitura.



7. Execute um dos seguintes procedimentos:
   - Saia da página para manter o balde no modo só de leitura. Por exemplo, você pode manter um bucket vazio no modo somente leitura para reservar o nome do bucket para uso futuro.
   - Elimine o balde. Você pode selecionar **Excluir bucket** para excluir um único bucket ou retornar a página Buckets e selecionar **Actions** > **Delete** buckets para remover mais de um bucket.

     Se você não conseguir excluir um bucket versionado depois que todos os objetos foram excluídos, os marcadores de exclusão podem permanecer. Para eliminar o intervalo, tem de remover todos os marcadores de eliminação restantes.

   - Retorne o bucket ao modo de gravação e, opcionalmente, reutilize-o para novos objetos. Você pode selecionar **Parar de excluir objetos** para um único bucket ou retornar à página Buckets e selecionar **Ação** > **Parar de excluir objetos** para mais de um bucket.

Eliminar o balde S3

Você pode usar o Gerenciador do Locatário para excluir um ou mais buckets do S3 vazios.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Os intervalos que você deseja excluir estão vazios. Se os intervalos que você deseja excluir estiverem *não* vazios, "eliminar objetos do intervalo".

Sobre esta tarefa

Estas instruções descrevem como excluir um bucket do S3 usando o Gerenciador do locatário. Também é possível excluir buckets do S3 usando o "API de gerenciamento do locatário" ou o "S3 API REST".

Não é possível excluir um bucket do S3 se ele contiver objetos, versões de objetos não atuais ou marcadores de exclusão. Para obter informações sobre como os objetos com versão S3 são excluídos, "Como os objetos são excluídos"consulte .

Passos

1. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.

   A página baldes é exibida e mostra todos os baldes S3 existentes.

2. Use o menu **ações** ou a página de detalhes de um intervalo específico.

   Menu ações

   a. Selecione a caixa de verificação para cada intervalo que pretende eliminar.

   b. Selecione **ações** > **Excluir buckets**.

   Página de detalhes

   a. Selecione um nome de bucket para exibir seus detalhes.

   b. Selecione **Eliminar balde**.

3. Quando a caixa de diálogo de confirmação for exibida, selecione **Sim**.

   O StorageGRID confirma que cada bucket está vazio e, em seguida, exclui cada bucket. Esta operação pode demorar alguns minutos.

   Se um balde não estiver vazio, é apresentada uma mensagem de erro. Você deve "exclua todos os objetos e quaisquer marcadores de exclusão no bucket" antes de poder excluir o bucket.

Use o Console S3

Você pode usar o Console S3 para exibir e gerenciar os objetos em um bucket do S3.

S3 Console permite que você:

- Carregar, transferir, mudar o nome, copiar, mover e eliminar objetos
- Exibir, reverter, baixar e excluir versões de objetos
- Pesquisar objetos por prefixo
- Gerenciar tags de objeto
- Exibir metadados de objetos
- Exibir, criar, renomear, copiar, mover e excluir pastas

O console S3 oferece uma experiência de usuário aprimorada para os casos mais comuns. Ele não foi projetado para substituir as operações CLI ou API em todas as situações.

Se o uso do Console S3 resulta em operações demoradas demais (por exemplo, minutos ou horas), considere:

- Reduzindo o número de objetos selecionados
- Usando métodos não gráficos (API ou CLI) para acessar seus dados

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Se você quiser gerenciar objetos, você pertence a um grupo de usuários que tem a permissão de acesso root. Como alternativa, você pertence a um grupo de usuários que tem a permissão usar a guia Console S3 e a permissão Exibir todos os buckets ou Gerenciar todos os buckets. "Permissões de gerenciamento do locatário"Consulte .
- Uma política de grupo S3 ou balde foi configurada para o utilizador. "Use políticas de acesso de grupo e bucket"Consulte .
- Você sabe o ID da chave de acesso do usuário e a chave de acesso secreta. Opcionalmente, você tem um `.csv` arquivo contendo essas informações. Consulte "instruções para criar chaves de acesso".

Passos

1. Selecione **STORAGE** > **Buckets** > ***bucket name***.
2. Selecione a guia Console do S3.
3. Cole o ID da chave de acesso e a chave de acesso secreta nos campos. Caso contrário, selecione **carregar chaves de acesso** e selecione o seu `.csv` ficheiro.
4. Selecione **entrar**.
5. É apresentada a tabela de objetos de balde. Você pode gerenciar objetos conforme necessário.

Informações adicionais

- **Busca por prefixo**: O recurso de pesquisa de prefixo procura apenas objetos que começam com uma palavra específica relativa à pasta atual. A pesquisa não inclui objetos que contenham a palavra em outro lugar. Esta regra também se aplica a objetos dentro de pastas. Por exemplo, uma pesquisa `folder1/folder2/somefile-` retornaria objetos que estão dentro da `folder1/folder2/` pasta e começaria com a palavra `somefile-`.
- * Arrastar e soltar*: Você pode arrastar e soltar arquivos do gerenciador de arquivos do computador para o console S3. No entanto, não é possível carregar pastas.
- **Operações em pastas**: Quando você move, copia ou renomeia uma pasta, todos os objetos na pasta são atualizados um de cada vez, o que pode levar tempo.
- **Exclusão permanente quando o controle de versão do bucket está desativado**: Quando você substitui ou exclui um objeto em um bucket com o controle de versão desativado, a operação é permanente. "Alterar o controle de versão de objetos para um bucket"Consulte .

Gerenciar os serviços da plataforma S3

Serviços de plataforma S3

Antes de implementar serviços de plataforma, revise a visão geral e as considerações sobre o uso desses serviços.

Para obter informações sobre o S3, "USE A API REST DO S3"consulte .

Visão geral dos serviços da plataforma

Os serviços de plataforma StorageGRID ajudam você a implementar uma estratégia de nuvem híbrida permitindo que você envie notificações de eventos e cópias de objetos S3 e metadados de objetos para destinos externos.

Como o local de destino para serviços de plataforma geralmente é externo à implantação do StorageGRID, os serviços de plataforma oferecem a você o poder e a flexibilidade decorrentes do uso de recursos de storage externos, serviços de notificação e serviços de pesquisa ou análise para seus dados.

Qualquer combinação de serviços de plataforma pode ser configurada para um único bucket do S3. Por exemplo, você pode configurar o "Serviço CloudMirror" e "notificações" em um bucket do StorageGRID S3 para que você possa espelhar objetos específicos para o Amazon Simple Storage Service (S3), enquanto envia uma notificação sobre cada objeto a um aplicativo de monitoramento de terceiros para ajudá-lo a controlar suas despesas da AWS.

> O uso de serviços de plataforma deve ser habilitado para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de Gerenciamento de Grade.

Como os serviços de plataforma são configurados

Os serviços de plataforma comunicam-se com endpoints externos que você configura usando o "Gerente do locatário" ou o "API de gerenciamento do locatário". Cada endpoint representa um destino externo, como um bucket do StorageGRID S3, um bucket do Amazon Web Services, um tópico do Amazon SNS ou um cluster do Elasticsearch hospedado localmente, na AWS ou em qualquer outro lugar.

Depois de criar um endpoint externo, você pode habilitar um serviço de plataforma para um bucket adicionando a configuração XML ao bucket. A configuração XML identifica os objetos nos quais o bucket deve agir, a ação que o bucket deve realizar e o ponto final que o bucket deve usar para o serviço.

Você deve adicionar configurações XML separadas para cada serviço de plataforma que você deseja configurar. Por exemplo:

- Se você quiser que todos os objetos cujas chaves comecem por `/images` ser replicados em um bucket do Amazon S3, adicione uma configuração de replicação ao bucket de origem.
- Se você também quiser enviar notificações quando esses objetos estiverem armazenados no bucket, adicione uma configuração de notificações.
- Se você quiser indexar os metadados para esses objetos, adicione a configuração de notificação de metadados usada para implementar a integração de pesquisa.

O formato para a configuração XML é regido pelas S3 REST APIs usadas para implementar serviços de plataforma StorageGRID:

Serviço de plataforma	S3 API REST	Consulte
Replicação do CloudMirror	• GetBucketReplication • PutBucketReplication	• "Replicação do CloudMirror" • "Operações em baldes"
Notificações	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notificações" • "Operações em baldes"
Integração de pesquisa	• OBTER configuração de notificação de metadados do bucket • COLOQUE a configuração de notificação de metadados do bucket	• "Integração de pesquisa" • "Operações personalizadas do StorageGRID"

Considerações sobre o uso de serviços de plataforma

Consideração	Detalhes
Monitoramento de endpoint de destino	Você deve monitorar a disponibilidade de cada endpoint de destino. Se a conetividade com o endpoint de destino for perdida por um longo período de tempo e existir um grande backlog de solicitações, solicitações de cliente adicionais (como SOLICITAÇÕES PUT) para o StorageGRID falharão. Você deve tentar novamente essas solicitações com falha quando o endpoint se tornar acessível.
Limitação do ponto de extremidade de destino	O software StorageGRID pode controlar as solicitações recebidas do S3 para um bucket se a taxa na qual as solicitações estão sendo enviadas exceder a taxa na qual o endpoint de destino pode receber as solicitações. O estrangulamento só ocorre quando há um backlog de solicitações aguardando para serem enviadas para o endpoint de destino. O único efeito visível é que as solicitações S3 recebidas demorarão mais tempo para serem executadas. Se você começar a detetar desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o backlog de solicitações continuar a crescer, as operações do cliente S3 (como SOLICITAÇÕES PUT) acabarão falhando. As solicitações do CloudMirror são mais propensas a serem afetadas pelo desempenho do endpoint de destino, pois essas solicitações geralmente envolvem mais transferência de dados do que solicitações de integração de pesquisa ou notificação de eventos.

Consideração	Detalhes
Garantias de encomenda	A StorageGRID garante o pedido de operações em um objeto dentro de um site. Desde que todas as operações contra um objeto estejam dentro do mesmo local, o estado final do objeto (para replicação) sempre será igual ao estado no StorageGRID. A StorageGRID faz o melhor esforço para solicitar solicitações quando as operações são feitas em sites da StorageGRID. Por exemplo, se você escrever um objeto inicialmente no site A e depois sobrescrever o mesmo objeto no site B, o objeto final replicado pelo CloudMirror para o bucket de destino não será garantido como o objeto mais recente.
Exclusões de objetos orientadas por ILM	Para corresponder ao comportamento de exclusão do AWS CRR e do Amazon Simple Notification Service, as solicitações de notificação de eventos e CloudMirror não são enviadas quando um objeto no bucket de origem é excluído devido às regras do StorageGRID ILM. Por exemplo, nenhuma solicitação de notificações do CloudMirror ou evento será enviada se uma regra ILM excluir um objeto após 14 dias. Em contraste, as solicitações de integração de pesquisa são enviadas quando os objetos são excluídos por causa do ILM.
Usando endpoints Kafka	Para endpoints Kafka, TLS mútuo não é suportado. Como resultado, se você tiver `ssl.client.auth` definido como `required` na configuração do seu broker Kafka, isso pode causar problemas de configuração do endpoint do Kafka. A autenticação dos endpoints do Kafka usa os seguintes tipos de autenticação. Esses tipos são diferentes daqueles usados para autenticação de outros endpoints, como o Amazon SNS, e exigem credenciais de nome de usuário e senha. • SASL/PLANÍCIE • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Observação:** as configurações de proxy de armazenamento configuradas não se aplicam aos pontos de extremidade dos serviços da plataforma Kafka.

Considerações para usar o serviço de replicação do CloudMirror

Consideração	Detalhes
Estado da replicação	O StorageGRID não suporta o `x-amz-replication-status` colhedor.

Consideração	Detalhes
Tamanho do objeto	O tamanho máximo para objetos que podem ser replicados para um bucket de destino pelo serviço de replicação do CloudMirror é 5 TIB, o que é o mesmo que o tamanho máximo de objeto *suportado*. **Nota**: O tamanho máximo *recomendado* para uma única operação PutObject é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart.
Controle de versão do bucket e IDs de versão	Se o bucket S3 de origem no StorageGRID tiver o controle de versão ativado, você também deverá habilitar o controle de versão para o bucket de destino. Ao usar o controle de versão, observe que o pedido de versões de objetos no intervalo de destino é o melhor esforço e não é garantido pelo serviço CloudMirror, devido às limitações no protocolo S3. **Nota**: Os IDs de versão para o bucket de origem no StorageGRID não estão relacionados com os IDs de versão para o bucket de destino.
Marcação para versões de objetos	O serviço CloudMirror não replica nenhuma solicitação PutObjectTagging ou DeleteObjectTagging que forneça uma ID de versão, devido a limitações no protocolo S3. Como os IDs de versão para a origem e destino não estão relacionados, não há como garantir que uma atualização de tag para uma ID de versão específica seja replicada. Em contraste, o serviço CloudMirror replica solicitações PutObjectTagging ou solicitações DeleteObjectTagging que não especificam um ID de versão. Essas solicitações atualizam as tags para a chave mais recente (ou a versão mais recente se o bucket for versionado). Inests normais com tags (não marcando atualizações) também são replicados.
Carregamentos e valores multiparte `ETag`	Ao espelhar objetos que foram carregados usando um upload multipart, o serviço CloudMirror não preserva as peças. Como resultado, o `ETag` valor para o objeto espelhado será diferente do valor do objeto `ETag` original.
Objetos criptografados com SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente)	O serviço CloudMirror não suporta objetos que são criptografados com SSE-C. se você tentar ingerir um objeto no bucket de origem para replicação do CloudMirror e a solicitação incluir os cabeçalhos de solicitação SSE-C, a operação falhará.
Balde com bloqueio de objetos S3 ativado	A replicação não é suportada para buckets de origem ou destino com o bloqueio de objetos S3 ativado.

Entenda o serviço de replicação do CloudMirror

Você pode habilitar a replicação do CloudMirror para um bucket do S3 se quiser que o StorageGRID replique objetos especificados adicionados ao bucket a um ou mais buckets de destino externos.

Por exemplo, você pode usar a replicação do CloudMirror para espelhar Registros específicos de clientes no Amazon S3 e aproveitar os serviços da AWS para realizar análises nos seus dados.

> A replicação do CloudMirror não é suportada se o bucket de origem tiver o S3 Object Lock ativado.

CloudMirror e ILM

A replicação do CloudMirror opera independentemente das políticas de ILM ativas da grade. O serviço CloudMirror replica objetos à medida que eles são armazenados no bucket de origem e os entrega ao bucket de destino o mais rápido possível. A entrega de objetos replicados é acionada quando a ingestão de objetos é bem-sucedida.

Replicação entre grades e CloudMirror

A replicação do CloudMirror tem semelhanças e diferenças importantes com o recurso de replicação entre grades. "Compare a replicação entre redes e a replicação do CloudMirror"Consulte a .

Buckets do CloudMirror e do S3

A replicação do CloudMirror normalmente é configurada para usar um bucket externo do S3 como destino. No entanto, você também pode configurar a replicação para usar outra implantação do StorageGRID ou qualquer serviço compatível com S3.

Buckets existentes

Quando você ativa a replicação do CloudMirror para um bucket existente, apenas os novos objetos adicionados a esse bucket são replicados. Quaisquer objetos existentes no bucket não são replicados. Para forçar a replicação de objetos existentes, você pode atualizar os metadados do objeto existente executando uma cópia de objeto.

> Se você estiver usando a replicação do CloudMirror para copiar objetos para um destino do Amazon S3, saiba que o Amazon S3 limita o tamanho dos metadados definidos pelo usuário em cada cabeçalho de SOLICITAÇÃO PUT para 2 KB. Se um objeto tiver metadados definidos pelo usuário com mais de 2 KB, esse objeto não será replicado.

Vários buckets de destino

Para replicar objetos em um único bucket para vários buckets de destino, especifique o destino para cada regra no XML de configuração de replicação. Não é possível replicar um objeto para mais de um bucket ao mesmo tempo.

Baldes versionados ou não versionados

Você pode configurar a replicação do CloudMirror em buckets versionados ou não versionados. Os intervalos de destino podem ser versionados ou não versionados. Você pode usar qualquer combinação de buckets versionados e não versionados. Por exemplo, você pode especificar um bucket versionado como o destino para um bucket de origem não versionado, ou vice-versa. Você também pode replicar entre buckets não versionados.

Exclusão, loops de replicação e eventos

Comportamento de exclusão

É o mesmo que o comportamento de exclusão do serviço Amazon S3, replicação entre regiões (CRR). A exclusão de um objeto em um bucket de origem nunca exclui um objeto replicado no destino. Se os intervalos de origem e destino forem versionados, o marcador de exclusão será replicado. Se o intervalo de

destino não tiver versão, a exclusão de um objeto no intervalo de origem não replica o marcador de exclusão para o intervalo de destino ou exclui o objeto de destino.

Proteção contra loops de replicação

À medida que os objetos são replicados para o intervalo de destino, o StorageGRID os marca como "réplicas". Um bucket do StorageGRID de destino não replicará objetos marcados como réplicas novamente, protegendo-o de loops de replicação acidentais. Essa marcação de réplica é interna ao StorageGRID e não impede que você aproveite o AWS CRR ao usar um bucket do Amazon S3 como destino.

> O cabeçalho personalizado usado para marcar uma réplica é `x-ntap-sg-replica`. Esta marcação impede um espelho em cascata. O StorageGRID oferece suporte a um CloudMirror bidirecional entre duas grades.

Eventos no intervalo de destino

A singularidade e a ordem dos eventos no intervalo de destino não são garantidas. Mais de uma cópia idêntica de um objeto de origem pode ser entregue ao destino como resultado de operações tomadas para garantir o sucesso da entrega. Em casos raros, quando o mesmo objeto é atualizado simultaneamente de dois ou mais locais diferentes do StorageGRID, a ordenação de operações no intervalo de destino pode não corresponder à ordenação de eventos no intervalo de origem.

Entenda as notificações para buckets

Você pode ativar a notificação de eventos para um bucket do S3 se quiser que o StorageGRID envie notificações sobre eventos especificados para um cluster do Kafka de destino ou para o Amazon Simple Notification Service.

Por exemplo, você pode configurar alertas para serem enviados aos administradores sobre cada objeto adicionado a um bucket, onde os objetos representam arquivos de log associados a um evento crítico do sistema.

As notificações de eventos são criadas no intervalo de origem conforme especificado na configuração de notificação e são entregues ao destino. Se um evento associado a um objeto for bem-sucedido, uma notificação sobre esse evento será criada e colocada em fila para entrega.

A singularidade e a ordem das notificações não são garantidas. Mais de uma notificação de um evento pode ser entregue ao destino como resultado de operações tomadas para garantir o sucesso da entrega. E como a entrega é assíncrona, o tempo de ordenação das notificações no destino não é garantido para corresponder à ordenação de eventos no intervalo de origem, particularmente para operações originadas de diferentes sites da StorageGRID. Você pode usar a `sequencer` chave na mensagem de evento para determinar a ordem dos eventos para um determinado objeto, conforme descrito na documentação do Amazon S3.

As notificações de eventos do StorageGRID seguem a API do Amazon S3 com algumas limitações.

- Os seguintes tipos de evento são suportados:
  - S3:ObjectCreated:
  - S3:ObjectCreated:put
  - S3:ObjectCreated:Post
  - S3:ObjectCreated:Copy
  - S3:ObjectCreated:CompleteMultipartUpload

- S3:ObjectRemovado:
- S3:ObjectRemovado:Excluir
- S3:ObjectRemoved:DeleteMarkerCreated
- S3:ObjectRestore:Post

- As notificações de eventos enviadas pelo StorageGRID usam o formato JSON padrão, mas não incluem algumas chaves e usam valores específicos para outras, como mostrado na tabela:

Nome da chave	Valor StorageGRID
EventSource	`sgws:s3`
AwsRegion	*não incluído*
x-amz-id-2	*não incluído*
arn	`urn:sgws:s3:::bucket_name`

Compreender o serviço de integração de pesquisa

Você pode habilitar a integração de pesquisa para um bucket do S3 se quiser usar um serviço de pesquisa e análise de dados externos para os metadados de objetos.

O serviço de integração de pesquisa é um serviço StorageGRID personalizado que envia automaticamente e assincronamente metadados de objeto S3 para um endpoint de destino sempre que um objeto é criado ou excluído, ou seus metadados ou tags são atualizados. Depois, você pode usar ferramentas sofisticadas de pesquisa, análise de dados, visualização ou aprendizado de máquina fornecidas pelo serviço de destino para pesquisar, analisar e obter insights a partir dos dados do objeto.

Por exemplo, você pode configurar seus buckets para enviar metadados de objeto S3 para um serviço Elasticsearch remoto. Você pode usar o Elasticsearch para realizar pesquisas entre buckets e realizar análises sofisticadas de padrões presentes nos metadados do objeto.

Embora a integração do Elasticsearch possa ser configurada em um bucket com o S3 Object Lock ativado, os metadados do S3 Object Lock (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nos metadados enviados ao Elasticsearch.

> Como o serviço de integração de pesquisa faz com que os metadados de objeto sejam enviados para um destino, seu XML de configuração é chamado de "*metadata* notificação configuração XML." Este XML de configuração é diferente do "XML de configuração de notificação" usado para ativar as notificações *event*.

Integração de pesquisa e buckets do S3

Você pode ativar o serviço de integração de pesquisa para qualquer bucket com versão ou não versionado. A integração de pesquisa é configurada associando o XML de configuração de notificação de metadados ao intervalo que especifica quais objetos agir e o destino para os metadados de objeto.

As notificações de metadados são geradas na forma de um documento JSON chamado com o nome do intervalo, nome do objeto e ID da versão, se houver. Cada notificação de metadados contém um conjunto

padrão de metadados do sistema para o objeto, além de todas as tags do objeto e metadados do usuário.

> Para tags e metadados de usuários, o StorageGRID passa datas e números para o Elasticsearch como strings ou como notificações de eventos do S3. Para configurar o Elasticsearch para interpretar essas strings como datas ou números, siga as instruções do Elasticsearch para mapeamento de campos dinâmicos e para os formatos de data de mapeamento. Você deve ativar os mapeamentos de campo dinâmicos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

Notificações de pesquisa

As notificações de metadados são geradas e colocadas em fila para entrega sempre que:

- Um objeto é criado.
- Um objeto é excluído, inclusive quando os objetos são excluídos como resultado da operação da política ILM da grade.
- Metadados de objetos ou tags são adicionados, atualizados ou excluídos. O conjunto completo de metadados e tags é sempre enviado na atualização - não apenas os valores alterados.

Depois de adicionar XML de configuração de notificação de metadados a um bucket, as notificações são enviadas para quaisquer novos objetos que você criar e para quaisquer objetos que você modificar atualizando seus dados, metadados de usuário ou tags. No entanto, as notificações não são enviadas para quaisquer objetos que já estavam no intervalo. Para garantir que os metadados de objetos para todos os objetos no bucket sejam enviados para o destino, você deve fazer um dos seguintes procedimentos:

- Configure o serviço de integração de pesquisa imediatamente após criar o bucket e antes de adicionar quaisquer objetos.
- Execute uma ação em todos os objetos já no intervalo que acionará uma mensagem de notificação de metadados a ser enviada para o destino.

Serviço de integração de pesquisa e Elasticsearch

O serviço de integração de pesquisa StorageGRID suporta um cluster Elasticsearch como destino. Tal como acontece com os outros serviços da plataforma, o destino é especificado no endpoint cuja URN é usada no XML de configuração para o serviço. Use o "Ferramenta de Matriz de interoperabilidade do NetApp" para determinar as versões suportadas do Elasticsearch.

Gerenciar endpoints de serviços de plataforma

Configurar endpoints de serviços de plataforma

Antes de configurar um serviço de plataforma para um bucket, você deve configurar pelo menos um endpoint para ser o destino do serviço de plataforma.

O acesso a serviços de plataforma é ativado por locatário por administrador do StorageGRID. Para criar ou usar um endpoint de serviços de plataforma, você deve ser um usuário de locatário com permissão Gerenciar endpoints ou acesso raiz, em uma grade cuja rede foi configurada para permitir que os nós de storage acessem recursos de endpoint externos. Para um único locatário, você pode configurar um máximo de 500 endpoints de serviços de plataforma. Contacte o administrador do StorageGRID para obter mais informações.

O que é um endpoint de serviços de plataforma?

Um endpoint de serviços de plataforma especifica as informações que o StorageGRID precisa para acessar o destino externo.

Por exemplo, se você quiser replicar objetos de um bucket do StorageGRID para um bucket do Amazon S3, crie um endpoint de serviços de plataforma que inclua as informações e credenciais que o StorageGRID precisa para acessar o bucket de destino na Amazon.

Cada tipo de serviço de plataforma requer seu próprio endpoint, então você deve configurar pelo menos um endpoint para cada serviço de plataforma que você planeja usar. Depois de definir um endpoint de serviços de plataforma, você usa o URN do endpoint como o destino no XML de configuração usado para ativar o serviço.

Você pode usar o mesmo ponto de extremidade que o destino para mais de um intervalo de origem. Por exemplo, você pode configurar vários buckets de origem para enviar metadados de objetos para o mesmo endpoint de integração de pesquisa para que você possa realizar pesquisas em vários buckets. Você também pode configurar um bucket de origem para usar mais de um endpoint como destino, o que permite que você faça coisas como enviar notificações sobre a criação de objetos para um tópico do Amazon Simple Notification Service (Amazon SNS) e notificações sobre a exclusão de objetos para um segundo tópico do Amazon SNS.

Endpoints para replicação do CloudMirror

O StorageGRID é compatível com pontos de extremidade de replicação que representam buckets do S3. Esses buckets podem estar hospedados no Amazon Web Services, na mesma ou em uma implantação remota do StorageGRID ou em outro serviço.

Endpoints para notificações

O StorageGRID suporta endpoints Amazon SNS e Kafka. Os endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.

Para endpoints Kafka, TLS mútuo não é suportado. Como resultado, se você tiver `ssl.client.auth` definido como `required` na configuração do seu broker Kafka, isso pode causar problemas de configuração do endpoint do Kafka.

Endpoints para o serviço de integração de pesquisa

O StorageGRID é compatível com endpoints de integração de pesquisa que representam clusters do Elasticsearch. Esses clusters do Elasticsearch podem estar em um data center local ou hospedados em uma nuvem da AWS ou em outro lugar.

O endpoint de integração de pesquisa refere-se a um índice e tipo específicos do Elasticsearch. Você deve criar o índice no Elasticsearch antes de criar o endpoint no StorageGRID, ou a criação do endpoint falhará. Você não precisa criar o tipo antes de criar o endpoint. O StorageGRID criará o tipo, se necessário, quando envia metadados de objeto para o endpoint.

Informações relacionadas

"Administrar o StorageGRID"

Especifique URN para endpoint de serviços de plataforma

Ao criar um endpoint de serviços de plataforma, você deve especificar um Nome de recurso exclusivo (URN). Você usará a URN para referenciar o endpoint quando criar um XML de configuração para o serviço da plataforma. A URNA para cada endpoint deve

ser única.

O StorageGRID valida endpoints de serviços de plataforma à medida que os cria. Antes de criar um endpoint de serviços de plataforma, confirme se o recurso especificado no endpoint existe e se ele pode ser alcançado.

URNA elementos

A URNA para um endpoint de serviços de plataforma deve começar com `arn:aws` ou `urn:mysite`, da seguinte forma:

- Se o serviço estiver hospedado na Amazon Web Services (AWS), use `arn:aws`
- Se o serviço estiver hospedado no Google Cloud Platform (GCP), use `arn:aws`
- Se o serviço estiver hospedado localmente, use `urn:mysite`

Por exemplo, se você estiver especificando a URNA para um endpoint do CloudMirror hospedado no StorageGRID, a URNA pode começar com `urn:sgws`.

O próximo elemento da URNA especifica o tipo de serviço de plataforma, como segue:

Serviço	Tipo
Replicação do CloudMirror	`s3`
Notificações	`sns` ou `kafka`
Integração de pesquisa	`es`

Por exemplo, para continuar especificando a URN para um endpoint do CloudMirror hospedado no StorageGRID, você adicionaria `s3` ao GET `urn:sgws:s3`.

O elemento final da URNA identifica o recurso alvo específico no URI de destino.

Serviço	Recurso específico
Replicação do CloudMirror	`bucket-name`
Notificações	`sns-topic-name` ou `kafka-topic-name`
Integração de pesquisa	`domain-name/index-name/type-name` **Observação:** se o cluster Elasticsearch estiver configurado para criar índices automaticamente, você deverá criar o índice manualmente antes de criar o endpoint.

Urnas para serviços hospedados na AWS e no GCP

Para entidades da AWS e do GCP, a URN completa é um AWS ARN válido. Por exemplo:

- Replicação do CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notificações:

```
arn:aws:sns:region:account-id:topic-name
```

- Integração de pesquisa:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> Para um endpoint de integração de pesquisa da AWS, o `domain-name` deve incluir a cadeia de carateres literal `domain/` , como mostrado aqui.

Urnas para serviços hospedados localmente

Ao usar serviços hospedados localmente em vez de serviços em nuvem, você pode especificar a URNA de qualquer forma que crie uma URNA válida e única, desde que a URNA inclua os elementos necessários na terceira e última posições. Você pode deixar os elementos indicados por opcional em branco, ou você pode especificá-los de qualquer forma que o ajude a identificar o recurso e tornar a URNA única. Por exemplo:

- Replicação do CloudMirror:

```
urn:mysite:s3:optional:optional:bucket-name
```

Para um endpoint do CloudMirror hospedado no StorageGRID, você pode especificar uma URNA válida que começa com `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notificações:

Especifique um endpoint do Amazon Simple Notification Service:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

Especifique um ponto final Kafka:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- Integração de pesquisa:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

Para endpoints de integração de pesquisa hospedados localmente, o `domain-name` elemento pode ser qualquer string, desde que a URNA do endpoint seja única.

Criar endpoint de serviços de plataforma

Você deve criar pelo menos um endpoint do tipo correto antes de habilitar um serviço de plataforma.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".
- O recurso referenciado pelo endpoint de serviços da plataforma foi criado:
  - Replicação do CloudMirror: Bucket do S3
  - Notificação de eventos: Tópico do Amazon Simple Notification Service (Amazon SNS) ou Kafka
  - Notificação de pesquisa: Índice Elasticsearch, se o cluster de destino não estiver configurado para criar índices automaticamente.
- Você tem as informações sobre o recurso de destino:
  - Host e porta para o URI (Uniform Resource Identifier)

    Se você planeja usar um bucket hospedado em um sistema StorageGRID como endpoint para replicação do CloudMirror, entre em Contato com o administrador da grade para determinar os valores que você precisa inserir.

  - Nome de recurso único (URN)

    "Especifique URN para endpoint de serviços de plataforma"

  - Credenciais de autenticação (se necessário):

Endpoints de integração de pesquisa

Para endpoints de integração de pesquisa, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- HTTP básico: Nome de usuário e senha

Endpoints de replicação do CloudMirror

Para endpoints de replicação do CloudMirror, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- CAP (Portal de Acesso C2S): URL de credenciais temporárias, certificados de servidor e cliente, chaves de cliente e uma senha de chave privada do cliente opcional.

Endpoints do Amazon SNS

Para endpoints do Amazon SNS, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta

Pontos finais Kafka

Para endpoints do Kafka, você pode usar as seguintes credenciais:

- SASL/PLAIN: Nome de usuário e senha
- SASL/SCRAM-SHA-256: Nome de usuário e senha
- SASL/SCRAM-SHA-512: Nome de usuário e senha

  - Certificado de segurança (se estiver usando um certificado de CA personalizado)

- Se os recursos de segurança do Elasticsearch estiverem ativados, você terá o privilégio de cluster do monitor para teste de conetividade e o privilégio de índice de gravação ou o Privileges de índice de índice e exclusão para atualizações de documentos.

Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**. A página de endpoints dos serviços da plataforma é exibida.
2. Selecione **criar endpoint**.
3. Introduza um nome de apresentação para descrever brevemente o ponto final e a respetiva finalidade.

   O tipo de serviço de plataforma que o endpoint suporta é mostrado ao lado do nome do endpoint quando ele está listado na página Endpoints, para que você não precise incluir essas informações no nome.

4. No campo **URI**, especifique o URI (Unique Resource Identifier) do endpoint.

   Use um dos seguintes formatos:

   ```
   https://host:port
   http://host:port
   ```

   Se você não especificar uma porta, as seguintes portas padrão serão usadas:

- Porta 443 para URIs HTTPS e porta 80 para URIs HTTP (a maioria dos endpoints)
- Porta 9092 para URIs HTTPS e HTTP (somente endpoints Kafka)

Por exemplo, o URI para um bucket hospedado no StorageGRID pode ser:

```
https://s3.example.com:10443
```

Neste exemplo, `s3.example.com` representa a entrada DNS para o IP virtual (VIP) do grupo StorageGRID high availability (HA) e `10443` representa a porta definida no ponto de extremidade do balanceador de carga.

> Sempre que possível, você deve se conectar a um grupo de HA de nós de balanceamento de carga para evitar um único ponto de falha.

Da mesma forma, o URI para um bucket hospedado na AWS pode ser:

```
https://s3-aws-region.amazonaws.com
```

> Se o endpoint for usado para o serviço de replicação do CloudMirror, não inclua o nome do bucket no URI. Você inclui o nome do bucket no campo **URN**.

5. Insira o Nome do recurso exclusivo (URN) para o endpoint.

> Você não pode alterar a URNA DE um endpoint depois que o endpoint foi criado.

6. Selecione **continuar**.
7. Selecione um valor para **tipo de autenticação**.

Endpoints de integração de pesquisa

Introduza ou carregue as credenciais para um endpoint de integração de pesquisa.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
Chave de acesso	Usa credenciais de estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreto
HTTP básico	Usa um nome de usuário e senha para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe

Endpoints de replicação do CloudMirror

Insira ou carregue as credenciais para um endpoint de replicação do CloudMirror.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
Chave de acesso	Usa credenciais de estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreto
CAP (Portal de Acesso C2S)	Usa certificados e chaves para autenticar conexões com o destino.	• URL de credenciais temporárias • Certificado CA do servidor (upload de arquivo PEM) • Certificado de cliente (upload de arquivo PEM) • Chave privada do cliente (upload de arquivo PEM, formato criptografado OpenSSL ou formato de chave privada não criptografado) • Senha de chave privada do cliente (opcional)

Endpoints do Amazon SNS

Insira ou carregue as credenciais de um endpoint do Amazon SNS.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
Chave de acesso	Usa credenciais de estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreto

Pontos finais Kafka

Introduza ou carregue as credenciais para um endpoint Kafka.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
SASL/PLANÍCIE	Usa um nome de usuário e senha com texto simples para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe
SASL/SCRAM-SHA-256	Usa um nome de usuário e senha usando um protocolo de resposta a desafios e hash SHA-256 para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe
SASL/SCRAM-SHA-512	Usa um nome de usuário e senha usando um protocolo de resposta a desafios e hash SHA-512 para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe

Selecione **usar autenticação de delegação tomada** se o nome de usuário e a senha forem derivados de um token de delegação obtido de um cluster Kafka.

8. Selecione **continuar**.
9. Selecione um botão de opção para **verificar servidor** para escolher como a conexão TLS com o endpoint é verificada.

Tipo de verificação do certificado	Descrição
Use certificado CA personalizado	Use um certificado de segurança personalizado. Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto **certificado CA**.
Use o certificado CA do sistema operacional	Use o certificado de CA de grade padrão instalado no sistema operacional para proteger conexões.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado. Esta opção não é segura.

10. Selecione **testar e criar endpoint**.
    - Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada local.
    - Uma mensagem de erro será exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **retornar aos detalhes do endpoint** e atualize as informações. Em seguida, selecione **testar e criar endpoint**.

> A criação de endpoint falha se os serviços de plataforma não estiverem ativados para sua conta de locatário. Contacte o administrador do StorageGRID.

Depois de configurar um endpoint, você pode usar seu URN para configurar um serviço de plataforma.

Informações relacionadas

- "Especifique URN para endpoint de serviços de plataforma"
- "Configurar a replicação do CloudMirror"
- "Configurar notificações de eventos"
- "Configurar o serviço de integração de pesquisa"

Teste a conexão para endpoint de serviços de plataforma

Se a conexão com um serviço de plataforma tiver sido alterada, você pode testar a conexão para que o endpoint valide que o recurso de destino existe e que ele pode ser alcançado usando as credenciais especificadas.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

Sobre esta tarefa

O StorageGRID não valida se as credenciais têm as permissões corretas.

Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da

plataforma que já foram configurados.

2. Selecione o ponto final cuja ligação pretende testar.

   A página de detalhes do ponto final é exibida.

3. Selecione **Test Connection**.
   - Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada local.
   - Uma mensagem de erro será exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Configuração** e atualize as informações. Em seguida, selecione **testar e salvar alterações**.

Editar endpoint de serviços de plataforma

Você pode editar a configuração de um endpoint de serviços de plataforma para alterar seu nome, URI ou outros detalhes. Por exemplo, talvez seja necessário atualizar credenciais expiradas ou alterar o URI para apontar para um índice de backup do Elasticsearch para failover. Não é possível alterar a URN para um endpoint de serviços de plataforma.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.

2. Selecione o ponto de extremidade que pretende editar.

   A página de detalhes do ponto final é exibida.

3. Selecione **Configuração**.
4. Conforme necessário, altere a configuração do endpoint.

   > Você não pode alterar a URNA DE um endpoint depois que o endpoint foi criado.

   a. Para alterar o nome de exibição do endpoint, selecione o ícone de edição .
   b. Conforme necessário, altere o URI.
   c. Conforme necessário, altere o tipo de autenticação.
      - Para autenticação da chave de acesso, altere a chave conforme necessário selecionando **Editar chave S3** e colando uma nova ID de chave de acesso e chave de acesso secreta. Se você precisar cancelar suas alterações, selecione **Reverter S3 key edit**.
      - Para autenticação CAP (C2S Access Portal), altere a URL de credenciais temporárias ou a senha de chave privada do cliente opcional e carregue novos arquivos de certificado e chave conforme necessário.

> A chave privada do cliente deve estar no formato encriptado OpenSSL ou no formato de chave privada não encriptada.

d. Conforme necessário, altere o método para verificar o servidor.

5. Selecione **Teste e salve as alterações**.
   - Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é verificada a partir de um nó em cada local.
   - Uma mensagem de erro será exibida se a validação do endpoint falhar. Modifique o ponto final para corrigir o erro e selecione **testar e salvar alterações**.

Excluir endpoint de serviços de plataforma

Você pode excluir um endpoint se não quiser mais usar o serviço de plataforma associado.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.

2. Selecione a caixa de verificação para cada ponto de extremidade que pretende eliminar.

> Se você excluir um endpoint de serviços de plataforma que está em uso, o serviço de plataforma associado será desativado para quaisquer buckets que usam o endpoint. Quaisquer solicitações que ainda não foram concluídas serão descartadas. Todas as novas solicitações continuarão sendo geradas até que você altere a configuração do bucket para não fazer mais referência à URNA excluída. O StorageGRID reportará essas solicitações como erros irrecuperáveis.

3. Selecione **ações** > **Excluir endpoint**.

   É apresentada uma mensagem de confirmação.

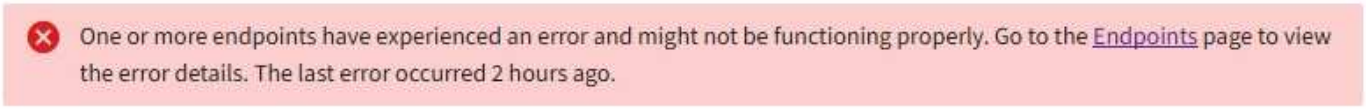
4. Selecione **Excluir endpoint**.

Solucionar erros de endpoint dos serviços da plataforma

Se ocorrer um erro quando o StorageGRID tenta se comunicar com um endpoint de serviços de plataforma, uma mensagem é exibida no painel. Na página pontos finais dos serviços da plataforma, a coluna último erro indica quanto tempo atrás o erro ocorreu. Nenhum erro é exibido se as permissões associadas às credenciais de um endpoint estiverem incorretas.

Determine se ocorreu um erro

Se algum erro de endpoint de serviços de plataforma tiver ocorrido nos últimos 7 dias, o painel do Gerenciador do Locatário exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.



O mesmo erro que aparece no painel também aparece na parte superior da página de endpoints dos serviços da plataforma. Para ver uma mensagem de erro mais detalhada:

Passos

1. Na lista de endpoints, selecione o endpoint que tem o erro.
2. Na página de detalhes do endpoint, selecione **conexão**. Esta guia exibe apenas o erro mais recente para um endpoint e indica quanto tempo atrás o erro ocorreu. Erros que incluem o ícone X vermelho  ocorreram nos últimos 7 dias.

Verifique se o erro ainda está atual

Alguns erros podem continuar a ser mostrados na coluna **último erro** mesmo depois de resolvidos. Para ver se um erro é atual ou forçar a remoção de um erro resolvido da tabela:

Passos

1. Selecione o ponto final.

   A página de detalhes do ponto final é exibida.

2. Selecione **Connection** > **Test Connection**.

Selecionar **testar conexão** faz com que o StorageGRID valide que o endpoint dos serviços da plataforma existe e que ele pode ser alcançado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada local.

Resolver erros de endpoint

Você pode usar a mensagem **último erro** na página de detalhes do endpoint para ajudar a determinar o que está causando o erro. Alguns erros podem exigir que você edite o endpoint para resolver o problema. Por exemplo, um erro de espelhamento de nuvem pode ocorrer se o StorageGRID não conseguir acessar o bucket do destino S3 porque ele não tem as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "as credenciais de endpoint ou o acesso de destino precisa ser atualizado", e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

Se você precisar editar o endpoint para resolver um erro, selecionar **testar e salvar alterações** faz com que o StorageGRID valide o endpoint atualizado e confirme que ele pode ser alcançado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada local.

Passos

1. Selecione o ponto final.
2. Na página de detalhes do endpoint, selecione **Configuração**.
3. Edite a configuração do endpoint conforme necessário.

4. Selecione **Connection** > **Test Connection**.

Credenciais de endpoint com permissões insuficientes

Quando o StorageGRID valida um endpoint de serviços de plataforma, ele confirma que as credenciais do endpoint podem ser usadas para entrar em Contato com o recurso de destino e faz uma verificação básica de permissões. No entanto, o StorageGRID não valida todas as permissões necessárias para determinadas operações de serviços de plataforma. Por esse motivo, se você receber um erro ao tentar usar um serviço de plataforma (como "403 proibido"), verifique as permissões associadas às credenciais do endpoint.

Informações relacionadas

- **Administrar o StorageGRID › solucionar problemas de serviços da plataforma**
- "Criar endpoint de serviços de plataforma"
- "Teste a conexão para endpoint de serviços de plataforma"
- "Editar endpoint de serviços de plataforma"

Configurar a replicação do CloudMirror

Para ativar a replicação do CloudMirror para um bucket, você cria e aplica um XML de configuração de replicação de bucket válido.

Antes de começar

- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket para agir como a origem de replicação.
- O endpoint que você pretende usar como destino para a replicação do CloudMirror já existe e você tem sua URN.
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

Sobre esta tarefa

A replicação do CloudMirror copia objetos de um bucket de origem para um bucket de destino especificado em um endpoint.

Para obter informações gerais sobre replicação de bucket e como configurá-la, "Documentação do Amazon Simple Storage Service (S3): Replicação de objetos" consulte . Para obter informações sobre como o StorageGRID implementa o GetBucketReplication, DeleteBucketReplication e o PutBucketReplication, consulte o "Operações em baldes".

> ⓘ A replicação do CloudMirror tem semelhanças e diferenças importantes com o recurso de replicação entre grades. Para saber mais, "Compare a replicação entre redes e a replicação do CloudMirror"consulte .

Observe os seguintes requisitos e caraterísticas ao configurar a replicação do CloudMirror:

- Quando você cria e aplica um XML de configuração de replicação de bucket válido, ele deve usar a URN de um endpoint de bucket S3 para cada destino.
- A replicação não é suportada para buckets de origem ou destino com o bloqueio de objetos S3 ativado.

- Se você habilitar a replicação do CloudMirror em um bucket que contém objetos, novos objetos adicionados ao bucket serão replicados, mas os objetos existentes no bucket não serão replicados. Você deve atualizar objetos existentes para acionar a replicação.
- Se você especificar uma classe de armazenamento no XML de configuração de replicação, o StorageGRID usará essa classe ao executar operações no endpoint S3 de destino. O endpoint de destino também deve suportar a classe de armazenamento especificada. Certifique-se de seguir quaisquer recomendações fornecidas pelo fornecedor do sistema de destino.

Passos

1. Habilite a replicação para o bucket de origem:
   - Use um editor de texto para criar a configuração de replicação XML necessária para habilitar a replicação, conforme especificado na API de replicação S3.
   - Ao configurar o XML:
     - Observe que o StorageGRID só suporta V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue convenções V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
     - Use a URNA de um endpoint de bucket S3 como o destino.
     - Opcionalmente, adicione o `<StorageClass>` elemento e especifique uma das seguintes opções:
       - `STANDARD`: A classe de armazenamento padrão. Se você não especificar uma classe de armazenamento ao carregar um objeto, a `STANDARD` classe de armazenamento será usada.
       - `STANDARD_IA`: (Standard - Acesso não frequente.) Use essa classe de storage para dados acessados com menos frequência, mas que ainda exigem acesso rápido quando necessário.
       - `REDUCED_REDUNDANCY`: Use esta classe de armazenamento para dados não críticos e reprodutíveis que podem ser armazenados com menos redundância do que a `STANDARD` classe de armazenamento.
     - Se você especificar um `Role` no XML de configuração, ele será ignorado. Este valor não é utilizado pelo StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Selecione **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do intervalo de origem.

   É apresentada a página de detalhes do balde.

4. Selecione **Serviços de plataforma** > **replicação**.
5. Marque a caixa de seleção **Ativar replicação**.
6. Cole o XML de configuração de replicação na caixa de texto e selecione **Salvar alterações**.

> Os serviços de plataforma devem estar habilitados para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Contacte o administrador do StorageGRID se ocorrer um erro ao guardar o XML de configuração.

7. Verifique se a replicação está configurada corretamente:
   a. Adicione um objeto ao bucket de origem que atenda aos requisitos de replicação, conforme especificado na configuração de replicação.

      No exemplo mostrado anteriormente, os objetos que correspondem ao prefixo "2020" são replicados.

   b. Confirme se o objeto foi replicado para o intervalo de destino.

      Para objetos pequenos, a replicação acontece rapidamente.

Informações relacionadas

"Criar endpoint de serviços de plataforma"

Configurar notificações de eventos

Você ativa notificações para um bucket criando XML de configuração de notificação e usando o Gerenciador de locatário para aplicar o XML a um bucket.

Antes de começar

- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket para agir como a fonte das notificações.
- O endpoint que você pretende usar como destino para notificações de eventos já existe, e você tem sua URNA.
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

Sobre esta tarefa

Você configura notificações de eventos associando o XML de configuração de notificação a um bucket de origem. O XML de configuração de notificação segue convenções S3 para configurar notificações de bucket, com o tópico Kafka de destino ou Amazon SNS especificado como a URNA de um endpoint.

Para obter informações gerais sobre notificações de eventos e como configurá-las, consulte o "Documentação da Amazon". Para obter informações sobre como o StorageGRID implementa a API de configuração de notificação de bucket do S3, consulte o "Instruções para a implementação de aplicativos cliente S3".

Observe os seguintes requisitos e caraterísticas ao configurar notificações de eventos para um bucket:

- Quando você cria e aplica XML de configuração de notificação válida, ele deve usar a URN de um endpoint de notificações de eventos para cada destino.

- Embora a notificação de evento possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nas mensagens de notificação.
- Depois de configurar notificações de eventos, sempre que um evento especificado ocorre para um objeto no bucket de origem, uma notificação é gerada e enviada para o tópico Amazon SNS ou Kafka usado como o endpoint de destino.
- Se você ativar notificações de eventos para um bucket que contém objetos, as notificações serão enviadas apenas para ações executadas após a configuração de notificação ser salva.

Passos

1. Ativar notificações para o intervalo de origem:
   - Use um editor de texto para criar a configuração de notificação XML necessário para habilitar notificações de eventos, conforme especificado na API de notificação S3.
   - Ao configurar o XML, use a URNA de um endpoint de notificações de eventos como o tópico de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. No Gerenciador do Locatário, selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do intervalo de origem.

   É apresentada a página de detalhes do balde.

4. Selecione **Serviços de plataforma** > **notificações de eventos**.
5. Marque a caixa de seleção **Ativar notificações de eventos**.
6. Cole o XML de configuração de notificação na caixa de texto e selecione **Salvar alterações**.

> Os serviços de plataforma devem estar habilitados para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Contacte o administrador do StorageGRID se ocorrer um erro ao guardar o XML de configuração.

7. Verifique se as notificações de eventos estão configuradas corretamente:

   a. Execute uma ação em um objeto no bucket de origem que atenda aos requisitos para acionar uma notificação conforme configurado no XML de configuração.

      No exemplo, uma notificação de evento é enviada sempre que um objeto é criado com o `images/` prefixo.

   b. Confirme se uma notificação foi entregue ao tópico do Amazon SNS ou Kafka de destino.

      Por exemplo, se o tópico de destino estiver hospedado no Amazon SNS, você poderá configurar o serviço para enviar um e-mail quando a notificação for entregue.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+
Se a notificação for recebida no tópico de destino, você configurou com êxito o bucket de origem para notificações do StorageGRID.

Informações relacionadas

"Entenda as notificações para buckets"

"USE A API REST DO S3"

"Criar endpoint de serviços de plataforma"

Configure o serviço de integração de pesquisa

Você ativa a integração de pesquisa para um bucket criando XML de integração de pesquisa e usando o Gerenciador de inquilinos para aplicar o XML ao bucket.

Antes de começar

- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket do S3 cujo conteúdo você deseja indexar.
- O endpoint que você pretende usar como destino para o serviço de integração de pesquisa já existe, e você tem sua URNA.
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

Sobre esta tarefa

Depois de configurar o serviço de integração de pesquisa para um bucket de origem, criar um objeto ou atualizar metadados ou tags de um objeto aciona metadados de objeto para serem enviados para o endpoint de destino.

Se você ativar o serviço de integração de pesquisa para um bucket que já contém objetos, as notificações de metadados não serão enviadas automaticamente para objetos existentes. Atualize esses objetos existentes para garantir que seus metadados sejam adicionados ao índice de pesquisa de destino.

Passos

1. Ativar a integração de pesquisa para um bucket:
    - Use um editor de texto para criar o XML de notificação de metadados necessário para habilitar a integração de pesquisa.
    - Ao configurar o XML, use a URNA de um endpoint de integração de pesquisa como o destino.

      Os objetos podem ser filtrados no prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `images` para um destino e metadados para objetos com o prefixo `videos` para outro. As configurações que têm prefixos sobrepostos não são válidas e são rejeitadas quando são enviadas. Por exemplo, uma configuração que inclua uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não é permitida.

      Conforme necessário, consulte Exemplos para a configuração de metadados XMLa .

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Elementos no XML de configuração de notificação de metadados:

Nome	Descrição	Obrigatório
MetadataNotificationConfiguration	Tag de contentor para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos de regra.	Sim
Regra	Tag container para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
ID	Identificador exclusivo para a regra. Incluído no elemento regra.	Não
Estado	O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas. Incluído no elemento regra.	Sim
Prefixo	Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento regra.	Sim
Destino	Etiqueta de contentor para o destino de uma regra. Incluído no elemento regra.	Sim

Nome	Descrição	Obrigatório
Urna	URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário `domain-name/myindex/mytype`. Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O endpoint deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. URNA está incluído no elemento destino.	Sim

2. No Gerenciador do Locatário, selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do intervalo de origem.

   É apresentada a página de detalhes do balde.

4. Selecione **Platform services** > **Search integration**
5. Marque a caixa de seleção **Ativar integração de pesquisa**.
6. Cole a configuração de notificação de metadados na caixa de texto e selecione **Salvar alterações**.

   > Os serviços de plataforma devem estar habilitados para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de gerenciamento. Contacte o administrador do StorageGRID se ocorrer um erro ao guardar o XML de configuração.

7. Verifique se o serviço de integração de pesquisa está configurado corretamente:
   a. Adicione um objeto ao bucket de origem que atenda aos requisitos para acionar uma notificação de metadados conforme especificado no XML de configuração.

      No exemplo mostrado anteriormente, todos os objetos adicionados ao bucket acionam uma notificação de metadados.

   b. Confirme se um documento JSON que contém metadados e tags do objeto foi adicionado ao índice de pesquisa especificado no endpoint.

Depois de terminar

Conforme necessário, você pode desativar a integração de pesquisa para um bucket usando um dos seguintes métodos:

- Selecione **STORAGE (S3)** > **Buckets** e desmarque a caixa de seleção **Enable search integration** (Ativar integração de pesquisa).
- Se você estiver usando a API do S3 diretamente, use uma solicitação de notificação de metadados de DELETE Bucket. Consulte as instruções para a implementação de aplicativos cliente S3.

exemplo: Configuração de notificação de metadados que se aplica a todos os objetos

Neste exemplo, metadados de objetos para todos os objetos são enviados para o mesmo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Exemplo: Configuração de notificação de metadados com duas regras

Neste exemplo, metadados de objetos para objetos que correspondem ao prefixo `/images` são enviados para um destino, enquanto metadados de objetos para objetos que correspondem ao prefixo `/videos` são enviados para um segundo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Formato de notificação de metadados

Quando você ativa o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado para o endpoint de destino cada vez que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

Este exemplo mostra um exemplo do JSON que pode ser gerado quando um objeto com a chave `SGWS/Tagging.txt` é criado em um intervalo `test` chamado . O `test` bucket não está versionado, então a `versionId` tag está vazia.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Campos incluídos no documento JSON

O nome do documento inclui o nome do intervalo, o nome do objeto e a ID da versão, se presente.

Informações sobre o balde e o objeto

`bucket`: Nome do balde

`key`: Nome da chave do objeto

`versionID`: Versão do objeto, para objetos em buckets versionados

`region`: Região do balde, por exemplo `us-east-1`

Metadados do sistema

`size`: Tamanho do objeto (em bytes) como visível para um cliente HTTP

`md5`: Hash de objeto

Metadados do usuário

`metadata`: Todos os metadados de usuário para o objeto, como pares de chave-valor

`key:value`

Tags

`tags`: Todas as tags de objeto definidas para o objeto, como pares chave-valor

`key:value`

Como ver os resultados em Elasticsearch

Para tags e metadados de usuários, o StorageGRID passa datas e números para o Elasticsearch como strings ou como notificações de eventos do S3. Para configurar o Elasticsearch para interpretar essas strings

como datas ou números, siga as instruções do Elasticsearch para mapeamento de campos dinâmicos e para os formatos de data de mapeamento. Ative os mapeamentos de campos dinâmicos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

USE A API REST DO S3

S3 versões e atualizações suportadas pela API REST

O StorageGRID oferece suporte à API Simple Storage Service (S3), que é implementada como um conjunto de serviços da Web de transferência de Estado representacional (REST).

O suporte à API REST do S3 permite conetar aplicativos orientados a serviços desenvolvidos para serviços da Web do S3 ao storage de objetos no local que usa o sistema StorageGRID. São necessárias alterações mínimas no uso atual de chamadas de API REST do aplicativo cliente S3.

Versões suportadas

O StorageGRID suporta as seguintes versões específicas do S3 e HTTP.

Item	Versão
Especificação da API S3	"Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service"
HTTP	1,1 Para obter mais informações sobre HTTP, consulte HTTP/1,1 (RFCs 7230-35). "IETF RFC 2616: Protocolo de transferência de hipertexto (HTTP/1,1)" **Nota**: O StorageGRID não suporta a canalização HTTP/1,1.

Atualizações para o suporte à API REST do S3

Solte	Comentários
11,9	• Adicionado suporte para valores de checksum SHA-256 pré-calculados para as seguintes solicitações e cabeçalhos suportados. Você pode usar esse recurso para verificar a integridade dos objetos carregados: ◦ CompleteMultipartUpload: `x-amz-checksum-sha256` ◦ CreateMultipartUpload: `x-amz-checksum-algorithm` ◦ GetObject: `x-amz-checksum-mode` ◦ Objeto cabeçalho: `x-amz-checksum-mode` ◦ ListParts ◦ Objeto Put: `x-amz-checksum-sha256` ◦ UploadPart: `x-amz-checksum-sha256` • Adicionada a capacidade de o administrador da grade controlar as configurações de retenção e conformidade no nível do locatário. Estas definições afetam as definições de bloqueio de objetos do S3. ◦ Modo de retenção padrão do bucket e modo de retenção de objetos: Governança ou conformidade, se permitido pelo administrador da grade. ◦ Período de retenção padrão do bucket e data até retenção do objeto: Deve ser menor ou igual ao permitido pelo período de retenção máximo definido pelo administrador da grade. • Suporte aprimorado para `aws-chunked` codificação de conteúdo e valores de streaming `x-amz-content-sha256`. Limitações: ◦ Se presente, `chunk-signature` é opcional e não validado ◦ Se presente, `x-amz-trailer` o conteúdo é ignorado
11,8	Atualizado os nomes das operações S3 para corresponder aos nomes usados no "Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service".
11,7	• Adicionado "Referência rápida: Solicitações de API S3 suportadas". • Adicionado suporte para usar o modo DE GOVERNANÇA com o bloqueio de objetos S3. • Adicionado suporte para o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status` para OBTER solicitações DE objeto e objeto PRINCIPAL. Este cabeçalho fornece o status de replicação de um objeto para replicação entre grade. • As solicitações SelectObjectContent agora suportam objetos Parquet.

Solte	Comentários
11,6	• Adicionado suporte para o uso do `partNumber` parâmetro Request em solicitações GET Object e HEAD Object. • Adicionado suporte para um modo de retenção padrão e um período de retenção padrão no nível do bucket para o bloqueio de objetos S3. • Adicionado suporte para a `s3:object-lock-remaining-retention-days` chave de condição de política para definir o intervalo de períodos de retenção permitidos para seus objetos. • Alterado o tamanho máximo *recommended* para uma única operação PUT Object para 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart.
11,5	• Adicionado suporte para gerenciar a criptografia de bucket. • Adicionado suporte para S3 Object Lock e solicitações de conformidade legadas obsoletas. • Adicionado suporte para o uso DE EXCLUIR vários objetos em buckets versionados. • O `Content-MD5` cabeçalho de solicitação agora é suportado corretamente.
11,4	• Adicionado suporte para EXCLUIR marcação de balde, OBTER marcação de balde e COLOCAR marcação de balde. As etiquetas de alocação de custos não são suportadas. • Para buckets criados no StorageGRID 11,4, não é mais necessário restringir nomes de chaves de objeto para atender às práticas recomendadas de desempenho. • Adicionado suporte para notificações de intervalo no `s3:ObjectRestore:Post` tipo de evento. • Os limites de tamanho da AWS para peças de várias partes agora são aplicados. Cada parte em um upload de várias partes deve estar entre 5 MIB e 5 GiB. A última parte pode ser menor do que 5 MIB. • Adicionado suporte para TLS 1,3
11,3	• Adicionado suporte para criptografia no lado do servidor de dados de objeto com chaves fornecidas pelo cliente (SSE-C). • Adicionado suporte para as operações DE ELIMINAÇÃO, OBTENÇÃO e COLOCAÇÃO do ciclo de vida do balde (apenas ação de expiração) e para o `x-amz-expiration` cabeçalho de resposta. • PUT Object, put Object - Copy e Multipart Upload atualizados para descrever o impactos das regras ILM que usam o posicionamento síncrono na ingestão. • As cifras TLS 1,1 não são mais suportadas.

Solte	Comentários
11,2	Adicionado suporte para restauração PÓS-objeto para uso com Cloud Storage Pools. Adicionado suporte para o uso da sintaxe da AWS para ARN, chaves de condição de política e variáveis de política em políticas de grupo e bucket. As políticas de grupo e bucket existentes que usam a sintaxe StorageGRID continuarão a ser suportadas. **Observação:** os usos de ARN/URN em outra configuração JSON/XML, incluindo aqueles usados em recursos personalizados do StorageGRID, não foram alterados.
11,1	Adicionado suporte para compartilhamento de recursos entre origens (CORS), HTTP para conexões de clientes S3 para nós de grade e configurações de conformidade em buckets.
11,0	Adicionado suporte para configuração de serviços de plataforma (replicação do CloudMirror, notificações e integração de pesquisa do Elasticsearch) para buckets. Também foi adicionado suporte para restrições de localização de marcação de objetos para buckets e a consistência disponível.
10,4	Adicionado suporte para alterações de verificação de ILM para controle de versão, atualizações de página de nomes de domínio de endpoints, condições e variáveis em políticas, exemplos de políticas e a permissão PutOverwriteObject.
10,3	Adicionado suporte para controle de versão.
10,2	Adicionado suporte para políticas de acesso de grupo e bucket, e para cópia de várias partes (Upload de peça - cópia).
10,1	Adicionado suporte para upload em várias partes, solicitações virtuais de estilo hospedado e autenticação v4.1X.
10,0	Suporte inicial da API REST do S3 pelo sistema StorageGRID. A versão atualmente suportada da *Simple Storage Service API Reference* é 2006-03-01.

Referência rápida: Solicitações de API S3 suportadas

Esta página resume como o StorageGRID oferece suporte às APIs do Amazon Simple Storage Service (S3).

Esta página inclui apenas as operações S3 com suporte do StorageGRID.

Para ver a documentação da AWS para cada operação, selecione o link no título.

Parâmetros comuns de consulta URI e cabeçalhos de solicitação

A menos que indicado, os seguintes parâmetros comuns de consulta URI são suportados:

- `versionId` (conforme necessário para operações de objetos)

Salvo indicação em contrário, os seguintes cabeçalhos de solicitação comuns são suportados:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informações relacionadas

- "Detalhes da implementação da API REST do S3"
- "Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns"

"AbortMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para esta solicitação, além deste parâmetro de consulta URI adicional:

- `uploadId`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações para uploads de várias partes"

"CompleteMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para esta solicitação, além deste parâmetro de consulta URI adicional:

- `uploadId`
- `x-amz-checksum-sha256`

Solicitar tags XML do corpo

O StorageGRID suporta essas tags XML do corpo de solicitação:

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`

- `Part`
- `PartNumber`

Documentação do StorageGRID

"CompleteMultipartUpload"

"CopyObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses cabeçalhos adicionais:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"CopyObject"

"CreateBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses cabeçalhos adicionais:

- `x-amz-bucket-object-lock-enabled`

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"CreateMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses cabeçalhos adicionais:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"CreateMultipartUpload"

"DeleteBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketLifecycle"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

- "Operações em baldes"
- "Crie a configuração do ciclo de vida do S3"

"DeleteBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação, além deste cabeçalho de solicitação adicional:

- `x-amz-bypass-governance-retention`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"DeleteObjects"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação, além deste cabeçalho de solicitação adicional:

- `x-amz-bypass-governance-retention`

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em objetos"

"DeleteObjectTagging"

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"GetBucketAcl"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"GetBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"GetBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"GetBucketLifecycleConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

- "Operações em baldes"
- "Crie a configuração do ciclo de vida do S3"

"GetBucketlocalização"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"GetBucketNotificationConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Política de GetBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"GetBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"GetBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"GetBucketControle de versão"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"GetObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

E esses cabeçalhos de solicitação adicionais:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"GetObject"

"GetObjectAcl"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"GetObjectLegalHod"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objetos do S3"

"GetObjectLockConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objetos do S3"

"GetObjectRetention"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objetos do S3"

"GetObjectTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"Balde para a cabeça"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"HeadObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses cabeçalhos adicionais:

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"HeadObject"

"ListBuckets"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

Operações no serviço › ListBuckets

"ListMultipartUploads"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses parâmetros adicionais:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"ListMultipartUploads"

"ListObjects"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses parâmetros adicionais:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ListObjectsV2"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses parâmetros adicionais:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ListObjectVersions"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses parâmetros adicionais:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ListParts"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses parâmetros adicionais:

- `max-parts`

- `part-number-marker`
- `uploadId`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"ListMultipartUploads"

"PutBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"PutBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Solicitar tags XML do corpo

O StorageGRID suporta essas tags XML do corpo de solicitação:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentação do StorageGRID

"Operações em baldes"

"PutBucketLifecycleConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Solicitar tags XML do corpo

O StorageGRID suporta essas tags XML do corpo de solicitação:

- `And`
- `Days`
- `Expiration`

- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentação do StorageGRID

- "Operações em baldes"
- "Crie a configuração do ciclo de vida do S3"

"PutBucketNotificationConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Solicitar tags XML do corpo

O StorageGRID suporta essas tags XML do corpo de solicitação:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentação do StorageGRID

"Operações em baldes"

"Política de PutBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Para obter detalhes sobre os campos de corpo JSON suportados, "Use políticas de acesso de grupo e bucket"consulte .

"PutBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Solicitar tags XML do corpo

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

Documentação do StorageGRID

"Operações em baldes"

"PutBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"PutBucketControle de versão"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Solicitar parâmetros do corpo

O StorageGRID suporta estes parâmetros do corpo do pedido:

- `VersioningConfiguration`
- `Status`

Documentação do StorageGRID

"Operações em baldes"

"PutObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para essa solicitação, além desses cabeçalhos adicionais:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo do pedido

- Dados binários do objeto

Documentação do StorageGRID

"PutObject"

"PutObjectLegalHod"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objetos do S3"

"PutObjectLockConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objetos do S3"

"Retenção PutObjectRetention"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para esta solicitação, além deste cabeçalho adicional:

- `x-amz-bypass-governance-retention`

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objetos do S3"

"Marcação de objetos"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em objetos"

"RestoreObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Para obter detalhes sobre os campos corpo suportados, "RestoreObject"consulte .

"Selecione ObjectContent"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo parâmetros e cabeçalhos comuns para essa solicitação.

Corpo do pedido

Para obter detalhes sobre os campos do corpo suportados, consulte o seguinte:

- "Utilize S3 Select (Selecionar)"
- "Selecione ObjectContent"

"UploadPart"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E esses cabeçalhos de solicitação adicionais:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corpo do pedido

- Dados binários da peça

Documentação do StorageGRID

"UploadPart"

"UploadPartCopy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo parâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E esses cabeçalhos de solicitação adicionais:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`

- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Corpo do pedido

Nenhum

Documentação do StorageGRID

"UploadPartCopy"

Teste a configuração da API REST do S3

Você pode usar a interface de linha de comando (AWS CLI) do Amazon Web Services para testar sua conexão com o sistema e verificar se é possível ler e gravar objetos.

Antes de começar

- Você baixou e instalou a AWS CLI do "aws.amazon.com/cli".
- Opcionalmente, você "criou um ponto de extremidade do balanceador de carga"tem . Caso contrário, você sabe o endereço IP do nó de armazenamento ao qual deseja se conetar e o número da porta a ser usado. "Endereços IP e portas para conexões de clientes"Consulte .
- Você "Criou uma conta de locatário do S3"tem .
- Você fez login no locatário e "criou uma chave de acesso"no .

Para obter detalhes sobre essas etapas, "Configurar conexões de cliente"consulte .

Passos

1. Configure as configurações da AWS CLI para usar a conta criada no sistema StorageGRID:
   a. Entre no modo de configuração: `aws configure`
   b. Introduza a ID da chave de acesso para a conta que criou.
   c. Introduza a chave de acesso secreta para a conta que criou.
   d. Introduza a região predefinida a utilizar. Por exemplo, `us-east-1`.
   e. Digite o formato de saída padrão a ser usado ou pressione **Enter** para selecionar JSON.
2. Crie um bucket.

   Este exemplo pressupõe que você tenha configurado um endpoint do balanceador de carga para usar o endereço IP 10.96.101.17 e a porta 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Se o bucket for criado com êxito, a localização do bucket será retornada, como visto no exemplo a seguir:

```
"Location": "/testbucket"
```

3. Carregue um objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Se o objeto for carregado com sucesso, um Etag é retornado que é um hash dos dados do objeto.

4. Liste o conteúdo do bucket para verificar se o objeto foi carregado.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Exclua o objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Elimine o balde.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Como o StorageGRID implementa a API REST do S3

Solicitações de cliente conflitantes

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes".

O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Valores de consistência

A consistência fornece um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de storage e locais. Você pode alterar a consistência conforme exigido pelo seu aplicativo.

Por padrão, o StorageGRID garante consistência de leitura após gravação para objetos recém-criados. Qualquer GET seguindo um PUT concluído com sucesso será capaz de ler os dados recém-escritos. As substituições de objetos existentes, atualizações de metadados e exclusões são, eventualmente, consistentes. As substituições geralmente levam segundos ou minutos para se propagar, mas podem levar até 15 dias.

Se você quiser executar operações de objeto em uma consistência diferente, você pode:

- Especifique uma consistência para cada baldeo .
- Especifique uma consistência para Cada operação da APIo .
- Altere a consistência padrão em toda a grade executando uma das seguintes tarefas:
  - No Gerenciador de Grade, vá para **CONFIGURATION** > **System** > **Storage settings** > **Default consistency**.
  - .

> Uma alteração na consistência em toda a grade se aplica somente aos buckets criados após a alteração da configuração. Para determinar os detalhes de uma alteração, consulte o log de auditoria localizado em `/var/local/log` (procure **consistencyLevel**).

Valores de consistência

A consistência afeta como os metadados que o StorageGRID usa para rastrear objetos são distribuídos entre nós e, portanto, a disponibilidade de objetos para solicitações de clientes.

Você pode definir a consistência de um bucket ou uma operação de API para um dos seguintes valores:

- **Todos**: Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
- **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- * Strong-site*: Garante consistência de leitura-após-gravação para todas as solicitações de clientes dentro de um site.
- **Read-after-novo-write**: (Padrão) fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
- **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

Use a consistência "Read-after-new-write" e "Available"

Quando uma operação HEAD ou GET usa a consistência "Read-after-new-write", o StorageGRID realiza a pesquisa em várias etapas, como segue:

- Ele primeiro procura o objeto usando uma baixa consistência.
- Se essa pesquisa falhar, ela repete a pesquisa no próximo valor de consistência até atingir uma consistência equivalente ao comportamento para strong-global.

Se uma operação HEAD ou GET usa a consistência "Read-after-new-write", mas o objeto não existe, a pesquisa de objeto sempre alcançará uma consistência equivalente ao comportamento para strong-global. Como essa consistência exige que várias cópias dos metadados de objetos estejam disponíveis em cada local, você pode receber um número alto de erros de servidor interno do 500 se dois ou mais nós de storage no mesmo local não estiverem disponíveis.

A menos que você exija garantias de consistência semelhantes ao Amazon S3, você pode evitar esses erros para operações HEAD and GET definindo a consistência como "disponível". Quando uma operação HEAD ou GET usa a consistência "disponível", o StorageGRID fornece consistência eventual apenas. Ele não tenta novamente uma operação com falha em aumentar a consistência, portanto, não requer que várias cópias dos metadados do objeto estejam disponíveis.

Especifique a consistência para a operação da API

Para definir a consistência para uma operação de API individual, os valores de consistência devem ser suportados para a operação e você deve especificar a consistência no cabeçalho da solicitação. Este exemplo define a consistência como "strong-site" para uma operação GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

> Você deve usar a mesma consistência para as operações PutObject e GetObject.

Especifique a consistência para o bucket

Para definir a consistência do bucket, você pode usar a solicitação StorageGRID"COLOQUE a consistência do balde". Ou você pode "altere a consistência de um balde" do Gerente do Locatário.

Ao definir a consistência de um balde, tenha em atenção o seguinte:

- Definir a consistência de um bucket determina qual consistência é usada para operações S3D executadas nos objetos no bucket ou na configuração do bucket. Não afeta as operações no próprio balde.
- A consistência de uma operação de API individual substitui a consistência do bucket.
- Em geral, os intervalos devem usar a consistência padrão, "Read-after-new-write". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar a consistência para cada solicitação de API. Defina a consistência no nível do balde apenas como último recurso.

como a consistência e as regras ILM interagem para afetar a proteção de dados

Tanto a sua escolha de consistência quanto a sua regra ILM afetam a forma como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, a consistência usada quando um objeto é armazenado afeta o posicionamento inicial dos

metadados do objeto, enquanto o comportamento de ingestão selecionado para a regra ILM afeta o posicionamento inicial das cópias do objeto. Como o StorageGRID exige acesso aos metadados de um objeto e aos dados para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para o comportamento de consistência e ingestão pode fornecer melhor proteção de dados iniciais e respostas do sistema mais previsíveis.

Estão disponíveis as seguintes "opções de ingestão"regras para ILM:

Commit duplo
: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

Rigoroso
: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido ao cliente.

Equilibrado
: O StorageGRID tenta fazer todas as cópias especificadas na regra ILM na ingestão; se isso não for possível, cópias provisórias são feitas e o sucesso é retornado ao cliente. As cópias especificadas na regra ILM são feitas quando possível.

Exemplo de como a consistência e a regra ILM podem interagir

Suponha que você tenha uma grade de dois locais com a seguinte regra ILM e a seguinte consistência:

- **Regra ILM**: Crie duas cópias de objeto, uma no local e outra em um local remoto. Use um comportamento rigoroso de ingestão.
- **Consistência**: Strong-global (metadados de objetos são imediatamente distribuídos para todos os sites).

Quando um cliente armazena um objeto na grade, o StorageGRID faz cópias de objeto e distribui metadados para ambos os sites antes de retornar sucesso ao cliente.

O objeto é totalmente protegido contra perda no momento da mensagem de ingestão bem-sucedida. Por exemplo, se o local for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existem no local remoto. O objeto é totalmente recuperável.

Se, em vez disso, você usou a mesma regra ILM e a consistência do site forte, o cliente pode receber uma mensagem de sucesso depois que os dados do objeto são replicados para o site remoto, mas antes que os metadados do objeto sejam distribuídos lá. Nesse caso, o nível de proteção dos metadados de objetos não corresponde ao nível de proteção dos dados de objeto. Se o site local for perdido logo após a ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Controle de versão de objetos

Você pode definir o estado de controle de versão de um bucket se quiser reter várias versões de cada objeto. Ativar o controle de versão para um bucket pode ajudar a proteger contra a exclusão acidental de objetos e permite que você recupere e restaure versões anteriores de um objeto.

O sistema StorageGRID implementa o controle de versão com suporte para a maioria dos recursos, e com

algumas limitações. O StorageGRID suporta até 10.000 versões de cada objeto.

O controle de versão de objetos pode ser combinado com o gerenciamento do ciclo de vida das informações do StorageGRID (ILM) ou com a configuração do ciclo de vida do bucket do S3. Você deve habilitar explicitamente o controle de versão para cada bucket. Quando o controle de versão é ativado para um bucket, cada objeto adicionado ao bucket recebe um ID de versão, que é gerado pelo sistema StorageGRID.

O uso de MFA (autenticação multifator) Excluir não é compatível.

> O controle de versão pode ser ativado somente em buckets criados com o StorageGRID versão 10,3 ou posterior.

ILM e versionamento

As políticas de ILM são aplicadas a cada versão de um objeto. Um processo de digitalização ILM verifica continuamente todos os objetos e os reavalia em relação à política ILM atual. Quaisquer alterações feitas às políticas ILM são aplicadas a todos os objetos ingeridos anteriormente. Isso inclui versões ingeridas anteriormente se o controle de versão estiver ativado. A digitalização ILM aplica novas alterações ILM a objetos ingeridos anteriormente.

Para objetos S3 em buckets habilitados para versionamento, o suporte para versionamento permite criar regras ILM que usam "tempo não atual" como tempo de referência (selecione **Sim** para a pergunta, "aplicar esta regra apenas a versões de objetos mais antigos?" no "Etapa 1 do assistente criar uma regra ILM"). Quando um objeto é atualizado, suas versões anteriores se tornam não atuais. O uso de um filtro "tempo não atual" permite criar políticas que reduzem o impactos de armazenamento de versões anteriores de objetos.

> Quando você carrega uma nova versão de um objeto usando uma operação de upload multipart, o tempo não atual para a versão original do objeto reflete quando o upload multipart foi criado para a nova versão, não quando o upload multipart foi concluído. Em casos limitados, o tempo não atual para a versão original pode ser horas ou dias antes do tempo para a versão atual.

Informações relacionadas

- "Como objetos com versão S3 são excluídos"
- "Regras e políticas do ILM para objetos com versão S3 (exemplo 4)".

Use a API REST do S3 para configurar o bloqueio de objetos do S3

Se a configuração global de bloqueio de objetos S3 estiver ativada para o seu sistema StorageGRID, você poderá criar buckets com o bloqueio de objetos S3 ativado. Você pode especificar a retenção padrão para cada bucket ou configurações de retenção para cada versão do objeto.

Como ativar o bloqueio de objetos S3D para um balde

Se a configuração global de bloqueio de objetos S3 estiver ativada para o seu sistema StorageGRID, você poderá ativar opcionalmente o bloqueio de objetos S3 quando criar cada bucket.

S3 Object Lock é uma configuração permanente que só pode ser ativada quando você cria um bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um bucket.

Para ativar o bloqueio de objetos S3D para um bucket, use um destes métodos:

- Crie o bucket usando o Gerenciador do locatário. "Crie um balde S3D."Consulte .
- Crie o bucket usando uma solicitação CreateBucket com o `x-amz-bucket-object-lock-enabled` cabeçalho da solicitação. "Operações em baldes"Consulte .

O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando o bucket é criado. Não é possível suspender o controle de versão para o bucket. "Controle de versão de objetos"Consulte .

Configurações de retenção padrão para um balde

Quando o bloqueio de objetos S3D está ativado para um bucket, você pode opcionalmente habilitar a retenção padrão para o bucket e especificar um modo de retenção padrão e um período de retenção padrão.

Modo de retenção predefinido

- No modo DE CONFORMIDADE:
  - O objeto não pode ser excluído até que sua data de retenção seja alcançada.
  - O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- No MODO DE GOVERNANÇA:
  - Os usuários com `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as configurações de retenção.
  - Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada.
  - Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto.

Período de retenção predefinido

Cada bucket pode ter um período de retenção padrão especificado em anos ou dias.

Como definir a retenção padrão para um balde

Para definir a retenção padrão para um bucket, use um destes métodos:

- Gerencie as configurações do balde a partir do Gerenciador do Locatário. "Crie um bucket do S3"Consulte e "Atualização S3 retenção padrão bloqueio Objeto".
- Emita uma solicitação PutObjectLockConfiguration para que o bucket especifique o modo padrão e o número padrão de dias ou anos.

PutObjectLockConfiguration

A solicitação PutObjectLockConfiguration permite que você defina e modifique o modo de retenção padrão e o período de retenção padrão para um bucket com o bloqueio de objetos S3 ativado. Você também pode remover as configurações de retenção padrão configuradas anteriormente.

Quando novas versões de objetos são ingeridas para o bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` e `x-amz-object-lock-retain-until-date` não forem especificados. O período de retenção padrão é usado para calcular a data de retenção até se `x-amz-object-lock-retain-until-date` não for especificado.

Se o período de retenção padrão for modificado após a ingestão de uma versão de objeto, a data de retenção até a versão do objeto permanecerá a mesma e não será recalculada usando o novo período de retenção padrão.

Você deve ter a `s3:PutBucketObjectLockConfiguration` permissão, ou ser raiz da conta, para concluir esta operação.

O `Content-MD5` cabeçalho da solicitação deve ser especificado na solicitação DE COLOCAÇÃO.

Exemplo de solicitação

Este exemplo habilita o bloqueio de objetos S3 para um bucket e define o modo de retenção padrão para CONFORMIDADE e o período de retenção padrão para 6 anos.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Como determinar a retenção padrão para um balde

Para determinar se o bloqueio de objeto S3 está ativado para um bucket e para ver o modo de retenção e o período de retenção padrão, use um destes métodos:

- Veja o bucket no Gerenciador do Locatário. "Veja os baldes do S3"Consulte .
- Emita uma solicitação GetObjectLockConfiguration.

GetObjectLockConfiguration

A solicitação GetObjectLockConfiguration permite que você determine se o bloqueio de objeto S3 está ativado para um bucket e, se ele está ativado, veja se há um modo de retenção padrão e período de retenção configurados para o bucket.

Quando novas versões de objetos são ingeridas para o bucket, o modo de retenção padrão é aplicado se `x-`

`amz-object-lock-mode` não for especificado. O período de retenção padrão é usado para calcular a data de retenção até se `x-amz-object-lock-retain-until-date` não for especificado.

Você deve ter a `s3:GetBucketObjectLockConfiguration` permissão, ou ser raiz da conta, para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Exemplo de resposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Como especificar configurações de retenção para um objeto

Um bucket com o bloqueio de objetos S3 ativado pode conter uma combinação de objetos com e sem as configurações de retenção do bloqueio de objetos S3.

As configurações de retenção no nível do objeto são especificadas usando a API REST do S3. As configurações de retenção de um objeto substituem quaisquer configurações de retenção padrão para o

bucket.

Você pode especificar as seguintes configurações para cada objeto:

- **Modo de retenção**: CONFORMIDADE ou GOVERNANÇA.
- **Retent-until-date**: Uma data especificando quanto tempo a versão do objeto deve ser mantida pelo StorageGRID.
  - No modo DE CONFORMIDADE, se a data de retenção estiver no futuro, o objeto pode ser recuperado, mas não pode ser modificado ou excluído. A data de retenção até pode ser aumentada, mas esta data não pode ser diminuída ou removida.
  - No MODO DE GOVERNANÇA, os usuários com permissão especial podem ignorar a configuração reter até a data. Eles podem excluir uma versão de objeto antes que seu período de retenção tenha decorrido. Eles também podem aumentar, diminuir ou até mesmo remover a data de retenção.
- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar colocar uma retenção legal em um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até que seja explicitamente removida.

  A configuração de retenção legal para um objeto é independente do modo de retenção e da data de retenção. Se uma versão de objeto estiver sob uma retenção legal, ninguém poderá excluir essa versão.

Para especificar as configurações de bloqueio de objetos do S3 ao adicionar uma versão de objeto a um bucket, emita uma solicitação"PutObject" , "CopyObject"ou "CreateMultipartUpload".

Você pode usar o seguinte:

- `x-amz-object-lock-mode`, Que pode ser CONFORMIDADE ou GOVERNANÇA (diferencia maiúsculas de minúsculas).

  > Se você especificar `x-amz-object-lock-mode`, você também deve especificar `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - O valor reter-até-data deve estar no formato `2020-08-10T21:46:00Z`. Segundos fracionários são permitidos, mas apenas 3 dígitos decimais são preservados (precisão de milissegundos). Outros formatos ISO 8601 não são permitidos.
  - A data de retenção deve ser no futuro.
- `x-amz-object-lock-legal-hold`

  Se a retenção legal estiver ATIVADA (sensível a maiúsculas e minúsculas), o objeto é colocado sob uma retenção legal. Se a retenção legal estiver DESLIGADA, nenhuma retenção legal será colocada. Qualquer outro valor resulta em um erro de 400 Bad Request (InvalidArgument).

Se você usar qualquer um desses cabeçalhos de solicitação, esteja ciente dessas restrições:

- O `Content-MD5` cabeçalho de solicitação é necessário se qualquer `x-amz-object-lock-*` cabeçalho de solicitação estiver presente na solicitação PutObject. `Content-MD5` Não é necessário para CopyObject ou CreateMultipartUpload.
- Se o bucket não tiver o bloqueio de objeto S3 ativado e um `x-amz-object-lock-*` cabeçalho de

solicitação estiver presente, um erro de solicitação incorreta 400 (InvalidRequest) será retornado.

- A solicitação PutObject suporta o uso do `x-amz-storage-class: REDUCED_REDUNDANCY` para corresponder ao comportamento da AWS. No entanto, quando um objeto é ingerido em um bucket com o bloqueio de objeto S3 ativado, o StorageGRID sempre realizará uma ingestão de confirmação dupla.
- Uma resposta DE versão GET ou HeadObject posterior incluirá os cabeçalhos `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e `x-amz-object-lock-legal-hold`, se configurado e se o remetente da solicitação tiver as permissões corretas `s3:Get*`.

Você pode usar a `s3:object-lock-remaining-retention-days` chave de condição de política para limitar os períodos de retenção mínimo e máximo permitidos para seus objetos.

Como atualizar as configurações de retenção para um objeto

Se você precisar atualizar as configurações de retenção legal ou retenção para uma versão de objeto existente, poderá executar as seguintes operações de subrecursos de objeto:

- `PutObjectLegalHold`

  Se o novo valor de retenção legal estiver ATIVADO, o objeto será colocado sob uma retenção legal. Se o valor de retenção legal estiver DESLIGADO, a retenção legal é levantada.

- `PutObjectRetention`
  - O valor do modo pode ser CONFORMIDADE ou GOVERNANÇA (sensível a maiúsculas e minúsculas).
  - O valor reter-até-data deve estar no formato `2020-08-10T21:46:00Z`. Segundos fracionários são permitidos, mas apenas 3 dígitos decimais são preservados (precisão de milissegundos). Outros formatos ISO 8601 não são permitidos.
  - Se uma versão de objeto tiver uma data retida-até-data existente, você só poderá aumentá-la. O novo valor deve estar no futuro.

Como usar o modo DE GOVERNANÇA

Os usuários que têm a `s3:BypassGovernanceRetention` permissão podem ignorar as configurações de retenção ativa de um objeto que usa o modo DE GOVERNANÇA. Qualquer operação DE EXCLUSÃO ou PutObjectRetention deve incluir o `x-amz-bypass-governance-retention:true` cabeçalho da solicitação. Esses usuários podem executar essas operações adicionais:

- Execute as operações DeleteObject ou DeleteObjects para excluir uma versão do objeto antes de seu período de retenção ter decorrido.

  Os objetos que estão sob uma retenção legal não podem ser excluídos. A retenção legal deve estar DESLIGADA.

- Execute as operações PutObjectRetention que alteram o modo DE uma versão DE objeto DE GOVERNANÇA para CONFORMIDADE antes que o período de retenção do objeto tenha decorrido.

  Alterar o modo DE CONFORMIDADE para GOVERNANÇA nunca é permitido.

- Execute operações PutObjectRetention para aumentar, diminuir ou remover o período de retenção de uma versão de objeto.

Informações relacionadas

- "Gerencie objetos com o S3 Object Lock"
- "Use o bloqueio de objetos S3D para reter objetos"
- "Guia do usuário do Amazon Simple Storage Service: Bloqueando objetos"

Crie a configuração do ciclo de vida do S3

Você pode criar uma configuração de ciclo de vida do S3 para controlar quando objetos específicos são excluídos do sistema StorageGRID.

O exemplo simples nesta seção ilustra como uma configuração do ciclo de vida do S3 pode controlar quando certos objetos são excluídos (expirados) de buckets específicos do S3. O exemplo nesta seção é apenas para fins ilustrativos. Para obter detalhes completos sobre como criar configurações de ciclo de vida do S3, "Guia do usuário do Amazon Simple Storage Service: Gerenciamento do ciclo de vida do objeto" consulte . Observe que o StorageGRID suporta apenas ações de expiração; ele não oferece suporte a ações de transição.

Qual é a configuração do ciclo de vida

Uma configuração de ciclo de vida é um conjunto de regras que são aplicadas aos objetos em buckets específicos do S3. Cada regra especifica quais objetos são afetados e quando esses objetos expirarão (em uma data específica ou após algum número de dias).

O StorageGRID dá suporte a até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML:

- Expiração: Exclua um objeto quando uma data especificada é atingida ou quando um número especificado de dias é atingido, a partir de quando o objeto foi ingerido.
- NoncurrentVersionExpiration: Exclua um objeto quando um número especificado de dias é atingido, a partir de quando o objeto se tornou inatual.
- Filtro (prefixo, Tag)
- Estado
- ID

Cada objeto segue as configurações de retenção de um ciclo de vida do bucket do S3 ou de uma política de ILM. Quando um ciclo de vida do bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política ILM para objetos que correspondam ao filtro do ciclo de vida do bucket. Os objetos que não correspondem ao filtro do ciclo de vida do bucket usam as configurações de retenção da política ILM. Se um objeto corresponder a um filtro do ciclo de vida do bucket e nenhuma ação de expiração for explicitamente especificada, as configurações de retenção da política ILM não serão usadas e está implícito que as versões do objeto serão mantidas para sempre. "Exemplos de prioridades para o ciclo de vida do bucket do S3 e a política de ILM"Consulte .

Como resultado, um objeto pode ser removido da grade, mesmo que as instruções de colocação em uma regra ILM ainda se apliquem ao objeto. Ou, um objeto pode ser retido na grade mesmo depois que quaisquer instruções de colocação de ILM para o objeto tiverem expirado. Para obter detalhes, "Como o ILM opera ao longo da vida de um objeto"consulte .

> ⓘ A configuração do ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis com legado.

O StorageGRID dá suporte ao uso das seguintes operações de bucket para gerenciar configurações do ciclo

de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Criar configuração do ciclo de vida

Como primeira etapa na criação de uma configuração de ciclo de vida, você cria um arquivo JSON que inclui uma ou mais regras. Por exemplo, este arquivo JSON inclui três regras, como segue:

1. A regra 1 aplica-se apenas a objetos que correspondam ao prefixo `category1/` e que tenham um `key2` valor `tag2` de . O `Expiration` parâmetro especifica que os objetos correspondentes ao filtro expirarão à meia-noite de 22 de agosto de 2020.
2. A regra 2 aplica-se apenas a objetos que correspondam ao prefixo `category2/`. O `Expiration` parâmetro especifica que os objetos correspondentes ao filtro expirarão 100 dias após serem ingeridos.

   > As regras que especificam um número de dias são relativas a quando o objeto foi ingerido. Se a data atual exceder a data de ingestão mais o número de dias, alguns objetos podem ser removidos do intervalo assim que a configuração do ciclo de vida for aplicada.

3. A regra 3 aplica-se apenas a objetos que correspondam ao prefixo `category3/`. O `Expiration` parâmetro especifica que quaisquer versões não atuais de objetos correspondentes expirarão 50 dias após se tornarem não atuais.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplique a configuração do ciclo de vida ao bucket

Depois de criar o arquivo de configuração do ciclo de vida, você o aplica a um bucket emitindo uma solicitação PutBucketLifecycleConfiguration.

Essa solicitação aplica a configuração do ciclo de vida no arquivo de exemplo a objetos em um bucket `testbucket` chamado .

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que uma configuração de ciclo de vida foi aplicada com sucesso ao bucket, emita uma solicitação GetBucketLifecycleConfiguration. Por exemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Uma resposta bem-sucedida lista a configuração do ciclo de vida que você acabou de aplicar.

Valide que a expiração do ciclo de vida do bucket se aplica ao objeto

Você pode determinar se uma regra de expiração na configuração do ciclo de vida se aplica a um objeto específico ao emitir uma solicitação PutObject, HeadObject ou GetObject. Se uma regra se aplicar, a resposta inclui um `Expiration` parâmetro que indica quando o objeto expira e qual regra de expiração foi correspondida.

> ⓘ Como o ciclo de vida do bucket substitui o ILM, a `expiry-date` mostrada é a data real em que o objeto será excluído. Para obter detalhes, "Como a retenção de objetos é determinada"consulte .

Por exemplo, essa solicitação PutObject foi emitida em 22 de junho de 2020 e coloca um objeto no `testbucket` intervalo.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

A resposta de sucesso indica que o objeto expirará em 100 dias (01 de outubro de 2020) e que correspondia à regra 2 da configuração do ciclo de vida.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Por exemplo, essa solicitação do HeadObject foi usada para obter metadados para o mesmo objeto no bucket do testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

A resposta de sucesso inclui os metadados do objeto e indica que o objeto expirará em 100 dias e que correspondia à regra 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Para buckets habilitados para controle de versão, o `x-amz-expiration` cabeçalho de resposta se aplica apenas às versões atuais dos objetos.

Recomendações para a implementação da API REST do S3

Você deve seguir estas recomendações ao implementar a API REST do S3 para uso com o StorageGRID.

Recomendações para heads to non-existent objects

Se o aplicativo verificar rotineiramente se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o "disponível" "consistência". Por exemplo, você deve usar a consistência "disponível" se seu aplicativo dirigir um local antes DE COLOCÁ-lo.

Caso contrário, se a operação PRINCIPAL não encontrar o objeto, poderá receber um número elevado de erros de servidor interno 500 se dois ou mais nós de armazenamento no mesmo local não estiverem disponíveis ou se um local remoto não estiver acessível.

Você pode definir a consistência "disponível" para cada bucket usando a "COLOQUE a consistência do balde" solicitação ou especificar a consistência no cabeçalho da solicitação para uma operação de API individual.

Recomendações para chaves de objeto

Siga estas recomendações para nomes de chave de objeto, com base em quando o intervalo foi criado pela primeira vez.

Buckets criados no StorageGRID 11,4 ou anterior

- Não use valores aleatórios como os primeiros quatro carateres de chaves de objeto. Isso contrasta com a antiga recomendação da AWS para prefixos-chave. Em vez disso, use prefixos não aleatórios e não exclusivos, como `image` .
- Se você seguir a antiga recomendação da AWS para usar carateres aleatórios e exclusivos em prefixos de chave, prefix as chaves de objeto com um nome de diretório. Ou seja, use este formato:

  `mybucket/mydir/f8e3-image3132.jpg`

  Em vez deste formato:

  `mybucket/f8e3-image3132.jpg`

Buckets criados no StorageGRID 11,4 ou posterior

Não é necessário restringir nomes de chaves de objeto para atender às práticas recomendadas de desempenho. Na maioria dos casos, você pode usar valores aleatórios para os primeiros quatro carateres de nomes de chave de objeto.

> Uma exceção a isso é uma carga de trabalho S3 que remove continuamente todos os objetos após um curto período de tempo. Para minimizar o impacto no desempenho desse caso de uso, varie uma parte principal do nome da chave a cada milhares de objetos com algo como a data. Por exemplo, suponha que um cliente S3 normalmente grava 2.000 objetos/segundo e que a política de ciclo de vida ILM ou bucket remove todos os objetos após três dias. Para minimizar o impactos no desempenho, você pode nomear chaves usando um padrão como este: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recomendações para "leituras de intervalo"

Se o "opção global para comprimir objetos armazenados" estiver ativado, os aplicativos cliente S3 devem evitar executar operações GetObject que especificam um intervalo de bytes que sejam retornados. Essas operações de "leitura de intervalo" são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GetObject que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

Se os intervalos forem lidos a partir de objetos compatados, as solicitações do cliente podem expirar.

> Se você precisar compactar objetos e seu aplicativo cliente precisar usar leituras de intervalo, aumente o tempo limite de leitura para o aplicativo.

Suporte para API REST do Amazon S3

Detalhes da implementação da API REST do S3

O sistema StorageGRID implementa a API de serviço de armazenamento simples (API versão 2006-03-01) com suporte para a maioria das operações e com algumas

limitações. Você precisa entender os detalhes da implementação quando você está integrando aplicativos clientes REST API do S3.

O sistema StorageGRID oferece suporte a solicitações virtuais de estilo hospedado e a solicitações de estilo de caminho.

Tratamento da data

A implementação do StorageGRID da API REST S3 suporta apenas formatos de data HTTP válidos.

O sistema StorageGRID suporta apenas formatos de data HTTP válidos para qualquer cabeçalho que aceite valores de data. A parte da hora da data pode ser especificada no formato Greenwich Mean Time (GMT) ou no formato Universal Coordinated Time (UTC) sem deslocamento de fuso horário (o 0000 deve ser especificado). Se você incluir o `x-amz-date` cabeçalho em sua solicitação, ele substituirá qualquer valor especificado no cabeçalho da solicitação de data. Ao usar o AWS Signature versão 4, o `x-amz-date` cabeçalho deve estar presente na solicitação assinada porque o cabeçalho de data não é suportado.

Cabeçalhos de solicitação comuns

O sistema StorageGRID suporta os cabeçalhos de solicitação comuns definidos pelo "Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns", com uma exceção.

Cabeçalho da solicitação	Implementação
Autorização	Suporte completo para AWS Signature versão 2 Suporte para AWS Signature versão 4, com as seguintes exceções: • Quando você fornece o valor real da soma de verificação da carga útil no `x-amz-content-sha256`, o valor é aceito sem validação, como se o valor `UNSIGNED-PAYLOAD` tivesse sido fornecido para o cabeçalho. Quando você fornece um `x-amz-content-sha256` valor de cabeçalho que implica `aws-chunked` streaming (por exemplo, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), as assinaturas de bloco não são verificadas em relação aos dados de bloco.
x-amz-security-token	Não implementado. Retorna `XNotImplemented`.

Cabeçalhos de resposta comuns

O sistema StorageGRID suporta todos os cabeçalhos de resposta comuns definidos pela *Simple Storage Service API Reference*, com uma exceção.

Cabeçalho de resposta	Implementação
x-amz-id-2	Não utilizado

Autenticar solicitações

O sistema StorageGRID suporta acesso autenticado e anônimo a objetos usando a API S3.

A API S3 suporta a assinatura versão 2 e a assinatura versão 4 para autenticar solicitações de API S3.

As solicitações autenticadas devem ser assinadas usando seu ID de chave de acesso e chave de acesso secreta.

O sistema StorageGRID suporta dois métodos de autenticação: O cabeçalho HTTP `Authorization` e o uso de parâmetros de consulta.

Use o cabeçalho de autorização HTTP

O cabeçalho HTTP `Authorization` é usado por todas as operações da API S3, exceto solicitações anônimas, onde permitido pela política de bucket. O `Authorization` cabeçalho contém todas as informações de assinatura necessárias para autenticar uma solicitação.

Use parâmetros de consulta

Você pode usar parâmetros de consulta para adicionar informações de autenticação a um URL. Isso é conhecido como pré-assinar o URL, que pode ser usado para conceder acesso temporário a recursos específicos. Os usuários com o URL pré-assinado não precisam saber a chave de acesso secreto para acessar o recurso, o que permite que você forneça acesso restrito de terceiros a um recurso.

Operações no serviço

O sistema StorageGRID suporta as seguintes operações no serviço.

Operação	Implementação
ListBuckets (Anteriormente chamado GET Service)	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.
OBTER uso de armazenamento	A solicitação do StorageGRID "OBTER uso de armazenamento"informa a quantidade total de storage em uso por uma conta e para cada bucket associado à conta. Esta é uma operação no serviço com um caminho de / e um parâmetro de consulta personalizado (`?x-ntap-sg-usage`) adicionado.
OPÇÕES /	Os aplicativos clientes podem emitir `OPTIONS /` solicitações para a porta S3 em um nó de storage, sem fornecer credenciais de autenticação S3.1X, para determinar se o nó de storage está disponível. Você pode usar essa solicitação para monitoramento ou permitir que balanceadores de carga externos identifiquem quando um nó de storage está inativo.

Operações em baldes

O sistema StorageGRID dá suporte a um máximo de 5.000 buckets para cada conta de locatário de S3 TB.

Cada grade pode ter um máximo de 100.000 baldes.

Para suportar buckets do 5.000, cada nó de armazenamento na grade deve ter um mínimo de 64 GB de RAM.

As restrições de nome de bucket seguem as restrições de região padrão dos EUA da AWS, mas você deve restringi-las ainda mais a convenções de nomenclatura de DNS para oferecer suporte a solicitações de estilo hospedado virtual S3.

Consulte o seguinte para obter mais informações:

- "Guia do usuário do Amazon Simple Storage Service: Cotas, restrições e limitações de bucket"
- "Configurar nomes de domínio de endpoint S3"

As operações ListObjects (GET Bucket) e ListObjectVersions (GET Bucket object versions) suportam StorageGRID "valores de consistência".

Você pode verificar se as atualizações para a última hora de acesso estão ativadas ou desativadas para buckets individuais. "OBTER último tempo de acesso do Bucket"Consulte .

A tabela a seguir descreve como o StorageGRID implementa as operações de bucket da API REST do S3. Para realizar qualquer uma dessas operações, as credenciais de acesso necessárias devem ser fornecidas para a conta.

Operação	Implementação
CreateBucket	Cria um novo balde. Ao criar o balde, você se torna o proprietário do balde. • Os nomes dos buckets devem estar em conformidade com as seguintes regras: ◦ Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). ◦ Deve ser compatível com DNS. ◦ Deve conter pelo menos 3 e não mais de 63 carateres. ◦ Pode ser uma série de uma ou mais etiquetas, com etiquetas adjacentes separadas por um período. Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens. ◦ Não deve se parecer com um endereço IP formatado em texto. ◦ Não deve usar períodos em solicitações de estilo hospedadas virtuais. Os períodos causarão problemas com a verificação do certificado curinga do servidor. • Por padrão, os intervalos são criados na `us-east-1` região; no entanto, você pode usar o `LocationConstraint` elemento de solicitação no corpo da solicitação para especificar uma região diferente. Ao usar o `LocationConstraint` elemento, você deve especificar o nome exato de uma região que foi definida usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Contacte o administrador do sistema se não souber o nome da região que deve utilizar. **Nota**: Ocorrerá um erro se a solicitação do CreateBucket usar uma região que não foi definida no StorageGRID. • Você pode incluir o `x-amz-bucket-object-lock-enabled` cabeçalho de solicitação para criar um bucket com o bloqueio de objeto S3 ativado. "Use a API REST do S3 para configurar o bloqueio de objetos do S3"Consulte . Você deve ativar o bloqueio de objeto S3 quando você criar o bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um bucket. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.
DeleteBucket	Elimina o balde.
DeleteBucketCors	Exclui a configuração CORS para o bucket.
DeleteBucketEncryption	Exclui a criptografia padrão do intervalo. Os objetos criptografados existentes permanecem criptografados, mas todos os novos objetos adicionados ao bucket não são criptografados.
DeleteBucketLifecycle	Exclui a configuração do ciclo de vida do bucket. "Crie a configuração do ciclo de vida do S3"Consulte .

Operação	Implementação
DeleteBucketPolicy	Exclui a política anexada ao bucket.
DeleteBucketReplication	Exclui a configuração de replicação anexada ao bucket.
DeleteBucketTagging	Usa o `tagging` subrecurso para remover todas as tags de um bucket. **Atenção**: Se uma tag de política ILM não padrão for definida para esse intervalo, haverá uma `NTAP-SG-ILM-BUCKET-TAG` tag de intervalo com um valor atribuído a ele. Não emita uma solicitação de identificação de DeleteBucketTagging se houver uma `NTAP-SG-ILM-BUCKET-TAG` etiqueta de intervalo. Em vez disso, emita uma solicitação PutBucketTagging com apenas a `NTAP-SG-ILM-BUCKET-TAG` tag e seu valor atribuído para remover todas as outras tags do bucket. Não modifique nem remova a `NTAP-SG-ILM-BUCKET-TAG` etiqueta do balde.
GetBucketAcl	Retorna uma resposta positiva e a ID, DisplayName e permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
GetBucketCors	Retorna a `cors` configuração para o bucket.
GetBucketEncryption	Retorna a configuração de criptografia padrão para o bucket.
GetBucketLifecycleConfiguration (Anteriormente chamado GET Bucket Lifecycle)	Retorna a configuração do ciclo de vida do bucket. "Crie a configuração do ciclo de vida do S3"Consulte .
GetBucketlocalização	Retorna a região que foi definida usando o `LocationConstraint` elemento na solicitação CreateBucket. Se a região do bucket for `us-east-1`, uma string vazia será retornada para a região.
GetBucketNotificationConfiguration (Anteriormente chamado GET Bucket notificação)	Retorna a configuração de notificação anexada ao bucket.
Política de GetBucketPolicy	Retorna a política anexada ao bucket.
GetBucketReplication	Retorna a configuração de replicação anexada ao bucket.

Operação	Implementação
GetBucketTagging	Usa o `tagging` subrecurso para retornar todas as tags para um bucket. **Atenção**: Se uma tag de política ILM não padrão for definida para esse intervalo, haverá uma `NTAP-SG-ILM-BUCKET-TAG` tag de intervalo com um valor atribuído a ele. Não modifique nem remova esta etiqueta.
GetBucketControle de versão	Essa implementação usa `versioning` o subrecurso para retornar o estado de controle de versão de um bucket. • *Blank*: O controle de versão nunca foi habilitado (bucket é "não versionado") • Habilitado: O controle de versão está habilitado • Suspenso: O controle de versão foi ativado anteriormente e está suspenso
GetObjectLockConfiguration	Retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurado. "Use a API REST do S3 para configurar o bloqueio de objetos do S3"Consulte .
Balde para a cabeça	Determina se existe um intervalo e você tem permissão para acessá-lo. Esta operação retorna: • `x-ntap-sg-bucket-id`: O UUID do bucket no formato UUID. • `x-ntap-sg-trace-id`: O ID de rastreamento exclusivo da solicitação associada.
ListObjects e ListObjectsV2 (Anteriormente chamado GET Bucket)	Retorna alguns ou todos (até 1.000) dos objetos em um bucket. A Classe de armazenamento para objetos pode ter um de dois valores, mesmo que o objeto tenha sido ingerido com a `REDUCED_REDUNDANCY` opção de classe de armazenamento: • `STANDARD`, Que indica que o objeto está armazenado em um pool de storage que consiste em nós de storage. • `GLACIER`, Que indica que o objeto foi movido para o bucket externo especificado pelo pool de armazenamento em nuvem. Se o intervalo contiver um grande número de chaves excluídas que tenham o mesmo prefixo, a resposta pode incluir algumas `CommonPrefixes` que não contêm chaves.
ListObjectVersions (Anteriormente CHAMADO OBTER versões de objetos bucket)	Com ACESSO DE LEITURA em um bucket, o uso dessa operação com o `versions` subrecurso lista metadados de todas as versões de objetos no bucket.

Operação	Implementação
PutBucketCors	Define a configuração do CORS para um bucket de modo que o bucket possa atender às solicitações de origem cruzada. O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos da Web do cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado `images` para armazenar gráficos. Ao definir a configuração CORS para o `images` intervalo, pode permitir que as imagens nesse intervalo sejam apresentadas no website `http://www.example.com`.
PutBucketEncryption	Define o estado de encriptação predefinido de um intervalo existente. Quando a criptografia no nível do bucket está ativada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID suporta criptografia no lado do servidor com chaves gerenciadas pelo StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o `SSEAlgorithm` parâmetro como `AES256`, e não use o `KMSMasterKeyID` parâmetro. A configuração de criptografia padrão do bucket é ignorada se a solicitação de upload de objeto já especificar criptografia (ou seja, se a solicitação incluir o `x-amz-server-side-encryption-*` cabeçalho da solicitação).
PutBucketLifecycleConfiguration (Anteriormente chamado PUT Bucket Lifecycle)	Cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID dá suporte a até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML: • Expiração (dias, Data, ExpiredObjectDeleteMarker) • Não-currentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtro (prefixo, Tag) • Estado • ID O StorageGRID não oferece suporte a essas ações: • AbortIncompleteMultipartUpload • Transição "Crie a configuração do ciclo de vida do S3"Consulte . Para entender como a ação de expiração em um ciclo de vida do bucket interage com as instruções de colocação do ILM, "Como o ILM opera ao longo da vida de um objeto"consulte . **Nota**: A configuração do ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis com o legado.

Operação	Implementação

PutBucketNotificationConfiguration
 	
(Anteriormente chamada DE NOTIFICAÇÃO PUT Bucket)
	Configura notificações para o bucket usando o XML de configuração de notificação incluído no corpo da solicitação. Você deve estar ciente dos seguintes detalhes de implementação:
	
	• O StorageGRID oferece suporte a tópicos do Amazon Simple Notification Service (Amazon SNS) ou Kafka como destinos. Os endpoints do Simple Queue Service (SQS) ou do Amazon Lambda não são suportados.
	• O destino das notificações deve ser especificado como a URNA de um endpoint do StorageGRID. Os endpoints podem ser criados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário.
	
	O endpoint deve existir para que a configuração de notificação seja bem-sucedida. Se o endpoint não existir, um `400 Bad Request` erro é retornado com o código `InvalidArgument`.
	
	• Não é possível configurar uma notificação para os seguintes tipos de eventos. Esses tipos de eventos são **não** suportados.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, exceto que elas não incluem algumas chaves e usam valores específicos para outras, como mostrado na lista a seguir:
	◦ **EventSource**
	
	`sgws:s3`
	
	◦ **AwsRegion**
	
	não incluído
	
	◦ **x-amz-id-2**
	
	não incluído
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

Política de PutBucketPolicy	Define a política anexada ao bucket. "Use políticas de acesso de grupo e bucket"Consulte .

Operação	Implementação
PutBucketReplication	Configura "Replicação do StorageGRID CloudMirror" para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para a replicação do CloudMirror, você deve estar ciente dos seguintes detalhes de implementação: • O StorageGRID suporta apenas V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue convenções V1 para exclusão de versões de objetos. Para obter detalhes, "Guia do usuário do Amazon Simple Storage Service: Configuração de replicação" consulte . • A replicação do bucket pode ser configurada em buckets versionados ou não versionados. • Você pode especificar um intervalo de destino diferente em cada regra do XML de configuração de replicação. Um bucket de origem pode ser replicado para mais de um bucket de destino. • Os buckets de destino devem ser especificados como a URN dos endpoints do StorageGRID, conforme especificado no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. "Configurar a replicação do CloudMirror"Consulte . O endpoint deve existir para que a configuração de replicação seja bem-sucedida. Se o endpoint não existir, a solicitação falhará como um `400 Bad Request`. a mensagem de erro indica: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Não é necessário especificar um `Role` no XML de configuração. Este valor não é usado pelo StorageGRID e será ignorado se enviado. • Se você omitir a classe de armazenamento do XML de configuração, o StorageGRID usará a `STANDARD` classe de armazenamento por padrão. • Se você excluir um objeto do bucket de origem ou excluir o bucket de origem, o comportamento de replicação entre regiões é o seguinte: ◦ Se você excluir o objeto ou o bucket antes que ele tenha sido replicado, o objeto/bucket não será replicado e você não será notificado. ◦ Se você excluir o objeto ou o bucket depois que ele foi replicado, o StorageGRID segue o comportamento padrão de exclusão do Amazon S3 para V1 TB de replicação entre regiões.

Operação	Implementação
PutBucketTagging	Usa o `tagging` subrecurso para adicionar ou atualizar um conjunto de tags para um bucket. Ao adicionar etiquetas de bucket, esteja ciente das seguintes limitações: • O StorageGRID e o Amazon S3 suportam até 50 tags para cada bucket. • As tags associadas a um bucket devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 carateres Unicode de comprimento. • Os valores de tag podem ter até 256 carateres Unicode de comprimento. • Chave e valores são sensíveis a maiúsculas e minúsculas. **Atenção**: Se uma tag de política ILM não padrão for definida para esse intervalo, haverá uma `NTAP-SG-ILM-BUCKET-TAG` tag de intervalo com um valor atribuído a ele. Certifique-se de que a `NTAP-SG-ILM-BUCKET-TAG` tag bucket está incluída com o valor atribuído em todas as solicitações PutBucketTagging. Não modifique nem remova esta etiqueta. **Nota**: Esta operação irá substituir quaisquer tags atuais que o bucket já tenha. Se quaisquer tags existentes forem omitidas do conjunto, essas tags serão removidas para o intervalo.
PutBucketControle de versão	Usa o `versioning` subrecurso para definir o estado de controle de versão de um bucket existente. Você pode definir o estado de controle de versão com um dos seguintes valores: • Habilitado: Permite o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. • Suspenso: Desativa o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão `null` .
PutObjectLockConfiguration	Configura ou remove o modo de retenção padrão do bucket e o período de retenção padrão. Se o período de retenção padrão for modificado, a data de retenção até as versões de objetos existentes permanecerá a mesma e não será recalculada usando o novo período de retenção padrão. "Use a API REST do S3 para configurar o bloqueio de objetos do S3"Consulte para obter informações detalhadas.

Operações em objetos

Operações em objetos

Esta seção descreve como o sistema StorageGRID implementa S3 operações de API REST para objetos.

As seguintes condições se aplicam a todas as operações de objetos:

- Os StorageGRID "valores de consistência"são suportados por todas as operações em objetos, com exceção dos seguintes:
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHod
  - Retenção PutObjectRetention
  - Selecione ObjectContent
- As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.
- Todos os objetos em um bucket do StorageGRID são de propriedade do proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.
- Os objetos de dados ingeridos para o sistema StorageGRID através do Swift não podem ser acedidos através do S3.

A tabela a seguir descreve como o StorageGRID implementa operações de objetos API REST do S3.

Operação	Implementação
DeleteObject	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Ao processar uma solicitação de DeleteObject, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se for bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas dentro de 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID coloca as cópias em fila para remoção e, em seguida, indica sucesso para o cliente. **Controle de versão** Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o `versionId` subrecurso. O uso deste subrecurso exclui permanentemente a versão. Se o `versionId` corresponder a um marcador de exclusão, o cabeçalho de resposta `x-amz-delete-marker` será retornado como `true`. • Se um objeto for excluído sem o `versionId` subrecurso em um bucket com o controle de versão ativado, isso resultará na geração de um marcador de exclusão. O `versionId` para o marcador de exclusão é retornado usando o `x-amz-version-id` cabeçalho de resposta e o `x-amz-delete-marker` cabeçalho de resposta é retornado como `true`. • Se um objeto for excluído sem o `versionId` sub-recurso em um bucket com controle de versão suspenso, ele resultará em uma exclusão permanente de uma versão 'null' já existente ou um marcador 'null' delete, e a geração de um novo marcador 'null' delete. O `x-amz-delete-marker` cabeçalho de resposta é retornado definido como `true`. **Nota**: Em certos casos, vários marcadores de exclusão podem existir para um objeto. "Use a API REST do S3 para configurar o bloqueio de objetos do S3"Consulte para saber como excluir versões de objetos no MODO DE GOVERNANÇA.
DeleteObjects (Anteriormente CHAMADO EXCLUIR vários objetos)	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Vários objetos podem ser excluídos na mesma mensagem de solicitação. "Use a API REST do S3 para configurar o bloqueio de objetos do S3"Consulte para saber como excluir versões de objetos no MODO DE GOVERNANÇA.

Operação	Implementação
DeleteObjectTagging	Usa o `tagging` subrecurso para remover todas as tags de um objeto. **Controle de versão** Se o `versionId` parâmetro de consulta não for especificado na solicitação, a operação excluirá todas as tags da versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" é retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.
GetObject	"GetObject"
GetObjectAcl	Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retornará uma resposta positiva e a ID, DisplayName e permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto.
GetObjectLegalHod	"Use a API REST do S3 para configurar o bloqueio de objetos do S3"
GetObjectRetention	"Use a API REST do S3 para configurar o bloqueio de objetos do S3"
GetObjectTagging	Usa o `tagging` subrecurso para retornar todas as tags para um objeto. **Controle de versão** Se o `versionId` parâmetro de consulta não for especificado na solicitação, a operação retornará todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" é retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.
HeadObject	"HeadObject"
RestoreObject	"RestoreObject"
PutObject	"PutObject"
CopyObject (Anteriormente chamado PUT Object - Copy)	"CopyObject"
PutObjectLegalHod	"Use a API REST do S3 para configurar o bloqueio de objetos do S3"
Retenção PutObjectRetention	"Use a API REST do S3 para configurar o bloqueio de objetos do S3"

Operação	Implementação
Marcação de objetos	Usa o `tagging` subrecurso para adicionar um conjunto de tags a um objeto existente. **Limites da etiqueta do objeto** Você pode adicionar tags a novos objetos ao enviá-los ou adicioná-los a objetos existentes. O StorageGRID e o Amazon S3 suportam até 10 tags para cada objeto. Tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 carateres Unicode de comprimento e os valores de tag podem ter até 256 carateres Unicode de comprimento. Chave e valores são sensíveis a maiúsculas e minúsculas. **Tag atualizações e comportamento de ingestão** Quando você usa PutObjectTagging para atualizar as tags de um objeto, o StorageGRID não reingere o objeto. Isso significa que a opção de comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento de objetos que são acionadas pela atualização são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano. Isso significa que se a regra ILM usar a opção estrita para o comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objeto necessários não puderem ser feitos (por exemplo, porque um local recém-exigido não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível. **Resolução de conflitos** As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação. **Controle de versão** Se o `versionId` parâmetro de consulta não for especificado na solicitação, a operação adicionará tags à versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" é retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.
Selecione ObjectContent	"Selecione ObjectContent"

Utilize S3 Select (Selecionar)

O StorageGRID oferece suporte às seguintes cláusulas, tipos de dados e operadores do Amazon S3 Select para o "SelectObjectContent - comando".

Nenhum item não listado não é suportado.

Para obter a sintaxe, "Selecione ObjectContent"consulte . Para obter mais informações sobre S3 Select, consulte "Documentação da AWS para o S3 Select".

Apenas as contas de inquilino que tenham S3 Select ativado podem emitir consultas SelectObjectContent. Consulte "Considerações e requisitos para usar o S3 Select".

Cláusulas

- Selecione a lista
- Da cláusula
- Cláusula where
- CLÁUSULA LIMIT (LIMITE)

Tipos de dados

- bool
- número inteiro
- cadeia de carateres
- flutuação
- decimal, numérico
- timestamp

Operadores

Operadores lógicos

- E
- NÃO
- OU

Operadores de comparação

- *
- >
- &lt
- &gt
- .
- .
- >
- !
- ENTRE
- EM

Operadores de correspondência de padrões

- GOSTO
- _
- %

Operadores unitários

- É NULO
- NÃO É NULL

Operadores de matemática

- E
- -
- *
- /
- %

O StorageGRID segue a precedência do operador Amazon S3 Select.

Agregar funções

- MÉDIA ()
- CONTAGEM (*)
- MÁX. ()
- MIN. ()
- SOMA()

Funções condicionais

- CASO
- COALESCE
- NULLIF

Funções de conversão

- CAST (para tipos de dados suportados)

Funções de data

- DATE_ADD
- DATE_DIFF
- EXTRAIR
- TO_STRING
- TO_TIMESTAMP

- UTCNOW

Funções de cadeia de carateres

- CHAR_LENGTH, CHARACTER_LENGTH
- BAIXAR
- SUBSTRING
- APARAR
- SUPERIOR

Use a criptografia do lado do servidor

A criptografia do lado do servidor permite proteger os dados do objeto em repouso. O StorageGRID criptografa os dados enquanto grava o objeto e descriptografa os dados quando você acessa o objeto.

Se você quiser usar a criptografia do lado do servidor, você pode escolher uma das duas opções mutuamente exclusivas, com base em como as chaves de criptografia são gerenciadas:

- **SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID)**: Quando você emite uma solicitação S3 para armazenar um objeto, o StorageGRID criptografa o objeto com uma chave exclusiva. Quando você emite uma solicitação S3 para recuperar o objeto, o StorageGRID usa a chave armazenada para descriptografar o objeto.
- **SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente)**: Quando você emite uma solicitação S3 para armazenar um objeto, você fornece sua própria chave de criptografia. Quando você recupera um objeto, você fornece a mesma chave de criptografia como parte de sua solicitação. Se as duas chaves de criptografia corresponderem, o objeto será descriptografado e seus dados de objeto serão retornados.

  Enquanto o StorageGRID gerencia todas as operações de criptografia e descriptografia de objetos, você deve gerenciar as chaves de criptografia fornecidas.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.

> Se um objeto for criptografado com SSE ou SSE-C, quaisquer configurações de criptografia no nível de bucket ou no nível de grade serão ignoradas.

Use SSE

Para criptografar um objeto com uma chave exclusiva gerenciada pelo StorageGRID, use o seguinte cabeçalho de solicitação:

```
x-amz-server-side-encryption
```

O cabeçalho de solicitação SSE é suportado pelas seguintes operações de objeto:

- "PutObject"
- "CopyObject"

- "CreateMultipartUpload"

Use SSE-C

Para criptografar um objeto com uma chave exclusiva que você gerencia, use três cabeçalhos de solicitação:

Cabeçalho da solicitação	Descrição
`x-amz-server-side-encryption-customer-algorithm`	Especifique o algoritmo de criptografia. O valor da plataforma deve ser `AES256`.
`x-amz-server-side-encryption-customer-key`	Especifique a chave de criptografia que será usada para criptografar ou descriptografar o objeto. O valor da chave deve ser 256 bits, codificado em base64.
`x-amz-server-side-encryption-customer-key-MD5`	Especifique o resumo MD5 da chave de criptografia de acordo com a RFC 1321, que é usada para garantir que a chave de criptografia foi transmitida sem erros. O valor para o resumo MD5 deve ser base64-codificado 128-bit.

Os cabeçalhos de solicitação SSE-C são suportados pelas seguintes operações de objeto:

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Considerações sobre o uso de criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Antes de usar SSE-C, esteja ciente das seguintes considerações:

- Você deve usar https.

> O StorageGRID rejeita quaisquer solicitações feitas por http ao usar SSE-C. para considerações de segurança, você deve considerar qualquer chave que você enviar acidentalmente usando http para ser comprometida. Elimine a chave e rode-a conforme adequado.

- O ETag na resposta não é o MD5 dos dados do objeto.
- É necessário gerenciar o mapeamento de chaves de criptografia para objetos. O StorageGRID não armazena chaves de criptografia. Você é responsável por rastrear a chave de criptografia fornecida para cada objeto.
- Se seu bucket estiver habilitado para versionamento, cada versão do objeto deve ter sua própria chave de criptografia. Você é responsável por rastrear a chave de criptografia usada para cada versão do objeto.

- Como você gerencia chaves de criptografia no lado do cliente, você também deve gerenciar quaisquer proteções adicionais, como rotação de chaves, no lado do cliente.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.

- Se a replicação entre grade ou a replicação do CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

Informações relacionadas

"Guia do usuário do Amazon S3: Usando criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)"

CopyObject

Você pode usar a solicitação S3 CopyObject para criar uma cópia de um objeto que já está armazenado no S3. Uma operação CopyObject é a mesma que executar GetObject seguido por PutObject.

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use "carregamento multipart" em vez disso.

O tamanho máximo *suportado* para uma única operação PutObject é de 5 TIB (5.497.558.138.880 bytes).

> Se você atualizou do StorageGRID 11,6 ou anterior, o alerta COLOCAR tamanho do objeto muito grande S3 será acionado se você tentar carregar um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11,7 ou 11,8, o alerta não será acionado neste caso. No entanto, para se alinhar com o padrão AWS S3, futuras versões do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

UTF-8 carateres em metadados do usuário

Se uma solicitação incluir valores UTF-8 (não escapados) no nome da chave ou valor dos metadados definidos pelo usuário, o comportamento do StorageGRID é indefinido.

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Os carateres UTF-8 escapados são tratados como carateres ASCII:

- As solicitações são bem-sucedidas se os metadados definidos pelo usuário incluírem carateres UTF-8 escapados.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave incluir carateres não imprimíveis.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguido por um par de nome-valor contendo metadados definidos pelo usuário
- `x-amz-metadata-directive`: O valor padrão é `COPY`, que permite copiar o objeto e os metadados associados.

  Você pode especificar `REPLACE` para substituir os metadados existentes ao copiar o objeto ou para atualizar os metadados do objeto.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: O valor padrão é `COPY`, que permite copiar o objeto e todas as tags.

  Você pode especificar `REPLACE` para substituir as tags existentes ao copiar o objeto ou para atualizar as tags.

- S3 cabeçalhos de solicitação de bloqueio de objetos:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do intervalo serão usadas para calcular o modo de versão do objeto e manter até a data. "Use a API REST do S3 para configurar o bloqueio de objetos do S3"Consulte .

- Cabeçalhos de pedido SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Consulte Cabeçalhos de solicitação para criptografia do lado do servidor

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Quando você copia um objeto, se o objeto de origem tiver um checksum, o StorageGRID não copia esse valor de checksum para o novo objeto. Esse comportamento se aplica se você tentar ou não `x-amz-checksum-algorithm` usar na solicitação de objeto.

- `x-amz-website-redirect-location`

Opções de classe de armazenamento

O `x-amz-storage-class` cabeçalho de solicitação é suportado e afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM correspondente usar o compromisso duplo ou equilibrado "opção de ingestão".

- `STANDARD`

  (Padrão) especifica uma operação de ingestão de commit duplo quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de commit único quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

  > Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Usando x-amz-copy-source em CopyObject

Se o intervalo de origem e a chave, especificados no `x-amz-copy-source` cabeçalho, forem diferentes do intervalo de destino e da chave, uma cópia dos dados do objeto de origem será gravada no destino.

Se a origem e o destino corresponderem e o `x-amz-metadata-directive` cabeçalho for especificado como `REPLACE`, os metadados do objeto serão atualizados com os valores de metadados fornecidos na solicitação. Nesse caso, o StorageGRID não reingere o objeto. Isto tem duas consequências importantes:

- Não é possível usar CopyObject para criptografar um objeto existente no local ou para alterar a criptografia de um objeto existente no local. Se você fornecer o `x-amz-server-side-encryption`

cabeçalho ou o `x-amz-server-side-encryption-customer-algorithm` cabeçalho, o StorageGRID rejeita a solicitação e retorna `XNotImplemented`.

- A opção de comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento de objetos que são acionadas pela atualização são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano.

  Isso significa que se a regra ILM usar a opção estrita para o comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objeto necessários não puderem ser feitos (por exemplo, porque um local recém-exigido não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível.

Cabeçalhos de solicitação para criptografia do lado do servidor

Se "use a criptografia do lado do servidor"você , os cabeçalhos de solicitação fornecidos dependem se o objeto de origem está criptografado e se você planeja criptografar o objeto de destino.

- Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deve incluir os três cabeçalhos a seguir na solicitação CopyObject, para que o objeto possa ser descriptografado e copiado:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia fornecida quando você criou o objeto de origem.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.
- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva que você fornece e gerencia, inclua os três cabeçalhos a seguir:
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique uma nova chave de criptografia para o objeto de destino.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da nova chave de criptografia.

  > As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações para "usando criptografia do lado do servidor".

- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo StorageGRID (SSE), inclua esse cabeçalho na solicitação de CopyObject:
  - `x-amz-server-side-encryption`

  > O `server-side-encryption` valor do objeto não pode ser atualizado. Em vez disso, faça uma cópia com um novo `server-side-encryption` valor usando `x-amz-metadata-directive`: `REPLACE`.

Controle de versão

Se o bucket de origem for versionado, você pode usar o `x-amz-copy-source` cabeçalho para copiar a versão mais recente de um objeto. Para copiar uma versão específica de um objeto, você deve especificar explicitamente a versão a ser copiada usando o `versionId` subrecurso. Se o intervalo de destino for versionado, a versão gerada será retornada `x-amz-version-id` no cabeçalho de resposta. Se o controle de versão estiver suspenso para o bucket de destino, `x-amz-version-id` retorna um valor "nulo".

GetObject

Você pode usar a solicitação GetObject S3 para recuperar um objeto de um bucket do S3.

Objetos GetObject e multipart

Você pode usar o `partNumber` parâmetro Request para recuperar uma parte específica de um objeto multipart ou segmentado. O `x-amz-mp-parts-count` elemento de resposta indica quantas partes o objeto tem.

Você pode definir `partNumber` como 1 para objetos segmentados/multipartes e objetos não segmentados/não multipartes; no entanto, o `x-amz-mp-parts-count` elemento de resposta é retornado apenas para objetos segmentados ou multipartes.

UTF-8 carateres em metadados do usuário

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados em metadados definidos pelo usuário. Obter solicitações para um objeto com carateres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome ou valor da chave incluir carateres não imprimíveis.

Cabeçalho de solicitação suportado

O seguinte cabeçalho de solicitação é suportado:

- `x-amz-checksum-mode`: Especificar `ENABLED`

  O `Range` cabeçalho não é suportado com `x-amz-checksum-mode` para GetObject. Quando você inclui `Range` na solicitação com `x-amz-checksum-mode` habilitado, o StorageGRID não retorna um valor de checksum na resposta.

Cabeçalho de pedido não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented`:

- `x-amz-website-redirect-location`

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação busca a versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status "não encontrado" é retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use todos os três cabeçalhos se o objeto for criptografado com uma chave exclusiva que você forneceu.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações no "Use a criptografia do lado do servidor".

Comportamento do GetObject para objetos de pool de storage de nuvem

Se um objeto tiver sido armazenado em um "Cloud Storage Pool", o comportamento de uma solicitação GetObject depende do estado do objeto. "HeadObject"Consulte para obter mais detalhes.

> Se um objeto for armazenado em um pool de armazenamento em nuvem e uma ou mais cópias do objeto também existirem na grade, as solicitações GetObject tentarão recuperar dados da grade, antes de recuperá-los do pool de armazenamento em nuvem.

Estado do objeto	Comportamento de GetObject
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento	`200 OK` Uma cópia do objeto é recuperada.
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	`200 OK` Uma cópia do objeto é recuperada.
Objeto transicionado para um estado não recuperável	`403 Forbidden, InvalidObjectState` Use uma "RestoreObject" solicitação para restaurar o objeto para um estado recuperável.
Objeto em processo de restauração a partir de um estado não recuperável	`403 Forbidden, InvalidObjectState` Aguarde até que a solicitação de RestoreObject seja concluída.
Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK` Uma cópia do objeto é recuperada.

Objetos segmentados ou multiparte em um pool de armazenamento em nuvem

Se você carregou um objeto multipart ou se o StorageGRID dividir um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no pool de armazenamento em nuvem amostrando um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação GetObject pode retornar incorretamente `200 OK` quando algumas partes do objeto já tiverem sido transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não tiverem sido restauradas.

Nestes casos:

- A solicitação GetObject pode retornar alguns dados, mas parar no meio da transferência.
- Uma solicitação GetObject subsequente pode retornar `403 Forbidden`.

Replicação GetObject e cross-grid

Se você estiver usando "federação de grade" e "replicação entre grade" estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação GetObject. A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grelha	Estado da replicação
Fonte	• **COMPLETED**: A replicação foi bem-sucedida. • **PENDENTE**: O objeto ainda não foi replicado. • **FAILURE**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	• RÉPLICA*: O objeto foi replicado a partir da grade de origem.

> ⓘ O StorageGRID não suporta o `x-amz-replication-status` colhedor.

HeadObject

Você pode usar a solicitação S3 HeadObject para recuperar metadados de um objeto sem retornar o próprio objeto. Se o objeto for armazenado em um pool de armazenamento em nuvem, você poderá usar o HeadObject para determinar o estado de transição do objeto.

Objetos HeadObject e multipart

Você pode usar o `partNumber` parâmetro Request para recuperar metadados de uma parte específica de um objeto multipart ou segmentado. O `x-amz-mp-parts-count` elemento de resposta indica quantas partes o objeto tem.

Você pode definir `partNumber` como 1 para objetos segmentados/multipartes e objetos não segmentados/não multipartes; no entanto, o `x-amz-mp-parts-count` elemento de resposta é retornado apenas para objetos segmentados ou multipartes.

UTF-8 carateres em metadados do usuário

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados em metadados definidos pelo usuário. As solicitações HEAD para um objeto com carateres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome ou valor da chave incluir carateres não imprimíveis.

Cabeçalho de solicitação suportado

O seguinte cabeçalho de solicitação é suportado:

- `x-amz-checksum-mode`

  O `partNumber` parâmetro e `Range` o cabeçalho não são suportados com `x-amz-checksum-mode` o HeadObject. Quando você os inclui na solicitação com `x-amz-checksum-mode` habilitado, o StorageGRID não retorna um valor de checksum na resposta.

Cabeçalho de pedido não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented`:

- `x-amz-website-redirect-location`

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação busca a versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status "não encontrado" é retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use os três cabeçalhos se o objeto for criptografado com uma chave exclusiva que você forneceu.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações no "Use a criptografia do lado do servidor".

Respostas do HeadObject para objetos Pool de storage de nuvem

Se o objeto for armazenado em a "Cloud Storage Pool", os seguintes cabeçalhos de resposta serão retornados:

- `x-amz-storage-class: GLACIER`

- `x-amz-restore`

Os cabeçalhos de resposta fornecem informações sobre o estado de um objeto à medida que ele é movido para um pool de armazenamento em nuvem, opcionalmente transferido para um estado não recuperável e restaurado.

Estado do objeto	Resposta ao HeadObject
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento	`200 OK` (Nenhum cabeçalho de resposta especial é retornado.)

Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Até que o objeto seja transferido para um estado não recuperável, o valor para `expiry-date` é definido para algum tempo distante no futuro. A hora exata da transição não é controlada pelo sistema StorageGRID.

O objeto fez a transição para o estado não recuperável, mas pelo menos uma cópia também existe na grade	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	O valor para `expiry-date` é definido para algum tempo distante no futuro.
	
	Nota: Se a cópia na grade não estiver disponível (por exemplo, um nó de armazenamento está inativo), você deve emitir uma "RestoreObject" solicitação para restaurar a cópia do pool de armazenamento em nuvem antes de recuperar o objeto com êxito.

Objeto transicionado para um estado não recuperável e nenhuma cópia existe na grade	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Estado do objeto	Resposta ao HeadObject

Objeto em processo de restauração a partir de um estado não recuperável	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	O `expiry-date` indica quando o objeto no pool de armazenamento em nuvem será retornado a um estado não recuperável.

Objetos segmentados ou multiparte no Cloud Storage Pool

Se você carregou um objeto multipart ou se o StorageGRID dividir um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no pool de armazenamento em nuvem amostrando um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação de HeadObject pode retornar incorretamente `x-amz-restore: ongoing-request="false"` quando algumas partes do objeto já tiverem sido transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não tiverem sido restauradas.

Replicação de HeadObject e cross-grid

Se você estiver usando "federação de grade" e "replicação entre grade" estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação de HeadObject. A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grelha	Estado da replicação
Fonte	• **COMPLETED**: A replicação foi bem-sucedida. • **PENDENTE**: O objeto ainda não foi replicado. • **FAILURE**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	• RÉPLICA*: O objeto foi replicado a partir da grade de origem.

> O StorageGRID não suporta o `x-amz-replication-status` colhedor.

Você pode usar a solicitação S3 PutObject para adicionar um objeto a um bucket.

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use "carregamento multipart" em vez disso.

O tamanho máximo *suportado* para uma única operação PutObject é de 5 TIB (5.497.558.138.880 bytes).

> Se você atualizou do StorageGRID 11,6 ou anterior, o alerta COLOCAR tamanho do objeto muito grande S3 será acionado se você tentar carregar um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11,7 ou 11,8, o alerta não será acionado neste caso. No entanto, para se alinhar com o padrão AWS S3, futuras versões do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Tamanho dos metadados do usuário

O Amazon S3 limita o tamanho dos metadados definidos pelo usuário dentro de cada cabeçalho de SOLICITAÇÃO PUT para 2 KB. O StorageGRID limita os metadados do usuário a 24 KiB. O tamanho dos metadados definidos pelo usuário é medido tomando a soma do número de bytes na codificação UTF-8 de cada chave e valor.

UTF-8 carateres em metadados do usuário

Se uma solicitação incluir valores UTF-8 (não escapados) no nome da chave ou valor dos metadados definidos pelo usuário, o comportamento do StorageGRID é indefinido.

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Os carateres UTF-8 escapados são tratados como carateres ASCII:

- As solicitações PutObject, CopyObject, GetObject e HeadObject são bem-sucedidas se os metadados definidos pelo usuário incluírem carateres UTF-8 escapados.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave incluir carateres não imprimíveis.

Limites da etiqueta do objeto

Você pode adicionar tags a novos objetos ao enviá-los ou adicioná-los a objetos existentes. O StorageGRID e o Amazon S3 suportam até 10 tags para cada objeto. Tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 carateres Unicode de comprimento e os valores de tag podem ter até 256 carateres Unicode de comprimento. Chave e valores são sensíveis a maiúsculas e minúsculas.

Propriedade do objeto

No StorageGRID, todos os objetos são de propriedade da conta de proprietário do bucket, incluindo objetos criados por uma conta não proprietária ou um usuário anônimo.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  Quando você especifica `aws-chunked` para `Content-Encoding`o StorageGRID não verifica os seguintes itens:

  - O StorageGRID não verifica o `chunk-signature` contra os dados de bloco.
  - O StorageGRID não verifica o valor que você fornece `x-amz-decoded-content-length` em relação ao objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  A codificação de transferência Chunked é suportada se `aws-chunked` a assinatura de payload também for usada.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguido por um par de nome-valor contendo metadados definidos pelo usuário.

  Ao especificar o par nome-valor para metadados definidos pelo usuário, use este formato geral:

  ```
  x-amz-meta-name: value
  ```

  Se você quiser usar a opção **tempo de criação definido pelo usuário** como tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que Registram quando o objeto foi criado. Por exemplo:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  O valor para `creation-time` é avaliado em segundos desde 1 de janeiro de 1970.

Uma regra ILM não pode usar um **tempo de criação definido pelo usuário** para o tempo de referência e a opção de ingestão equilibrada ou rigorosa. Um erro é retornado quando a regra ILM é criada.

- `x-amz-tagging`
- S3 cabeçalhos de solicitação de bloqueio de objetos
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do intervalo serão usadas para calcular o modo de versão do objeto e manter até a data. "Use a API REST do S3 para configurar o bloqueio de objetos do S3"Consulte .
- Cabeçalhos de pedido SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Consulte Cabeçalhos de solicitação para criptografia do lado do servidor

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  O `x-amz-website-redirect-location` cabeçalho retorna `XNotImplemented`.

Opções de classe de armazenamento

O `x-amz-storage-class` cabeçalho da solicitação é suportado. O valor enviado para `x-amz-storage-class` afeta a forma como o StorageGRID protege os dados de objetos durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (que é determinado pelo ILM).

Se a regra ILM correspondente a um objeto ingerido usar a opção ingestão restrita, o `x-amz-storage-class` cabeçalho não terá efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class`:

- `STANDARD` (Predefinição)

- * Commit duplo*: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, assim que um objeto é ingerido, uma segunda cópia desse objeto é criada e distribuída para um nó de armazenamento diferente (commit duplo). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais satisfazem as instruções de colocação na regra. Caso contrário, novas cópias de objetos podem precisar ser feitas em locais diferentes e as cópias provisórias iniciais podem precisar ser excluídas.
- **Balanced**: Se a regra ILM especificar a opção Balanced e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes nós de storage.

  Se o StorageGRID puder criar imediatamente todas as cópias de objeto especificadas na regra ILM (colocação síncrona), `x-amz-storage-class` o cabeçalho não terá efeito.

- `REDUCED_REDUNDANCY`
  - **Commit duplo**: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
  - **Balanced**: Se a regra ILM especificar a opção Balanced, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. A `REDUCED_REDUNDANCY` opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

  A utilização da `REDUCED_REDUNDANCY` opção não é recomendada noutras circunstâncias. `REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a única cópia for inicialmente armazenada em um nó de armazenamento que falha antes que a avaliação ILM possa ocorrer.

> Ter 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.

Especificar `REDUCED_REDUNDANCY` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas ativas de ILM e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

> Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os cabeçalhos de solicitação a seguir para criptografar um objeto com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE**: Use o seguinte cabeçalho se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.
  - `x-amz-server-side-encryption`

    Quando o `x-amz-server-side-encryption` cabeçalho não é incluído na solicitação PutObject, a grade inteira "configuração de criptografia de objeto armazenado" é omitida da resposta PutObject.
- **SSE-C**: Use todos os três cabeçalhos se você quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações para "usando criptografia do lado do servidor".

> Se um objeto for criptografado com SSE ou SSE-C, quaisquer configurações de criptografia no nível de bucket ou no nível de grade serão ignoradas.

Controle de versão

Se o controle de versão estiver habilitado para um bucket, um exclusivo `versionId` será gerado automaticamente para a versão do objeto que está sendo armazenado. Isso `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão estiver suspenso, a versão do objeto será armazenada com um nulo `versionId` e se já existir uma versão nula, ela será substituída.

Cálculos de assinatura para o cabeçalho de autorização

Ao usar o `Authorization` cabeçalho para autenticar solicitações, o StorageGRID difere da AWS das seguintes maneiras:

- O StorageGRID não requer `host` que os cabeçalhos sejam incluídos no `CanonicalHeaders`.
- O StorageGRID não precisa `Content-Type` ser incluído no `CanonicalHeaders`.
- O StorageGRID não requer `x-amz-*` que os cabeçalhos sejam incluídos no `CanonicalHeaders`.

> Como uma prática recomendada geral, inclua sempre esses cabeçalhos `CanonicalHeaders` para garantir que eles sejam verificados; no entanto, se você excluir esses cabeçalhos, o StorageGRID não retornará um erro.

Para obter detalhes, "Cálculos de assinatura para o cabeçalho de autorização: Transferência de carga útil em uma única bloco (assinatura AWS versão 4)" consulte .

Informações relacionadas

- "Gerenciar objetos com ILM"
- "Referência de API do Amazon Simple Storage Service: PutObject"

RestoreObject

Você pode usar a solicitação S3 RestoreObject para restaurar um objeto armazenado em um pool de armazenamento em nuvem.

Tipo de solicitação suportada

O StorageGRID suporta apenas solicitações de RestoreObject para restaurar um objeto. Não suporta o `SELECT` tipo de restauração. Selecione Requests Return (retornar solicitações `XNotImplemented`).

Controle de versão

Opcionalmente, especifique `versionId` para restaurar uma versão específica de um objeto em um bucket com versão. Se você não especificar `versionId`, a versão mais recente do objeto será restaurada

Comportamento do RestoreObject em objetos de pool de storage de nuvem

Se um objeto tiver sido armazenado em um "Cloud Storage Pool", uma solicitação de RestoreObject tem o seguinte comportamento, com base no estado do objeto. "HeadObject"Consulte para obter mais detalhes.

> Se um objeto for armazenado em um pool de armazenamento em nuvem e uma ou mais cópias do objeto também existirem na grade, não haverá necessidade de restaurar o objeto emitindo uma solicitação de RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

Estado do objeto	Comportamento do RestoreObject
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto não está em um pool de storage de nuvem	`403 Forbidden`, `InvalidObjectState`
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	`200 OK` Nenhuma alteração é feita. **Nota**: Antes de um objeto ser transferido para um estado não recuperável, não é possível alterar o seu `expiry-date`.

Estado do objeto	Comportamento do RestoreObject
Objeto transicionado para um estado não recuperável	`202 Accepted` Restaura uma cópia recuperável do objeto para o pool de armazenamento em nuvem pelo número de dias especificado no corpo da solicitação. No final desse período, o objeto é retornado a um estado não recuperável. Opcionalmente, use o `Tier` elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para concluir (`Expedited`, `Standard` ou `Bulk`). Se você não especificar `Tier`, o `Standard` nível será usado. **Importante**: Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou se o Cloud Storage Pool usar o armazenamento Azure Blob, não será possível restaurá-lo usando o `Expedited` nível. O seguinte erro é retornado `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class.`
Objeto em processo de restauração a partir de um estado não recuperável	`409 Conflict`, `RestoreAlreadyInProgress`
Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK` **Nota:** se um objeto foi restaurado para um estado recuperável, você pode alterar o mesmo `expiry-date` reemitindo a solicitação de RestoreObject com um novo valor para `Days`. A data de restauração é atualizada em relação à hora da solicitação.

Selecione ObjectContent

Você pode usar a solicitação SelectObjectContent S3 para filtrar o conteúdo de um objeto S3 com base em uma instrução SQL simples.

Para obter mais informações, "Referência da API do Amazon Simple Storage Service: SelectObjectContent"consulte .

Antes de começar

- A conta de locatário tem a permissão S3 Select (Selecionar).
- Você tem `s3:GetObject` permissão para o objeto que deseja consultar.
- O objeto que você deseja consultar deve estar em um dos seguintes formatos:
  - **CSV**. Pode ser usado como está ou comprimido em arquivos GZIP ou bzip2.
  - **Parquet**. Requisitos adicionais para objetos em Parquet:
    - S3 Select suporta apenas compactação colunar usando GZIP ou Snappy. S3 Select não suporta compactação de objetos inteiros para objetos Parquet.
    - S3 a seleção não suporta saída em Parquet. Você deve especificar o formato de saída como CSV ou JSON.
    - O tamanho máximo do grupo de linhas não comprimidas é de 512 MB.

        - Você deve usar os tipos de dados especificados no esquema do objeto.
        - Você não pode usar os tipos lógicos INTERVALO, JSON, LISTA, HORA ou UUID.
- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer Registro na entrada ou resultados tem um comprimento máximo de 1 MIB.

Exemplo de sintaxe de solicitação CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemplo de sintaxe de solicitação de Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemplo de consulta SQL

Esta consulta obtém o nome do estado, 2010 populações, 2015 populações estimadas e a porcentagem de mudança dos dados do censo americano. Registros no arquivo que não são estados são ignorados.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

As primeiras linhas do arquivo a serem consultadas, `SUB-EST2020_ALL.csv`, são assim:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Exemplo de uso da AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

As primeiras linhas do arquivo de saída, `changes.csv`, são assim:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Exemplo de uso da AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

As primeiras linhas do arquivo de saída, Changes.csv, são assim:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operações para uploads de várias partes

Operações para uploads de várias partes

Esta seção descreve como o StorageGRID suporta operações para uploads de várias partes.

As seguintes condições e notas aplicam-se a todas as operações de carregamento em várias partes:

- Você não deve exceder 1.000 carregamentos simultâneos de várias partes para um único bucket, porque os resultados das consultas ListMultipartUploads para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para peças multipeças. S3 os clientes devem seguir estas diretrizes:
  - Cada parte em um upload de várias partes deve estar entre 5 MIB (5.242.880 bytes) e 5 GiB (5.368.709.120 bytes).
  - A última parte pode ser menor que 5 MIB (5.242.880 bytes).
  - Em geral, os tamanhos das peças devem ser tão grandes quanto possível. Por exemplo, use tamanhos de peças de 5 GiB para um objeto de 100 GiB. Como cada peça é considerada um objeto exclusivo, o uso de tamanhos grandes de peças reduz a sobrecarga de metadados do StorageGRID.
  - Para objetos menores que 5 GiB, considere usar upload não multipart.
- O ILM é avaliado para cada parte de um objeto multipart à medida que é ingerido e para o objeto como um todo quando o upload multipart é concluído, se a regra ILM usa o balanced ou strict ."opção de ingestão" Você deve estar ciente de como isso afeta o posicionamento do objeto e da peça:
  - Se o ILM mudar enquanto um upload multipart S3 estiver em andamento, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multipart for concluído. Qualquer

peça que não seja colocada corretamente está na fila para reavaliação ILM e movida para o local correto mais tarde.

    - Ao avaliar o ILM para uma peça, o StorageGRID filtra o tamanho da peça, não o tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos de ILM para o objeto como um todo. Por exemplo, se uma regra especifica que todos os objetos de 10 GB ou maior são armazenados em DC1 enquanto todos os objetos menores são armazenados em DC2, cada parte de 1 GB de um upload multipart de 10 partes é armazenada em DC2 na ingestão. No entanto, quando ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.

- Todas as operações de upload multipart suportam StorageGRID "valores de consistência".
- Quando um objeto é ingerido utilizando o carregamento em várias partes, o "Limite de segmentação de objetos (1 GiB)"não é aplicado.
- Conforme necessário, você pode usar "criptografia do lado do servidor" com uploads de várias partes. Para usar SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID), você inclui o `x-amz-server-side-encryption` cabeçalho da solicitação somente na solicitação CreateMultipartUpload. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), você especifica os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação CreateMultipartUpload e em cada solicitação de UploadPart subsequente.

Operação	Implementação
AbortMultipartUpload	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.
CompleteMultipartUpload	Consulte "CompleteMultipartUpload"
CreateMultipartUpload (Anteriormente nomeado iniciar carregamento de várias partes)	Consulte "CreateMultipartUpload"
ListMultipartUploads	Consulte "ListMultipartUploads"
ListParts	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.
UploadPart	Consulte "UploadPart"
UploadPartCopy	Consulte "UploadPartCopy"

CompleteMultipartUpload

A operação CompleteMultipartUpload completa um upload em várias partes de um objeto montando as peças carregadas anteriormente.

> O StorageGRID suporta valores não consecutivos em ordem crescente para o `partNumber` parâmetro Request com CompleteMultipartUpload. O parâmetro pode começar com qualquer valor.

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  O `x-amz-storage-class` cabeçalho afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM correspondente especificar o "Opção de confirmação dupla ou ingestão equilibrada".

- `STANDARD`

  (Padrão) especifica uma operação de ingestão de commit duplo quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de commit único quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

  > Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

> Se um upload multipart não for concluído dentro de 15 dias, a operação será marcada como inativa e todos os dados associados serão excluídos do sistema.

> O `ETag` valor retornado não é uma soma MD5 dos dados, mas segue a implementação da API do Amazon S3 do `ETag` valor para objetos multipart.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controle de versão

Esta operação completa um upload de várias partes. Se o controle de versão estiver habilitado para um bucket, a versão do objeto será criada após a conclusão do upload de várias partes.

Se o controle de versão estiver habilitado para um bucket, um exclusivo `versionId` será gerado automaticamente para a versão do objeto que está sendo armazenado. Isso `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão estiver suspenso, a versão do objeto será armazenada com um nulo `versionId` e se já existir uma versão nula, ela será substituída.

> Quando o controle de versão está habilitado para um bucket, concluir um upload multipart sempre cria uma nova versão, mesmo que haja carregamentos simultâneos de várias partes concluídos na mesma chave de objeto. Quando o controle de versão não está habilitado para um bucket, é possível iniciar um upload multipart e, em seguida, ter outro upload multipart iniciado e concluído primeiro na mesma chave de objeto. Em buckets não versionados, o upload multipart que completa o último tem precedência.

Falha na replicação, notificação ou notificação de metadados

Se o intervalo onde ocorre o upload de várias partes estiver configurado para um serviço de plataforma, o upload de várias partes será bem-sucedido mesmo se a ação de replicação ou notificação associada falhar.

Um locatário pode acionar a replicação ou notificação com falha atualizando os metadados ou as tags do objeto. Um locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

"Solucionar problemas de serviços de plataforma"Consulte a .

CreateMultipartUpload

A operação CreateMultipartUpload (anteriormente chamada Iniciar carregamento Multipart) inicia um upload multipart para um objeto e retorna um ID de upload.

O `x-amz-storage-class` cabeçalho da solicitação é suportado. O valor enviado para `x-amz-storage-class` afeta a forma como o StorageGRID protege os dados de objetos durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (que é determinado pelo ILM).

Se a regra ILM que corresponde a um objeto ingerido usar o strict "opção de ingestão", o `x-amz-storage-class` cabeçalho não terá efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class`:

- `STANDARD` (Predefinição)
  - * Commit duplo*: Se a regra ILM especificar a opção ingestão de commit duplo, assim que um objeto é ingerido, uma segunda cópia desse objeto é criada e distribuída para um nó de armazenamento diferente (commit duplo). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais satisfazem as instruções de colocação na regra. Caso contrário, novas cópias de objetos podem precisar ser feitas em locais diferentes e as cópias provisórias iniciais podem precisar ser excluídas.
  - **Balanced**: Se a regra ILM especificar a opção Balanced e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes nós de storage.

    Se o StorageGRID puder criar imediatamente todas as cópias de objeto especificadas na regra ILM (colocação síncrona), `x-amz-storage-class` o cabeçalho não terá efeito.

- `REDUCED_REDUNDANCY`
  - **Commit duplo**: Se a regra ILM especificar a opção Commit duplo, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
  - **Balanced**: Se a regra ILM especificar a opção Balanced, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. A `REDUCED_REDUNDANCY` opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

  A utilização da `REDUCED_REDUNDANCY` opção não é recomendada noutras circunstâncias. `REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a única cópia for inicialmente armazenada em um nó de armazenamento que falha antes que a avaliação ILM possa ocorrer.

> Ter 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.

Especificar `REDUCED_REDUNDANCY` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas ativas de ILM e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

> Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-checksum-algorithm`

  Atualmente, apenas o valor SHA256 para `x-amz-checksum-algorithm` é suportado.

- `x-amz-meta-`, seguido por um par de nome-valor contendo metadados definidos pelo usuário

  Ao especificar o par nome-valor para metadados definidos pelo usuário, use este formato geral:

```
x-amz-meta-_name_: `value`
```

  Se você quiser usar a opção **tempo de criação definido pelo usuário** como tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que Registram quando o

objeto foi criado. Por exemplo:

```
x-amz-meta-creation-time: 1443399726
```

O valor para `creation-time` é avaliado em segundos desde 1 de janeiro de 1970.

> ⓘ A adição `creation-time` de metadados definidos pelo usuário não é permitida se você estiver adicionando um objeto a um bucket que tenha a conformidade legada habilitada. Um erro será retornado.

- S3 cabeçalhos de solicitação de bloqueio de objetos:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do intervalo serão usadas para calcular a versão do objeto retida até a data.

  "Use a API REST do S3 para configurar o bloqueio de objetos do S3"

- Cabeçalhos de pedido SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Cabeçalhos de solicitação para criptografia do lado do servidor

> ⓘ Para obter informações sobre como o StorageGRID lida com carateres UTF-8, "PutObject"consulte .

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os cabeçalhos de solicitação a seguir para criptografar um objeto multiparte com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE**: Use o seguinte cabeçalho na solicitação CreateMultipartUpload se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: Use todos esses três cabeçalhos na solicitação CreateMultipartUpload (e em cada solicitação UploadPart subsequente) se você quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.

- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações para "usando criptografia do lado do servidor".

Cabeçalhos de solicitação não suportados

O seguinte cabeçalho de solicitação não é suportado:

- `x-amz-website-redirect-location`

  O `x-amz-website-redirect-location` cabeçalho retorna `XNotImplemented`.

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

ListMultipartUploads

A operação ListMultipartUploads lista os carregamentos de várias partes em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

UploadPart

A operação UploadPart carrega uma parte em um upload multipart para um objeto.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou criptografia SSE-C para a solicitação CreateMultipartUpload, você também deve incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia fornecida na solicitação CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações no "Use a criptografia do lado do servidor".

Se você especificou uma soma de verificação SHA-256 durante a solicitação CreateMultipartUpload, você também deve incluir o seguinte cabeçalho de solicitação em cada solicitação UploadPart:

- `x-amz-checksum-sha256`: Especifique a soma de verificação SHA-256 para esta parte.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

UploadPartCopy

A operação UploadPartCopy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação UploadPartCopy é implementada com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.

Essa solicitação lê e grava os dados de objeto especificados no `x-amz-copy-source-range` sistema StorageGRID.

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou criptografia SSE-C para a solicitação CreateMultipartUpload, você também deve incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia fornecida na solicitação CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.

Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deve incluir os três cabeçalhos a seguir na solicitação UploadPartCopy, para que o objeto possa ser descriptografado e copiado:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia fornecida quando você criou o objeto de origem.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações no "Use a criptografia do lado do servidor".

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

Respostas de erro

O sistema StorageGRID suporta todas as respostas de erro padrão da API REST S3 que se aplicam. Além disso, a implementação do StorageGRID adiciona várias respostas

personalizadas.

Códigos de erro S3 API suportados

Nome	Status HTTP
AccessDenied	403 proibido
BadDigest	400 pedido incorreto
BucketAlreadyExists	409 conflito
BucketNotEmpty	409 conflito
IncompleteBody	400 pedido incorreto
InternalError (erro internacional)	500 erro interno do servidor
InvalidAccessKeyId	403 proibido
InvalidArgument	400 pedido incorreto
InvalidBucketName	400 pedido incorreto
InvalidBucketState	409 conflito
InvalidDigest	400 pedido incorreto
InvalidEncryptionAlgorithmError	400 pedido incorreto
InvalidPart	400 pedido incorreto
InvalidPartOrder	400 pedido incorreto
Intervalo Invalidável	416 intervalo solicitado não satisfatório
InvalidRequest	400 pedido incorreto
InvalidStorageClass	400 pedido incorreto
InvalidTag	400 pedido incorreto
InvalidURI	400 pedido incorreto
KeyTooLong	400 pedido incorreto

Nome	Status HTTP
MalformedXML	400 pedido incorreto
MetadataTooLarge	400 pedido incorreto
MetodNotAlloved	Método 405 não permitido
MissingContentLength	411 comprimento necessário
MissingRequestBodyError	400 pedido incorreto
MissingSecurityHeader	400 pedido incorreto
NoSuchBucket	404 não encontrado
NoSuchKey	404 não encontrado
NoSuchUpload	404 não encontrado
Sem Implementado	501 não implementado
NoSuchBucketPolicy	404 não encontrado
ObjectLockConfigurationNotFounError	404 não encontrado
Pré-condiçãoFailed	412 Pré-condição falhou
RequestTimeTooSwed	403 proibido
Serviço indisponível	503 Serviço indisponível
SignatureDoesNotMatch	403 proibido
TooManyBuckets	400 pedido incorreto
UserKeyMustBeSpecified	400 pedido incorreto

Códigos de erro personalizados do StorageGRID

Nome	Descrição	Status HTTP
XBucketLifecycleNotAllowed	A configuração do ciclo de vida do bucket não é permitida em um bucket compatível com legado	400 pedido incorreto

Nome	Descrição	Status HTTP
XBucketPolicyParseException	Falha ao analisar JSON da política de bucket recebida.	400 pedido incorreto
XComplianceConflict	Operação negada devido às configurações de conformidade legadas.	403 proibido
XComplianceReducedRedundancyForbidden	Redundância reduzida não é permitida no bucket em conformidade com o legado	400 pedido incorreto
XMaxBucketPolicyLengthExceeded	Sua política excede o comprimento máximo permitido da política de intervalo.	400 pedido incorreto
XMissingInternalRequestHeader	Falta um cabeçalho de uma solicitação interna.	400 pedido incorreto
XNoSuchBucketCompliance	O bucket especificado não tem conformidade legada habilitada.	404 não encontrado
XNotAcceptable	A solicitação contém um ou mais cabeçalhos de aceitação que não puderam ser satisfeitos.	406 não aceitável
XNotImplementado	A solicitação que você forneceu implica funcionalidade que não é implementada.	501 não implementado

Operações personalizadas do StorageGRID

Operações personalizadas do StorageGRID

O sistema StorageGRID dá suporte a operações personalizadas que são adicionadas à API REST do S3.

A tabela a seguir lista as operações personalizadas suportadas pelo StorageGRID.

Operação	Descrição
"OBTER consistência de balde"	Retorna a consistência que está sendo aplicada a um balde específico.
"COLOQUE a consistência do balde"	Define a consistência aplicada a um balde específico.
"OBTER último tempo de acesso do Bucket"	Retorna se as atualizações da última hora de acesso estão ativadas ou desativadas para um intervalo específico.
"COLOQUE o último tempo de acesso do balde"	Permite-lhe ativar ou desativar as atualizações da última hora de acesso para um intervalo específico.

Operação	Descrição
"ELIMINAR configuração de notificação de metadados do bucket"	Exclui o XML de configuração de notificação de metadados associado a um bucket específico.
"OBTER configuração de notificação de metadados do bucket"	Retorna o XML de configuração de notificação de metadados associado a um intervalo específico.
"COLOQUE a configuração de notificação de metadados do bucket"	Configura o serviço de notificação de metadados para um bucket.
"OBTER uso de armazenamento"	Indica a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.
"Obsoleto: CreateBucket com configurações de conformidade"	Obsoleto e não suportado: Você não pode mais criar novos buckets com a conformidade ativada.
"Obsoleto: OBTENHA conformidade com Bucket"	Obsoleto, mas suportado: Retorna as configurações de conformidade atualmente em vigor para um bucket compatível com legado existente.
"Obsoleto: COLOQUE a conformidade com Bucket"	Obsoleto, mas suportado: Permite modificar as configurações de conformidade para um bucket compatível com legado existente.

OBTER consistência de balde

A solicitação GET Bucket Consistency permite determinar a consistência que está sendo aplicada a um determinado bucket.

A consistência padrão é definida para garantir leitura após gravação para objetos recém-criados.

Você deve ter a permissão S3:GetBucketConsistency, ou ser raiz da conta, para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Resposta

No XML de resposta `<Consistency>`, retornará um dos seguintes valores:

Consistência	Descrição
tudo	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
forte local	Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
leitura-após-nova-gravação	(Padrão) fornece consistência de leitura após gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
disponível	Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

Exemplo de resposta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informações relacionadas

"Valores de consistência"

COLOQUE a consistência do balde

A solicitação de consistência do PUT Bucket permite especificar a consistência a ser aplicada às operações realizadas em um bucket.

A consistência padrão é definida para garantir leitura após gravação para objetos recém-criados.

Antes de começar

Você deve ter a permissão S3:PutBucketConsistency, ou ser raiz da conta, para concluir esta operação.

Pedido

O `x-ntap-sg-consistency` parâmetro deve conter um dos seguintes valores:

Consistência	Descrição
tudo	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
forte local	Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
leitura-após-nova-gravação	(Padrão) fornece consistência de leitura após gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
disponível	Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

Nota: em geral, você deve usar a consistência "Read-after-new-write". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar a consistência para cada solicitação de API. Defina a consistência no nível do balde apenas como último recurso.

Exemplo de solicitação

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informações relacionadas

"Valores de consistência"

OBTER último tempo de acesso do Bucket

A solicitação de última hora de acesso do GET Bucket permite determinar se as atualizações da última hora de acesso estão ativadas ou desativadas para buckets individuais.

Você deve ter a permissão S3:GetBucketLastAccessTime, ou ser raiz da conta, para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

Este exemplo mostra que as atualizações da última hora de acesso estão ativadas para o intervalo.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

COLOQUE o último tempo de acesso do balde

A solicitação de última hora de acesso do PUT Bucket permite ativar ou desativar as atualizações da última hora de acesso para intervalos individuais. A desativação das atualizações da última hora de acesso melhora o desempenho e é a configuração padrão para todos os buckets criados com a versão 10,3.0 ou posterior.

Você deve ter a permissão S3:PutBucketLastAccessTime para um bucket, ou ser raiz da conta, para concluir esta operação.

> A partir da versão 10,3 do StorageGRID, as atualizações da última hora de acesso são desativadas por padrão para todos os novos buckets. Se você tiver buckets criados usando uma versão anterior do StorageGRID e quiser corresponder ao novo comportamento padrão, desative explicitamente as atualizações da última hora de acesso para cada um desses buckets anteriores. Você pode ativar ou desativar as atualizações para o último tempo de acesso usando a solicitação de última hora de acesso do PUT Bucket ou a partir da página de detalhes de um bucket no Gerenciador do Locatário. "Ative ou desative as atualizações da última hora de acesso"Consulte .

Se as atualizações da última hora de acesso estiverem desativadas para um bucket, o seguinte comportamento é aplicado às operações no bucket:

- As solicitações GetObject, GetObjectAcl, GetObjectTagging e HeadObject não atualizam o último tempo de acesso. O objeto não é adicionado às filas para avaliação do gerenciamento do ciclo de vida das informações (ILM).
- As solicitações CopyObject e PutObjectTagging que atualizam apenas os metadados também atualizam a última hora de acesso. O objeto é adicionado às filas para avaliação ILM.
- Se as atualizações para a última hora de acesso estiverem desativadas para o intervalo de origem, as solicitações de CopyObject não atualizam a última hora de acesso para o intervalo de origem. O objeto que foi copiado não é adicionado às filas para avaliação ILM para o bucket de origem. No entanto, para o destino, as solicitações de CopyObject sempre atualizam a última hora de acesso. A cópia do objeto é adicionada às filas para avaliação ILM.
- CompleteMultipartUpload Requests atualizam o último tempo de acesso. O objeto concluído é adicionado às filas para avaliação ILM.

Exemplos de pedidos

Este exemplo permite o último tempo de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Este exemplo desativa a última hora de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

ELIMINAR configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados DELETE Bucket permite desativar o serviço de integração de pesquisa para buckets individuais excluindo o XML de configuração.

Você deve ter a permissão S3:DeleteBucketMetadataNotification para um bucket, ou ser raiz de conta, para concluir esta operação.

Exemplo de solicitação

Este exemplo mostra a desativação do serviço de integração de pesquisa para um bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

OBTER configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados do GET Bucket permite recuperar o XML de configuração usado para configurar a integração de pesquisa para buckets individuais.

Você deve ter a permissão S3:GetBucketMetadataNotification, ou ser raiz da conta, para concluir esta operação.

Exemplo de solicitação

Essa solicitação recupera a configuração de notificação de metadados para o bucket chamado `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Resposta

O corpo da resposta inclui a configuração de notificação de metadados para o bucket. A configuração de notificação de metadados permite determinar como o intervalo é configurado para integração de pesquisa. Ou seja, ele permite determinar quais objetos são indexados e quais endpoints seus metadados de objeto estão sendo enviados.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Cada configuração de notificação de metadados inclui uma ou mais regras. Cada regra especifica os objetos aos quais se aplica e o destino onde o StorageGRID deve enviar metadados de objeto. Os destinos devem ser especificados usando a URNA de um endpoint StorageGRID.

Nome	Descrição	Obrigatório
MetadataNotificationConfiguration	Tag de contentor para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos de regra.	Sim
Regra	Tag container para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
ID	Identificador exclusivo para a regra. Incluído no elemento regra.	Não
Estado	O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas. Incluído no elemento regra.	Sim

Nome	Descrição	Obrigatório
Prefixo	Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento regra.	Sim
Destino	Etiqueta de contentor para o destino de uma regra. Incluído no elemento regra.	Sim
Urna	URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário `domain-name/myindex/mytype`. Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O endpoint deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. Urna está incluído no elemento destino.	Sim

Exemplo de resposta

O XML incluído entre as `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags mostra como a integração com um endpoint de integração de pesquisa é configurada para o bucket. Neste exemplo, metadados de objeto estão sendo enviados para um índice Elasticsearch nomeado `current` e tipo nomeado `2017` que está hospedado em um domínio da AWS `records` chamado .

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informações relacionadas

"Use uma conta de locatário"

COLOQUE a configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados do PUT Bucket permite ativar o serviço de integração de pesquisa para buckets individuais. O XML de configuração de notificação de metadados que você fornece no corpo da solicitação especifica os objetos cujos metadados são enviados para o índice de pesquisa de destino.

Você deve ter a permissão S3:PutBucketMetadataNotification para um bucket, ou ser raiz de conta, para concluir esta operação.

Pedido

A solicitação deve incluir a configuração de notificação de metadados no corpo da solicitação. Cada configuração de notificação de metadados inclui uma ou mais regras. Cada regra especifica os objetos aos quais se aplica e o destino ao qual o StorageGRID deve enviar metadados de objetos.

Os objetos podem ser filtrados no prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `/images` para um destino e objetos com o prefixo `/videos` para outro.

As configurações que têm prefixos sobrepostos não são válidas e são rejeitadas quando são enviadas. Por exemplo, uma configuração que incluía uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não seria permitida.

Os destinos devem ser especificados usando a URNA de um endpoint StorageGRID. O endpoint deve existir quando a configuração de notificação de metadados é enviada ou a solicitação falha como um `400 Bad`

`Request`. a mensagem de erro afirma: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

A tabela descreve os elementos no XML de configuração de notificação de metadados.

Nome	Descrição	Obrigatório
MetadataNotificationConfiguration	Tag de contentor para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos de regra.	Sim
Regra	Tag container para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
ID	Identificador exclusivo para a regra. Incluído no elemento regra.	Não
Estado	O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas. Incluído no elemento regra.	Sim

Nome	Descrição	Obrigatório
Prefixo	Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento regra.	Sim
Destino	Etiqueta de contentor para o destino de uma regra. Incluído no elemento regra.	Sim
Urna	URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário `domain-name/myindex/mytype`. Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O endpoint deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. Urna está incluído no elemento destino.	Sim

Exemplos de pedidos

Este exemplo mostra a ativação da integração de pesquisa para um bucket. Neste exemplo, metadados de objetos para todos os objetos são enviados para o mesmo destino.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Neste exemplo, metadados de objetos para objetos que correspondem ao prefixo `/images` são enviados para um destino, enquanto metadados de objetos para objetos que correspondem ao prefixo `/videos` são enviados para um segundo destino.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON gerado pelo serviço de integração de pesquisa

Quando você ativa o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado para o endpoint de destino cada vez que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

Este exemplo mostra um exemplo do JSON que pode ser gerado quando um objeto com a chave `SGWS/Tagging.txt` é criado em um intervalo `test` chamado . O `test` bucket não está versionado, então a `versionId` tag está vazia.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadados de objetos incluídos nas notificações de metadados

A tabela lista todos os campos que estão incluídos no documento JSON que é enviado para o endpoint de destino quando a integração de pesquisa está ativada.

O nome do documento inclui o nome do intervalo, o nome do objeto e a ID da versão, se presente.

Tipo	Nome do item	Descrição
Informações sobre o balde e o objeto	balde	Nome do balde
Informações sobre o balde e o objeto	chave	Nome da chave do objeto
Informações sobre o balde e o objeto	ID de versão	Versão do objeto, para objetos em buckets versionados
Informações sobre o balde e o objeto	região	Região do balde, por exemplo `us-east-1`
Metadados do sistema	tamanho	Tamanho do objeto (em bytes) como visível para um cliente HTTP
Metadados do sistema	md5	Hash de objeto
Metadados do usuário	metadados *`key:value`*	Todos os metadados de usuário para o objeto, como pares de chave-valor

Tipo	Nome do item	Descrição
Tags	tags *key:value*	Todas as tags de objeto definidas para o objeto, como pares chave-valor

> Para tags e metadados de usuários, o StorageGRID passa datas e números para o Elasticsearch como strings ou como notificações de eventos do S3. Para configurar o Elasticsearch para interpretar essas strings como datas ou números, siga as instruções do Elasticsearch para mapeamento de campos dinâmicos e para os formatos de data de mapeamento. Você deve ativar os mapeamentos de campo dinâmicos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

Informações relacionadas

"Use uma conta de locatário"

OBTER solicitação de uso de armazenamento

A solicitação OBTER uso do armazenamento informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.

A quantidade de armazenamento usada por uma conta e seus buckets pode ser obtida por uma solicitação de ListBuckets modificada com o `x-ntap-sg-usage` parâmetro de consulta. O uso do armazenamento de buckets é rastreado separadamente das SOLICITAÇÕES DE PUT e DELETE processadas pelo sistema. Pode haver algum atraso antes que os valores de uso correspondam aos valores esperados com base no processamento de solicitações, especialmente se o sistema estiver sob carga pesada.

Por padrão, o StorageGRID tenta recuperar informações de uso usando consistência global forte. Se a consistência global forte não puder ser alcançada, o StorageGRID tentará recuperar as informações de uso em uma consistência de site forte.

Você deve ter a permissão S3:ListAllMyBuckets, ou ser root da conta, para concluir esta operação.

Exemplo de solicitação

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

Este exemplo mostra uma conta que tem quatro objetos e 12 bytes de dados em dois buckets. Cada bucket contém dois objetos e seis bytes de dados.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Controle de versão

Cada versão de objeto armazenada contribuirá para os `ObjectCount` valores e `DataBytes` na resposta. Excluir marcadores não são adicionados ao `ObjectCount` total.

Informações relacionadas

"Valores de consistência"

Solicitações de bucket obsoletas para conformidade legada

Solicitações de bucket obsoletas para conformidade legada

Talvez seja necessário usar a API REST do StorageGRID S3 para gerenciar buckets criados com o recurso de conformidade legado.

Funcionalidade de conformidade obsoleta

O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3.

Se você ativou anteriormente a configuração de conformidade global, a configuração de bloqueio de objeto global S3 será ativada no StorageGRID 11,6. Você não pode mais criar novos buckets com a conformidade ativada. No entanto, conforme necessário, você pode usar a API REST do StorageGRID S3 para gerenciar buckets em conformidade existentes.

- "Use a API REST do S3 para configurar o bloqueio de objetos do S3"
- "Gerenciar objetos com ILM"
- "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

Solicitações de conformidade obsoletas:

- "Obsoleto - COLOCAR modificações de solicitação de balde para conformidade"

  O elemento SGCompliance XML está obsoleto. Anteriormente, você poderia incluir esse elemento personalizado do StorageGRID no corpo opcional da solicitação XML de SOLICITAÇÕES PUT Bucket para criar um bucket compatível.

- "Obsoleto - OBTER conformidade com balde"

  A solicitação de conformidade GET Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket em conformidade legado existente.

- "Obsoleto - COLOCAR conformidade com balde"

  A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para modificar as configurações de conformidade de um bucket em conformidade com o legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.

Obsoleto: CreateBucket solicita modificações para conformidade

O elemento SGCompliance XML está obsoleto. Anteriormente, você poderia incluir esse elemento personalizado do StorageGRID no corpo opcional de solicitação XML das solicitações do CreateBucket para criar um bucket compatível.

> O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3. Consulte o seguinte para obter mais detalhes:
>
> - "Use a API REST do S3 para configurar o bloqueio de objetos do S3"
> - "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

Você não pode mais criar novos buckets com a conformidade ativada. A seguinte mensagem de erro é retornada se você tentar usar o CreateBucket solicitar modificações para conformidade para criar um novo bucket compatível:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsoleto: OBTER solicitação de conformidade do bucket

A solicitação de conformidade GET Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket em conformidade legado existente.

> O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3. Consulte o seguinte para obter mais detalhes:
>
> - "Use a API REST do S3 para configurar o bloqueio de objetos do S3"
> - "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

Você deve ter a permissão S3:GetBucketCompliance, ou ser raiz da conta, para concluir esta operação.

Exemplo de solicitação

Esta solicitação de exemplo permite que você determine as configurações de conformidade para o bucket chamado `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

No XML de resposta, `<SGCompliance>` lista as configurações de conformidade em vigor para o bucket. Este exemplo de resposta mostra as configurações de conformidade de um intervalo no qual cada objeto será retido por um ano (525.600 minutos), a partir de quando o objeto é ingerido na grade. Atualmente, não existe qualquer retenção legal neste intervalo. Cada objeto será automaticamente excluído após um ano.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Repetição de PeriodMinutes	A duração do período de retenção para objetos adicionados a este intervalo, em minutos. O período de retenção começa quando o objeto é ingerido na grade.
LegalHod	• Verdadeiro: Este balde está atualmente sob uma guarda legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja levantada, mesmo que seu período de retenção tenha expirado. • Falso: Este balde não está atualmente sob um guarda legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Autodelete	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob uma retenção legal. • Falso: Os objetos neste intervalo não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Respostas de erro

Se o intervalo não foi criado para ser compatível, o código de status HTTP para a resposta é `404 Not Found`, com um código de erro S3 de `XNoSuchBucketCompliance`.

Obsoleto: COLOQUE a solicitação de conformidade do bucket

A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para modificar as configurações de conformidade de um bucket em conformidade com o legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.

O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3. Consulte o seguinte para obter mais detalhes:

- "Use a API REST do S3 para configurar o bloqueio de objetos do S3"
- "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

Você deve ter a permissão S3:PutBucketCompliance, ou ser root da conta, para concluir esta operação.

Você deve especificar um valor para cada campo das configurações de conformidade ao emitir uma solicitação de conformidade PUT Bucket.

Exemplo de solicitação

Esta solicitação de exemplo modifica as configurações de conformidade para o bucket `mybucket` chamado . Neste exemplo, os objetos em `mybucket` agora serão retidos por dois anos (1.051.200 minutos) em vez de um ano, a partir de quando o objeto é ingerido na grade. Não há retenção legal neste balde. Cada objeto será automaticamente excluído após dois anos.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Repetição de PeriodMinutes	A duração do período de retenção para objetos adicionados a este intervalo, em minutos. O período de retenção começa quando o objeto é ingerido na grade. **Importante** ao especificar um novo valor para RetentionPeriodMinutes, você deve especificar um valor igual ou maior que o período de retenção atual do bucket. Depois que o período de retenção do bucket for definido, você não poderá diminuir esse valor; você só poderá aumentá-lo.

Nome	Descrição
LegalHod	• Verdadeiro: Este balde está atualmente sob uma guarda legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja levantada, mesmo que seu período de retenção tenha expirado. • Falso: Este balde não está atualmente sob um guarda legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Autodelete	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob uma retenção legal. • Falso: Os objetos neste intervalo não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Consistência para configurações de conformidade

Quando você atualiza as configurações de conformidade de um bucket do S3 com uma solicitação de conformidade de ARMAZENAMENTO, o StorageGRID tenta atualizar os metadados do bucket na grade. Por padrão, o StorageGRID usa a consistência **strong-global** para garantir que todos os sites de data center e todos os nós de storage que contêm metadados de bucket tenham consistência de leitura após gravação para as configurações de conformidade alteradas.

Se o StorageGRID não conseguir obter a consistência **strong-global** porque um site de data center ou vários nós de armazenamento em um site não estão disponíveis, o código de status HTTP para a resposta é `503 Service Unavailable`.

Se você receber essa resposta, entre em Contato com o administrador da grade para garantir que os serviços de armazenamento necessários sejam disponibilizados o mais rápido possível. Se o administrador da grade não conseguir disponibilizar o suficiente dos nós de armazenamento em cada local, o suporte técnico pode direcioná-lo a tentar novamente a solicitação com falha, forçando a consistência **strong-site**.

> Nunca force a consistência **strong-site** para a conformidade com o bucket, a menos que você tenha sido direcionado a fazê-lo por suporte técnico e a menos que você entenda as possíveis consequências de usar esse nível.

Quando a consistência é reduzida para **strong-site**, o StorageGRID garante que as configurações de conformidade atualizadas terão consistência de leitura após gravação apenas para solicitações de clientes dentro de um site. Isso significa que o sistema StorageGRID pode ter temporariamente várias configurações inconsistentes para esse intervalo até que todos os sites e nós de storage estejam disponíveis. As definições inconsistentes podem resultar num comportamento inesperado e indesejado. Por exemplo, se você estiver colocando um bucket sob uma retenção legal e forçar uma consistência menor, as configurações de conformidade anteriores do bucket (ou seja, retenção legal) podem continuar em vigor em alguns sites de data center. Como resultado, os objetos que você acha que estão em retenção legal podem ser excluídos quando seu período de retenção expirar, seja pelo usuário ou pela exclusão automática, se ativado.

Para forçar o uso da consistência **strong-site**, volte a emitir a solicitação de conformidade PUT Bucket e inclua o `Consistency-Control` cabeçalho de solicitação HTTP, da seguinte forma:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respostas de erro

- Se o intervalo não foi criado para ser compatível, o código de status HTTP para a resposta é `404 Not Found`.
- Se `RetentionPeriodMinutes` na solicitação for inferior ao período de retenção atual do bucket, o código de status HTTP será `400 Bad Request`.

Informações relacionadas

"Obsoleto: Modificações de solicitação de Bucket para conformidade"

Políticas de acesso ao bucket e ao grupo

Use políticas de acesso de grupo e bucket

O StorageGRID usa a linguagem de política da Amazon Web Services (AWS) para permitir que os locatários do S3 controlem o acesso a buckets e objetos nesses buckets. O sistema StorageGRID implementa um subconjunto da linguagem de política da API REST S3. As políticas de acesso para a API S3 são escritas em JSON.

Visão geral da política de acesso

Existem dois tipos de políticas de acesso suportadas pelo StorageGRID.

- **Políticas de bucket**, que são gerenciadas usando as operações de API GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy S3 ou o Tenant Manager ou a API de Gerenciamento de Tenant. As políticas de bucket são anexadas a buckets, portanto, são configuradas para controlar o acesso dos usuários na conta de proprietário do bucket ou outras contas ao bucket e aos objetos nele contidos. Uma política de bucket se aplica a apenas um bucket e possivelmente a vários grupos.
- **Políticas de grupo**, que são configuradas usando o Gerenciador do locatário ou a API de gerenciamento do locatário. As políticas de grupo são anexadas a um grupo na conta, portanto são configuradas para permitir que esse grupo acesse recursos específicos de propriedade dessa conta. Uma política de grupo se aplica a apenas um grupo e possivelmente vários buckets.

> Não há diferença na prioridade entre as políticas de grupo e bucket.

As políticas de grupo e bucket do StorageGRID seguem uma gramática específica definida pela Amazon. Dentro de cada política há uma matriz de declarações de política, e cada declaração contém os seguintes elementos:

- ID de declaração (Sid) (opcional)
- Efeito
- Principal/NotPrincipal
- Recurso/não recurso
- Ação/não Ação

- Condição (opcional)

As instruções de política são criadas usando essa estrutura para especificar permissões: Grant <Effect> para permitir/negar que o <Principal> execute o <Action> no <Resource> quando o <Condition> se aplicar.

Cada elemento de política é usado para uma função específica:

Elemento	Descrição
SID	O elemento Sid é opcional. O Sid é apenas uma descrição para o usuário. Ele é armazenado, mas não interpretado pelo sistema StorageGRID.
Efeito	Use o elemento efeito para determinar se as operações especificadas são permitidas ou negadas. É necessário identificar operações que você permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Ação suportado.
Principal/NotPrincipal	Você pode permitir que usuários, grupos e contas acessem recursos específicos e executem ações específicas. Se nenhuma assinatura S3 estiver incluída na solicitação, o acesso anônimo será permitido especificando o caractere curinga (*) como principal. Por padrão, somente a raiz da conta tem acesso aos recursos de propriedade da conta. Você só precisa especificar o elemento principal em uma política de bucket. Para políticas de grupo, o grupo ao qual a política está anexada é o elemento principal implícito.
Recurso/não recurso	O elemento recurso identifica buckets e objetos. Você pode permitir ou negar permissões a buckets e objetos usando o Nome do recurso da Amazon (ARN) para identificar o recurso.
Ação/não Ação	Os elementos Ação e efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, é concedido ou negado o acesso ao recurso. O acesso é negado a menos que você atribua permissões especificamente, mas você pode usar Negar explícito para substituir uma permissão concedida por outra política.
Condição	O elemento de condição é opcional. As condições permitem que você crie expressões para determinar quando uma política deve ser aplicada.

No elemento Ação, você pode usar o caractere curinga (*) para especificar todas as operações ou um subconjunto de operações. Por exemplo, esta Ação corresponde a permissões como S3:GetObject, S3:PutObject e S3:DeleteObject.

```
s3:*Object
```

No elemento recurso, você pode usar os carateres curinga (**) e (?). Enquanto o asterisco (**) corresponde a 0 ou mais carateres, o ponto de interrogação (?) corresponde a qualquer caractere único.

No elemento principal, carateres curinga não são suportados, exceto para definir acesso anônimo, o que concede permissão a todos. Por exemplo, você define o caractere curinga (*) como o valor principal.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

No exemplo a seguir, a instrução está usando os elementos efeito, Principal, Ação e recurso. Este exemplo mostra uma declaração de política de bucket completa que usa o efeito "permitir" para dar aos Principals, ao grupo admin `federated-group/admin` e ao grupo financeiro `federated-group/finance` , permissões para executar a Ação `s3:ListBucket` no bucket nomeado e a Ação `s3:GetObject` em todos os objetos dentro desse bucket `mybucket`.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

A política de bucket tem um limite de tamanho de 20.480 bytes e a política de grupo tem um limite de tamanho de 5.120 bytes.

Consistência para políticas

Por padrão, quaisquer atualizações feitas para políticas de grupo são eventualmente consistentes. Quando uma política de grupo se torna consistente, as alterações podem levar mais 15 minutos para entrar em vigor, devido ao armazenamento em cache de políticas. Por padrão, todas as atualizações feitas às políticas de bucket são altamente consistentes.

Conforme necessário, você pode alterar as garantias de consistência para atualizações de política de bucket.

Por exemplo, você pode querer que uma alteração em uma política de bucket esteja disponível durante uma falha no local.

Nesse caso, você pode definir o `Consistency-Control` cabeçalho na solicitação PutBucketPolicy ou usar a solicitação DE consistência de COLOCAR bucket. Quando uma política de bucket se torna consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao armazenamento em cache de políticas.

> Se você definir a consistência para um valor diferente para contornar uma situação temporária, certifique-se de definir a configuração do nível do balde de volta ao valor original quando terminar. Caso contrário, todas as futuras solicitações de bucket usarão a configuração modificada.

Use ARN em declarações de política

Em declarações de política, o ARN é usado em elementos Principal e recursos.

- Use esta sintaxe para especificar o ARN de recursos S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Use esta sintaxe para especificar o ARN do recurso de identidade (usuários e grupos):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Outras considerações:

- Você pode usar o asterisco (*) como curinga para corresponder a zero ou mais carateres dentro da chave de objeto.
- Carateres internacionais, que podem ser especificados na chave do objeto, devem ser codificados usando JSON UTF-8 ou usando sequências de escape JSON. A codificação percentual não é suportada.

  "RFC 2141 sintaxe de URNA"

  O corpo de solicitação HTTP para a operação PutBucketPolicy deve ser codificado com charset UTF-8.

Especifique recursos em uma política

Em declarações de política, você pode usar o elemento recurso para especificar o intervalo ou objeto para o qual as permissões são permitidas ou negadas.

- Cada declaração de política requer um elemento recurso. Em uma política, os recursos são denotados pelo elemento `Resource` ou, alternativamente, `NotResource` para exclusão.

- Você especifica recursos com um ARN de recursos S3. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Você também pode usar variáveis de política dentro da chave de objeto. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- O valor do recurso pode especificar um intervalo que ainda não existe quando uma política de grupo é criada.

Especifique princípios em uma política

Use o elemento principal para identificar a conta de usuário, grupo ou locatário que é permitido/negado acesso ao recurso pela declaração de política.

- Cada declaração de política em uma política de bucket deve incluir um elemento principal. As declarações de política em uma política de grupo não precisam do elemento principal porque o grupo é entendido como o principal.
- Em uma política, os princípios são denotados pelo elemento "principal" ou, alternativamente, "NotPrincipal" para exclusão.
- As identidades baseadas em contas devem ser especificadas usando um ID ou um ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Este exemplo usa o ID de conta de locatário 27233906934684427525, que inclui a raiz da conta e todos os usuários na conta:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Você pode especificar apenas a raiz da conta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Você pode especificar um usuário federado específico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Você pode especificar um grupo federado específico ("gerentes"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Você pode especificar um principal anônimo:

```
"Principal": "*"
```

- Para evitar ambiguidade, você pode usar o usuário UUID em vez do nome de usuário:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Por exemplo, suponha que Alex deixe a organização e o nome de usuário `Alex` seja excluído. Se um novo Alex se juntar à organização e receber o mesmo `Alex` nome de usuário, o novo usuário poderá involuntariamente herdar as permissões concedidas ao usuário original.

- O valor principal pode especificar um nome de grupo/usuário que ainda não existe quando uma política de bucket é criada.

Especifique permissões em uma política

Em uma política, o elemento Ação é usado para permitir/negar permissões a um recurso. Há um conjunto de permissões que você pode especificar em uma política, que são denotadas pelo elemento "Ação" ou, alternativamente, "NotAction" para exclusão. Cada um desses elementos mapeia para operações específicas da API REST do S3.

As tabelas lista as permissões que se aplicam aos buckets e as permissões que se aplicam aos objetos.

> O Amazon S3 agora usa a permissão S3:PutReplicationConfiguration para as ações PutBucketReplication e DeleteBucketReplication. O StorageGRID usa permissões separadas para cada ação, que corresponde à especificação original do Amazon S3.

> Uma exclusão é executada quando uma put é usada para substituir um valor existente.

Permissões que se aplicam a buckets

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:CreateBucket	CreateBucket	Sim. **Nota**: Use somente na política de grupo.
S3:DeleteBucket	DeleteBucket	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:DeleteBucketMetadataNotification	ELIMINAR configuração de notificação de metadados do bucket	Sim
S3:DeleteBucketPolicy	DeleteBucketPolicy	
S3:DeleteReplicationConfiguration	DeleteBucketReplication	Sim, permissões separadas para COLOCAR e EXCLUIR
S3:GetBucketAcl	GetBucketAcl	
S3:GetBucketCompliance	OBTER conformidade com balde (obsoleto)	Sim
S3:GetBucketConsistência	OBTER consistência de balde	Sim
S3:GetBucketCORS	GetBucketCors	
S3:GetEncryptionConfiguration	GetBucketEncryption	
S3:GetBucketLastAccessTime	OBTER último tempo de acesso do Bucket	Sim
S3:GetBucketLocation	GetBucketlocalização	
S3:GetBucketMetadataNotification	OBTER configuração de notificação de metadados do bucket	Sim
S3:GetBucketNotification	GetBucketNotificationConfiguration	
S3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
S3:GetBucketPolicy	Política de GetBucketPolicy	
S3:GetBucketTagging	GetBucketTagging	
S3:GetBucketControle de versão	GetBucketControle de versão	
S3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
S3:GetReplicationConfiguration	GetBucketReplication	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:ListAllMyBuckets	• ListBuckets • OBTER uso de armazenamento	Sim, para OBTER uso de armazenamento. **Nota**: Use somente na política de grupo.
S3: ListBucket	• ListObjects • Balde para a cabeça • RestoreObject	
S3:ListBucketMultipartUploads	• ListMultipartUploads • RestoreObject	
S3:ListBucketVersions	OBTER versões Bucket	
S3:PutBucketCompliance	COLOCAR conformidade com balde (obsoleto)	Sim
S3:PutBucketConsistência	COLOQUE a consistência do balde	Sim
S3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
S3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
S3:PutBucketLastAccessTime	COLOQUE o último tempo de acesso do balde	Sim
S3:PutBucketMetadataNotification	COLOQUE a configuração de notificação de metadados do bucket	Sim
S3:PutBucketNotification	PutBucketNotificationConfiguration	
S3:PutBucketObjectLockConfiguration	• CreateBucket com o `x-amz-bucket-object-lock-enabled: true` cabeçalho de solicitação (também requer a permissão S3:CreateBucket) • PutObjectLockConfiguration	
S3:PutBucketPolicy	Política de PutBucketPolicy	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:PutBucketTagging	• DeleteBucketTagging† • PutBucketTagging	
S3:PutBucketControle de versão	PutBucketControle de versão	
S3:PutLifecycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
S3:PutReplicationConfiguration	PutBucketReplication	Sim, permissões separadas para COLOCAR e EXCLUIR

Permissões que se aplicam a objetos

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
S3:BypassGovernanceretenção	• DeleteObject • DeleteObjects • Retenção PutObjectRetention	
S3:DeleteObject	• DeleteObject • DeleteObjects • RestoreObject	
S3:DeleteObjectTagging	DeleteObjectTagging	
S3:DeleteObjectVersionTagging	DeleteObjectTagging (uma versão específica do objeto)	
S3:DeleteObjectVersion	DeleteObject (uma versão específica do objeto)	
S3:GetObject	• GetObject • HeadObject • RestoreObject • Selecione ObjectContent	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetObjectAcl	GetObjectAcl	
S3:GetObjectLegalHod	GetObjectLegalHod	
S3:GetObjectRetention	GetObjectRetention	
S3:GetObjectTagging	GetObjectTagging	
S3:GetObjectVersionTagging	GetObjectTagging (uma versão específica do objeto)	
S3:GetObjectVersion	GetObject (uma versão específica do objeto)	
S3:ListMultipartUploadParts	ListParts, RestoreObject	
S3:PutObject	• PutObject • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
S3:PutObjectLegalHod	PutObjectLegalHod	
S3:retenção de objetos Put	Retenção PutObjectRetention	
S3:PutObjectTagging	Marcação de objetos	
S3:PutObjectVersionTagging	PutObjectTagging (uma versão específica do objeto)	
S3:PutOverwriteObject	• PutObject • CopyObject • Marcação de objetos • DeleteObjectTagging • CompleteMultipartUpload	Sim
S3:RestoreObject	RestoreObject	

Use a permissão PutOverwriteObject

A permissão S3:PutOverwriteObject é uma permissão StorageGRID personalizada que se aplica a operações que criam ou atualizam objetos. A configuração dessa permissão determina se o cliente pode substituir os dados de um objeto, metadados definidos pelo usuário ou marcação de objeto S3.

As configurações possíveis para essa permissão incluem:

- **Allow**: O cliente pode substituir um objeto. Esta é a configuração padrão.
- **Deny**: O cliente não pode sobrescrever um objeto. Quando definida como Negar, a permissão PutOverwriteObject funciona da seguinte forma:
  - Se um objeto existente for encontrado no mesmo caminho:
    - Os dados do objeto, metadados definidos pelo usuário ou marcação de objeto S3 não podem ser sobrescritos.
    - Todas as operações de ingestão em andamento são canceladas e um erro é retornado.
    - Se o controle de versão S3 estiver ativado, a configuração Negar impede que as operações PutObjectTagging ou DeleteObjectTagging modifiquem o TagSet para um objeto e suas versões não atuais.
  - Se um objeto existente não for encontrado, essa permissão não terá efeito.
- Quando esta permissão não está presente, o efeito é o mesmo que se permitir foi definido.

> Se a política S3 atual permitir a substituição e a permissão PutOverwriteObject estiver definida como Negar, o cliente não poderá substituir os dados de um objeto, metadados definidos pelo usuário ou marcação de objeto. Além disso, se a caixa de verificação **Prevent client modifition** estiver selecionada (**CONFIGURATION** > **Security settings** > **Network and Objects**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Especifique condições em uma política

As condições definem quando uma política estará em vigor. As condições consistem em operadores e pares de valor-chave.

Condições Use pares chave-valor para avaliação. Um elemento de condição pode conter várias condições, e cada condição pode conter vários pares de chave-valor. O bloco de condição usa o seguinte formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

No exemplo a seguir, a condição ipaddress usa a chave de condição SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operadores de condição suportados

Os operadores de condição são categorizados da seguinte forma:

- Cadeia de carateres
- Numérico
- Booleano
- Endereço IP
- Verificação nula

Operadores de condição	Descrição
StringEquals	Compara uma chave com um valor de string baseado na correspondência exata (sensível a maiúsculas e minúsculas).
StringNotEquals	Compara uma chave com um valor de string baseado em correspondência negada (sensível a maiúsculas e minúsculas).
StringEquaisIgnoreCase	Compara uma chave com um valor de string baseado na correspondência exata (ignora caso).
StringNotEquaisIgnoreCase	Compara uma chave com um valor de string baseado em correspondência negada (ignora caso).
StringLike	Compara uma chave com um valor de string baseado na correspondência exata (sensível a maiúsculas e minúsculas). Pode incluir * e ? carateres curinga.
StringNotLike	Compara uma chave com um valor de string baseado em correspondência negada (sensível a maiúsculas e minúsculas). Pode incluir * e ? carateres curinga.
NumericEquals	Compara uma chave com um valor numérico baseado na correspondência exata.
NumericNotEquals	Compara uma chave com um valor numérico baseado em correspondência negada.

Operadores de condição	Descrição
NumericGreaterThan	Compara uma chave com um valor numérico baseado na correspondência "maior que".
NumericGreaterThanEquals	Compara uma chave com um valor numérico baseado na correspondência "maior que ou igual".
NumericLessThan	Compara uma chave com um valor numérico baseado na correspondência "inferior a".
NumericLessThanEquals	Compara uma chave com um valor numérico baseado na correspondência "inferior ou igual".
Bool	Compara uma chave com um valor booleano baseado na correspondência "verdadeiro ou falso".
Endereço IP	Compara uma chave com um endereço IP ou intervalo de endereços IP.
NotIpAddress	Compara uma chave com um endereço IP ou um intervalo de endereços IP com base na correspondência negada.
Nulo	Verifica se uma chave de condição está presente no contexto de solicitação atual.

Teclas de condição suportadas

Teclas de condição	Ações	Descrição
AWS:SourceIp	Operadores IP	Irá comparar com o endereço IP a partir do qual a solicitação foi enviada. Pode ser usado para operações de balde ou objetos. **Observação:** se a solicitação S3 tiver sido enviada pelo serviço Load Balancer nos nós Admin e Gateways, isso será comparado ao endereço IP upstream do serviço Load Balancer. **Nota**: Se um balanceador de carga não transparente de terceiros for usado, isso será comparado ao endereço IP desse balanceador de carga. Qualquer `X-Forwarded-For` cabeçalho será ignorado porque sua validade não pode ser determinada.
aws:nome de usuário	Recurso/identidade	Irá comparar com o nome de usuário do remetente a partir do qual a solicitação foi enviada. Pode ser usado para operações de balde ou objetos.

Teclas de condição	Ações	Descrição
s3:delimitador	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro delimitador especificado em uma solicitação ListObjects ou ListObjectVersions.
S3: ExistingObjectTag/<tag-key>	S3:DeleteObjectTagging S3:DeleteObjectVersionTagging S3:GetObject S3:GetObjectAcl 3:GetObjectTagging S3:GetObjectVersion S3:GetObjectVersionAcl S3:GetObjectVersionTagging S3:PutObjectAcl S3:PutObjectTagging S3:PutObjectVersionAcl S3:PutObjectVersionTagging	Exigirá que o objeto existente tenha a chave e o valor específicos da tag.
s3: teclas de max	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro Max-keys especificado em uma solicitação ListObjects ou ListObjectVersions.
s3: object-lock-resting-retension-days	S3:PutObject	Compara com a data de retenção até especificada no `x-amz-object-lock-retain-until-date` cabeçalho da solicitação ou calculada a partir do período de retenção padrão do intervalo para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações: • PutObject • CopyObject • CreateMultipartUpload

Teclas de condição	Ações	Descrição
s3: object-lock-resting-retension-days	S3:retenção de objetos Put	Compara com a data de retenção até especificada na solicitação PutObjectRetention para garantir que ela esteja dentro do intervalo permitido.
s3:prefixo	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro prefix especificado em uma solicitação ListObjects ou ListObjectVersions.
S3:RequestObjectTag/<tag-key>	S3:PutObject S3:PutObjectTagging S3:PutObjectVersionTagging	Exigirá uma chave de tag específica e um valor quando a solicitação de objeto incluir marcação.

Especifique variáveis em uma política

Você pode usar variáveis em políticas para preencher informações de política quando elas estiverem disponíveis. Você pode usar variáveis de política no `Resource` elemento e em comparações de string no `Condition` elemento.

Neste exemplo, a variável `${aws:username}` faz parte do elemento recurso:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Neste exemplo, a variável `${aws:username}` faz parte do valor da condição no bloco condição:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variável	Descrição
`${aws:SourceIp}`	Usa a chave SourceIp como a variável fornecida.
`${aws:username}`	Usa a chave de nome de usuário como a variável fornecida.
`${s3:prefix}`	Usa a chave de prefixo específica do serviço como a variável fornecida.

Variável	Descrição
`${s3:max-keys}`	Usa a chave de teclas de Max específicas do serviço como a variável fornecida.
`${*}`	Caráter especial. Usa o caractere como um caractere * literal.
`${?}`	Caráter especial. Usa o caractere como um caractere literal ?.
`${$}`	Caráter especial. Usa o caractere como um caractere literal.

Crie políticas que exijam tratamento especial

Às vezes, uma diretiva pode conceder permissões que são perigosas para a segurança ou perigosas para operações contínuas, como bloquear o usuário raiz da conta. A implementação da API REST do StorageGRID S3 é menos restritiva durante a validação de políticas do que a Amazon, mas igualmente rigorosa durante a avaliação de políticas.

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento de StorageGRID
Negar a si mesmo quaisquer permissões para a conta raiz	Balde	Válida e aplicada, mas a conta de usuário root mantém permissão para todas as operações de política de bucket do S3	O mesmo
Negar auto quaisquer permissões ao usuário/grupo	Grupo	Válido e aplicado	O mesmo
Permita a um grupo de conta estrangeiro qualquer permissão	Balde	Principal inválido	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido quando permitido por uma política
Permitir uma conta estrangeira root ou usuário qualquer permissão	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido quando permitido por uma política	O mesmo

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento de StorageGRID
Permitir permissões a todos para todas as ações	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido para a raiz da conta estrangeira e usuários	O mesmo
Negar permissões a todos para todas as ações	Balde	Válida e aplicada, mas a conta de usuário root mantém permissão para todas as operações de política de bucket do S3	O mesmo
Principal é um usuário ou grupo inexistente	Balde	Principal inválido	Válido
Recurso é um bucket S3 inexistente	Grupo	Válido	O mesmo
Principal é um grupo local	Balde	Principal inválido	Válido
A política concede a uma conta que não seja proprietária (incluindo contas anônimas) permissões para colocar objetos.	Balde	Válido. Os objetos são propriedade da conta de criador e a política de bucket não se aplica. A conta de criador deve conceder permissões de acesso ao objeto usando ACLs de objeto.	Válido. Os objetos são propriedade da conta de proprietário do bucket. Aplica-se a política de bucket.

Proteção WORM (write-once-read-many)

Você pode criar buckets do WORM (write-once-read-many) para proteger dados, metadados de objetos definidos pelo usuário e marcação de objetos do S3. Você configura os buckets WORM para permitir a criação de novos objetos e impedir substituições ou exclusões de conteúdo existente. Use uma das abordagens descritas aqui.

Para garantir que as substituições sejam sempre negadas, você pode:

- No Gerenciador de Grade, vá para **CONFIGURATION** > **Security** > **Security settings** > **Network and Objects**, e marque a caixa de seleção **Prevent client modification**.
- Aplique as seguintes regras e políticas do S3:
  - Adicione uma operação PutOverwriteObject NEGAR à política S3.
  - Adicione uma operação DeleteObject NEGAR à política S3.
  - Adicione uma operação PutObject PERMITIR à política S3.

A configuração DeleteObject para NEGAR em uma diretiva S3 não impede que o ILM exclua objetos quando uma regra como "zero cópias após 30 dias" existir.

Mesmo quando todas essas regras e políticas são aplicadas, elas não se protegem contra gravações simultâneas (ver situação A). Eles protegem contra substituições concluídas sequenciais (ver situação B).

Situação A: Gravações simultâneas (não protegidas contra)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situação B: Substituições sequenciais concluídas (protegidas contra)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informações relacionadas

- "Como as regras do StorageGRID ILM gerenciam objetos"
- "Exemplo de políticas de bucket"
- "Exemplo de políticas de grupo"
- "Gerenciar objetos com ILM"
- "Use uma conta de locatário"

Exemplo de políticas de bucket

Use os exemplos nesta seção para criar políticas de acesso ao StorageGRID para buckets.

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a diretiva está anexada. Você configura uma política de bucket usando a API S3 PutBucketPolicy por meio de uma destas ferramentas:

- "Gerente do locatário".
- AWS CLI usando este comando (consulte a "Operações em baldes"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemplo: Permita que todos acessem somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, podem listar objetos no bucket e executar operações GetObject em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que essa política pode não ser particularmente útil porque ninguém, exceto a raiz da conta, tem permissões para gravar no bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Exemplo: Permita que todos em uma conta tenham acesso total, e todos em outra conta tenham acesso somente leitura a um intervalo

Neste exemplo, todos em uma conta especificada têm acesso total a um bucket, enquanto todos em outra conta especificada só podem listar o bucket e executar operações GetObject em objetos no bucket começando com o `shared/` prefixo da chave do objeto.

> No StorageGRID, os objetos criados por uma conta não proprietária (incluindo contas anônimas) são de propriedade da conta de proprietário do bucket. A política de bucket aplica-se a esses objetos.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Exemplo: Permita que todos acessem somente leitura a um bucket e o acesso total por grupo especificado

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar operações GetObject em todos os objetos no bucket, enquanto somente usuários pertencentes ao grupo `Marketing` na conta especificada têm acesso total permitido.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemplo: Permita que todos leiam e gravem o acesso a um bucket se o cliente estiver no intervalo IP

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar quaisquer operações de Objeto em todos os objetos no bucket, desde que as solicitações venham de um intervalo IP especificado (54.240.143.0 a 54.240.143.255, exceto 54.240.143.188). Todas as outras operações serão negadas e todas as solicitações fora do intervalo de IP serão negadas.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Exemplo: Permitir acesso total a um bucket exclusivamente por um usuário federado especificado

Neste exemplo, o usuário federado Alex tem acesso total ao `examplebucket` bucket e seus objetos. Todos os outros usuários, incluindo "root", são explicitamente negados todas as operações. Note no entanto que "root" nunca é negada permissão para colocar/obter/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemplo: Permissão PutOverwriteObject

Neste exemplo, o `Deny` efeito para PutOverwriteObject e DeleteObject garante que ninguém pode substituir ou excluir os dados do objeto, metadados definidos pelo usuário e marcação de objetos S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Exemplo de políticas de grupo

Use os exemplos nesta seção para criar políticas de acesso ao StorageGRID para grupos.

As políticas de grupo especificam as permissões de acesso para o grupo ao qual a diretiva está anexada. Não `Principal` há nenhum elemento na política porque ela está implícita. As políticas de grupo são configuradas usando o Gerenciador de inquilinos ou a API.

Exemplo: Defina a política de grupo usando o Gerenciador do locatário

Quando você adiciona ou edita um grupo no Gerenciador do locatário, você pode selecionar uma política de grupo para determinar quais permissões de acesso do S3 os membros deste grupo terão. "Crie grupos para um locatário do S3"Consulte .

- **No S3 Access**: Opção padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
- **Acesso somente leitura**: Os usuários deste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
- **Acesso total**: Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
- **Mitigação de ransomware**: Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários deste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que têm o controle de versão de objeto habilitado.

  Os usuários do Gerenciador de locatários que têm a permissão Gerenciar todos os buckets podem substituir essa política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação multifator (MFA), onde disponível.

- **Custom**: Os usuários do grupo recebem as permissões que você especificar na caixa de texto.

Exemplo: Permitir o acesso total do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso total a todos os buckets pertencentes à conta de locatário, a menos que explicitamente negado pela política de bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: Permitir acesso somente leitura de grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso somente leitura a recursos do S3, a menos que explicitamente negado pela política de bucket. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: Permita que os membros do grupo tenham acesso total apenas à sua "pasta" em um intervalo

Neste exemplo, os membros do grupo só podem listar e acessar sua pasta específica (prefixo de chave) no intervalo especificado. Observe que as permissões de acesso de outras políticas de grupo e a política de bucket devem ser consideradas ao determinar a privacidade dessas pastas.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

S3 operações rastreadas nos logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. Você pode revisar as mensagens de auditoria específicas do S3 no log de auditoria para obter detalhes sobre operações de bucket e objetos.

Operações de bucket rastreadas nos logs de auditoria

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- Balde para a cabeça
- ListObjects
- ListObjectVersions
- COLOQUE a conformidade do balde
- PutBucketTagging
- PutBucketControle de versão

Operações de objeto rastreadas nos logs de auditoria

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- RestoreObject
- Selecionar Objeto
- UploadPart (quando uma regra ILM usa ingestão equilibrada ou rigorosa)
- UploadPartCopy (quando uma regra ILM usa ingestão equilibrada ou rigorosa)

Informações relacionadas

- "Acessar o arquivo de log de auditoria"
- "O cliente escreve mensagens de auditoria"
- "O cliente lê mensagens de auditoria"

Usar Swift REST API (fim de vida útil)

Use a API Swift REST

O suporte para a API Swift chegou ao fim da vida útil e será removido em uma versão futura.

Os detalhes do Swift foram removidos desta versão do site do doc. "StorageGRID 11,8: Use a API REST do Swift"Consulte .

Monitore e solucione problemas de um sistema StorageGRID

Monitore o sistema StorageGRID

Monitorar um sistema StorageGRID

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

Antes de começar

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

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

Sobre esta tarefa

Estas instruções descrevem como:

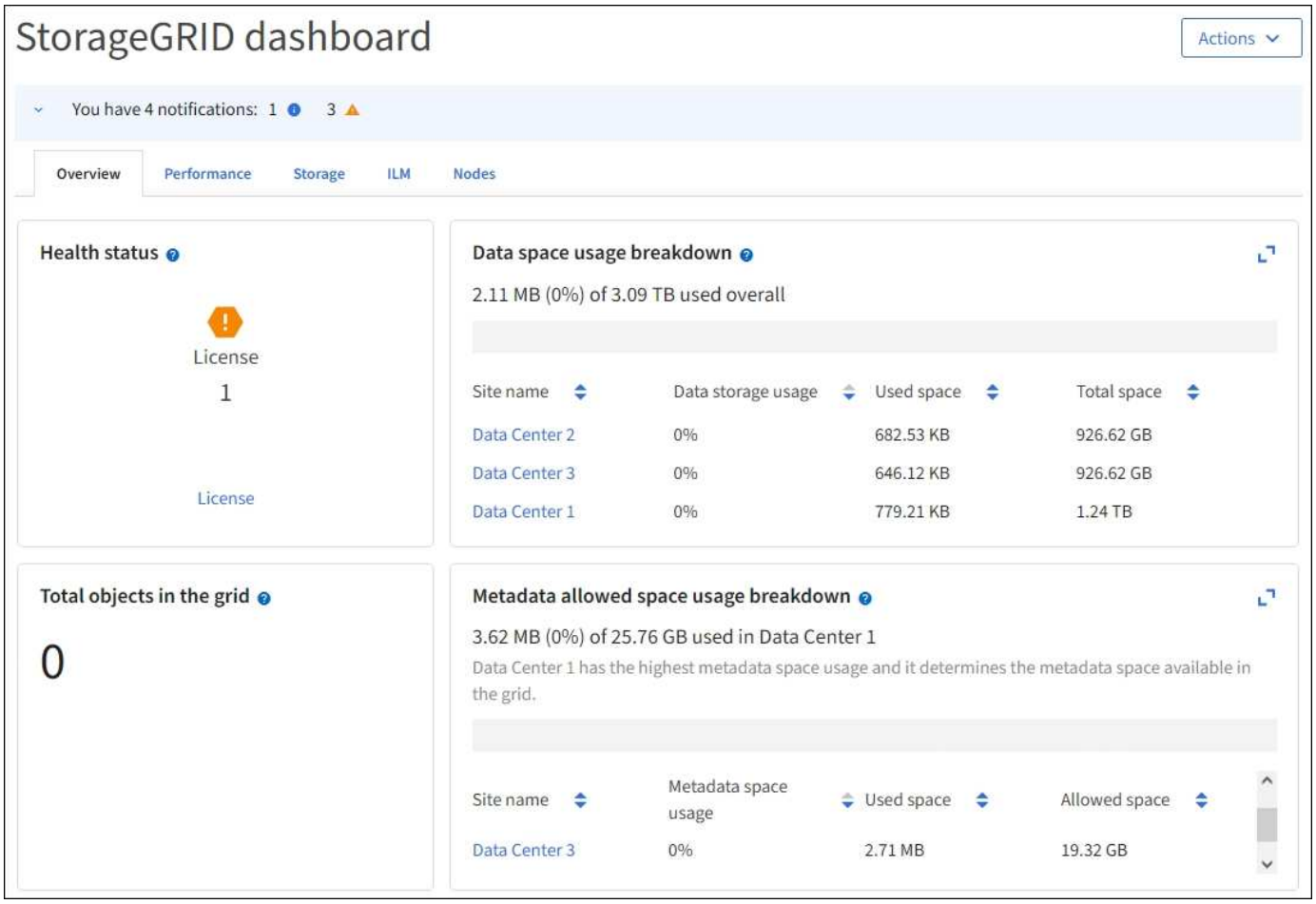
- "Visualizar e gerenciar o painel"
- "Exibir a página nós"
- "Monitorize estes aspetos do sistema regularmente:"
  - "Integridade do sistema"
  - "Capacidade de storage"
  - "Gerenciamento do ciclo de vida das informações"
  - "Recursos de rede e sistema"
  - "Atividade do locatário"
  - "Operações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

Visualizar e gerenciar o painel

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

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

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



Visualizar o painel de instrumentos

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

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

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

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

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

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

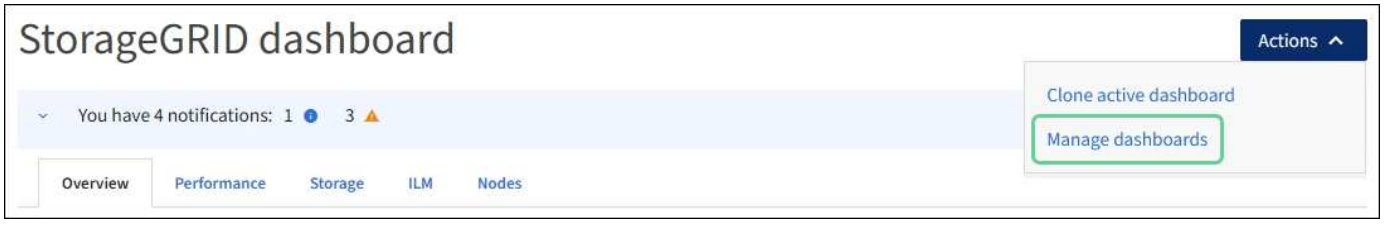
Gerenciar painéis

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

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

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

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



Configurar painéis

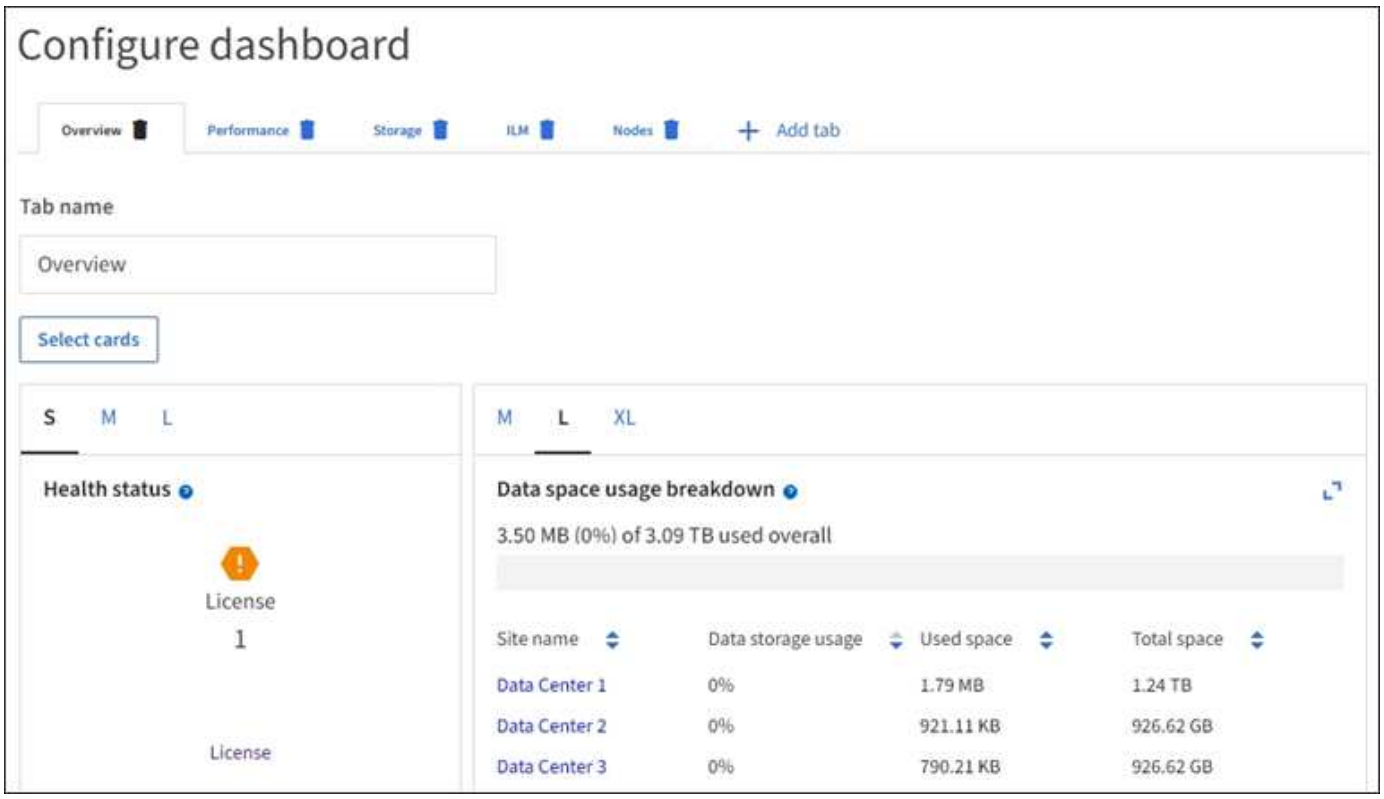
Para criar um novo painel clonando o painel ativo, selecione **ações** > **Clonar painel ativo**.

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

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

Ao configurar um dashboard, você pode:

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



Exibir a página nós

Exibir a página nós

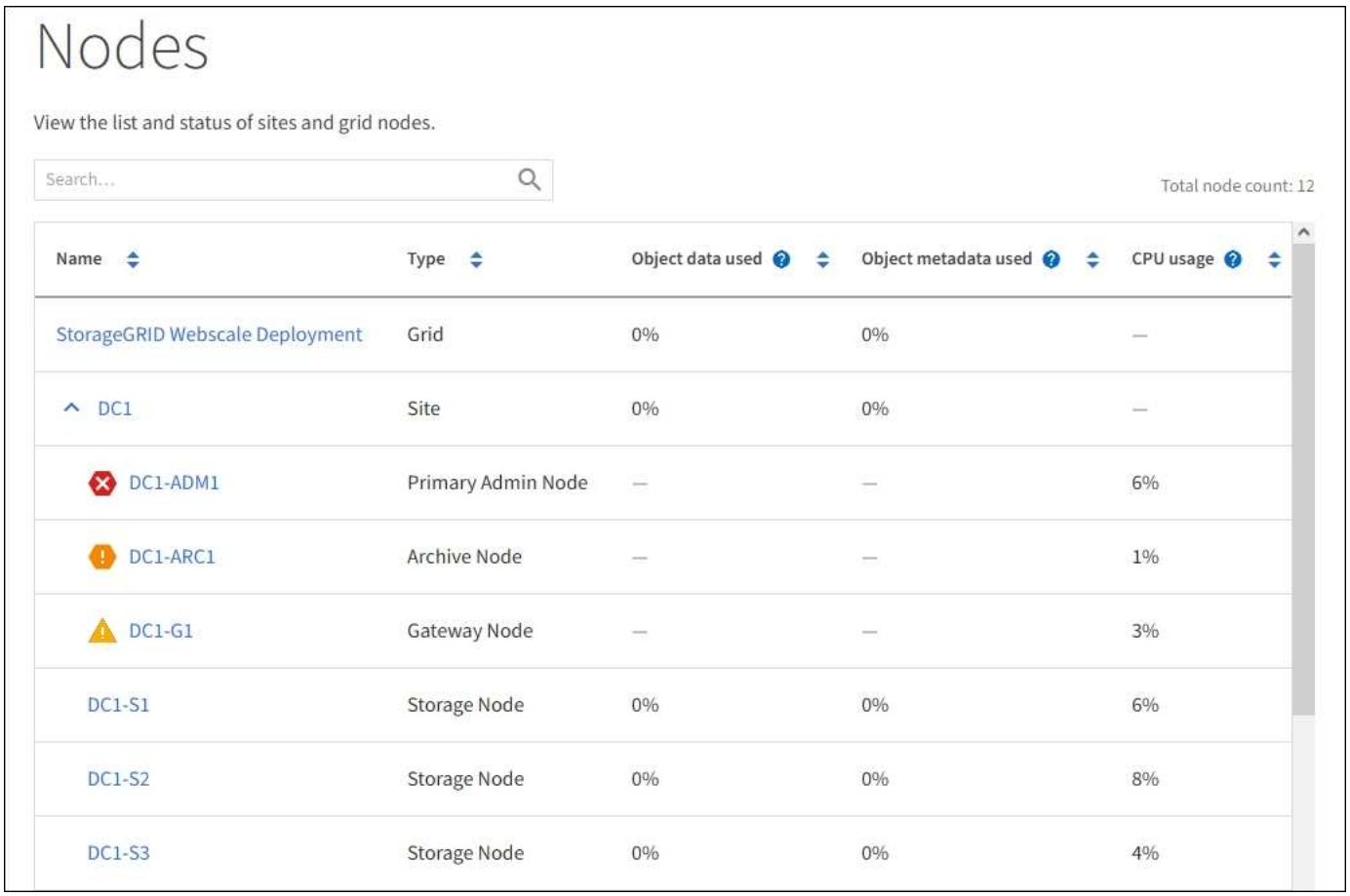
Quando você precisar de informações mais detalhadas sobre o seu sistema StorageGRID do que o painel fornece, você pode usar a página nós para exibir as métricas de toda a grade, cada local na grade e cada nó em um local.

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

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

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

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



Ícones de estado da ligação

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

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

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

Ícones de alerta

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

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

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

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

Exibir detalhes de um sistema, local ou nó

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

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

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

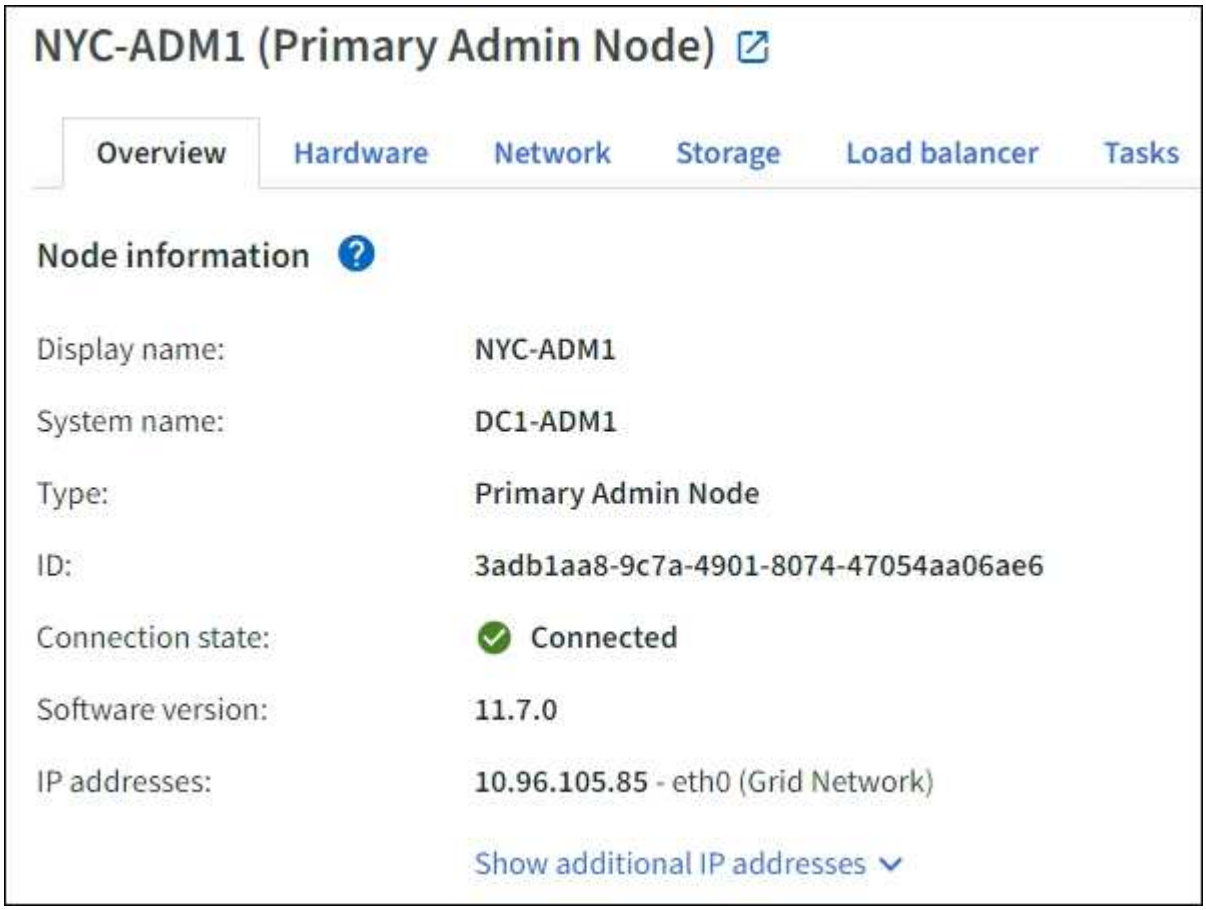
Veja a guia Visão geral

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

A guia Visão geral é mostrada para todos os nós.

Informações do nó

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



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

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

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

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

Alertas

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

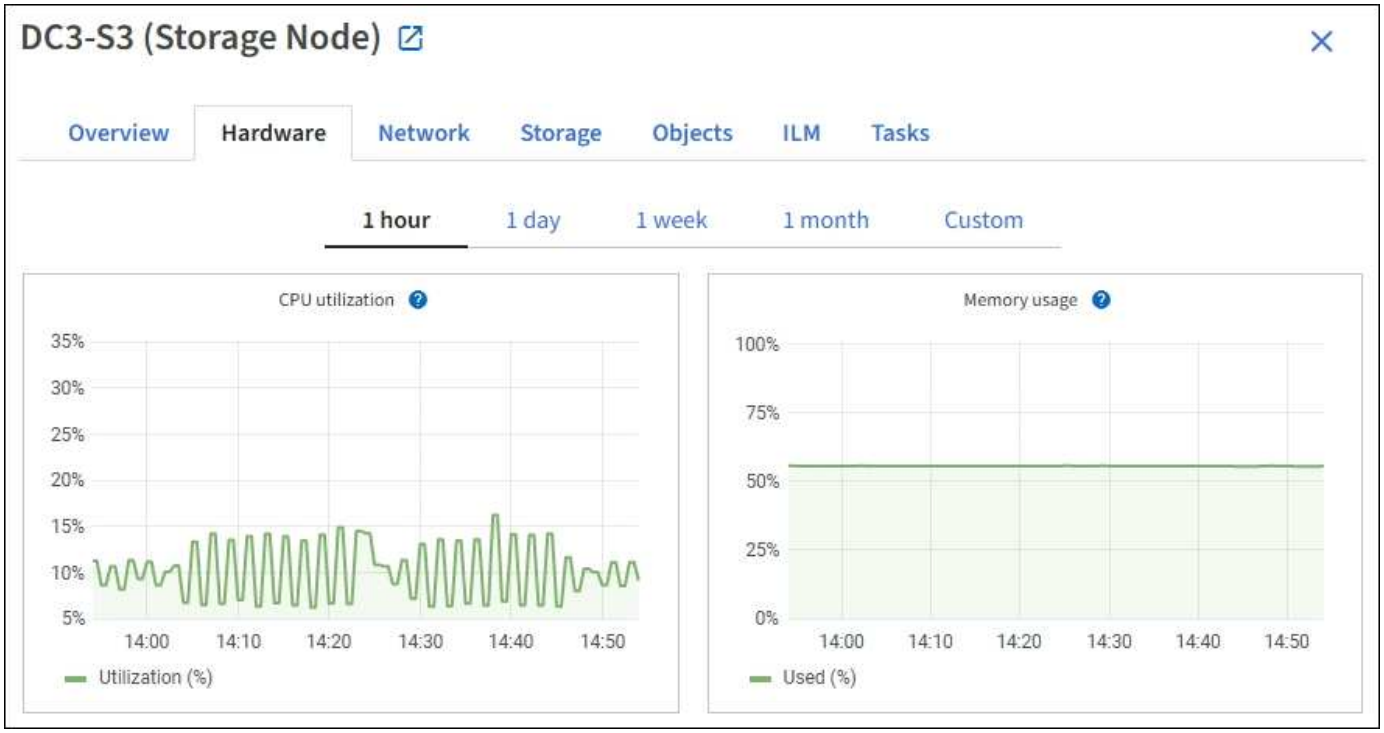
Os alertas também estão incluídos no "estados de conexão do nó".

Exibir a guia hardware

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

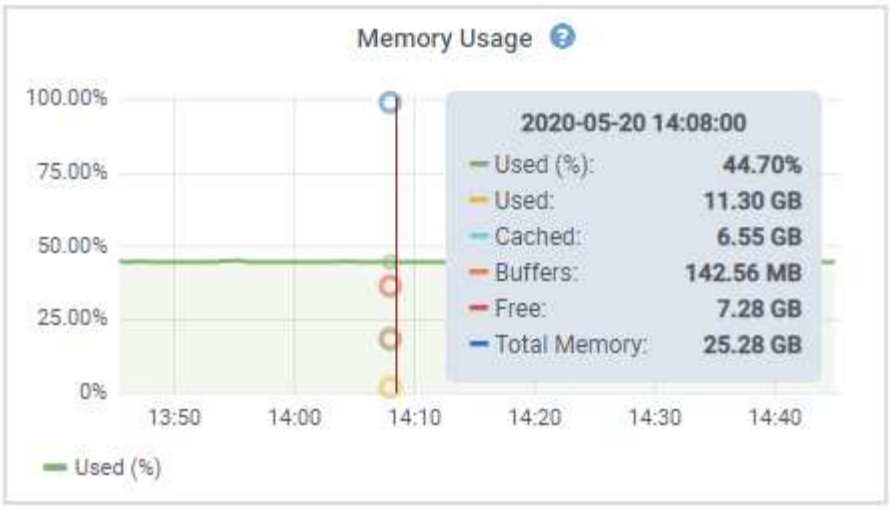
> O Gerenciador de Grade é atualizado com cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

A guia hardware é exibida para todos os nós.



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

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



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

Exibir informações sobre os nós de storage do dispositivo

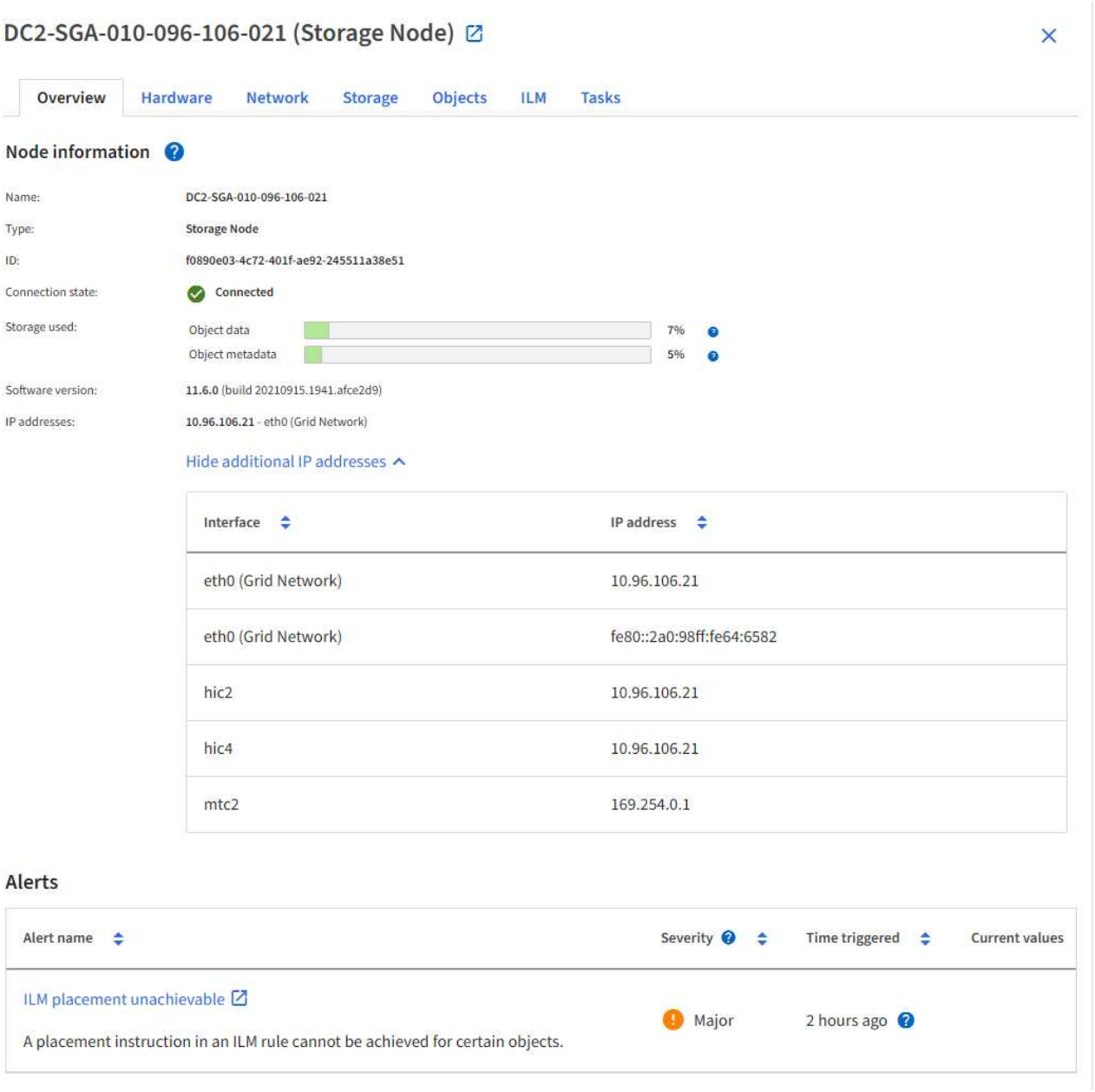
A página nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivo de disco e de rede para cada nó de storage do dispositivo. Você também pode ver memória, hardware de armazenamento, versão do firmware do controlador, recursos de rede, interfaces de rede,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

Passos

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

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

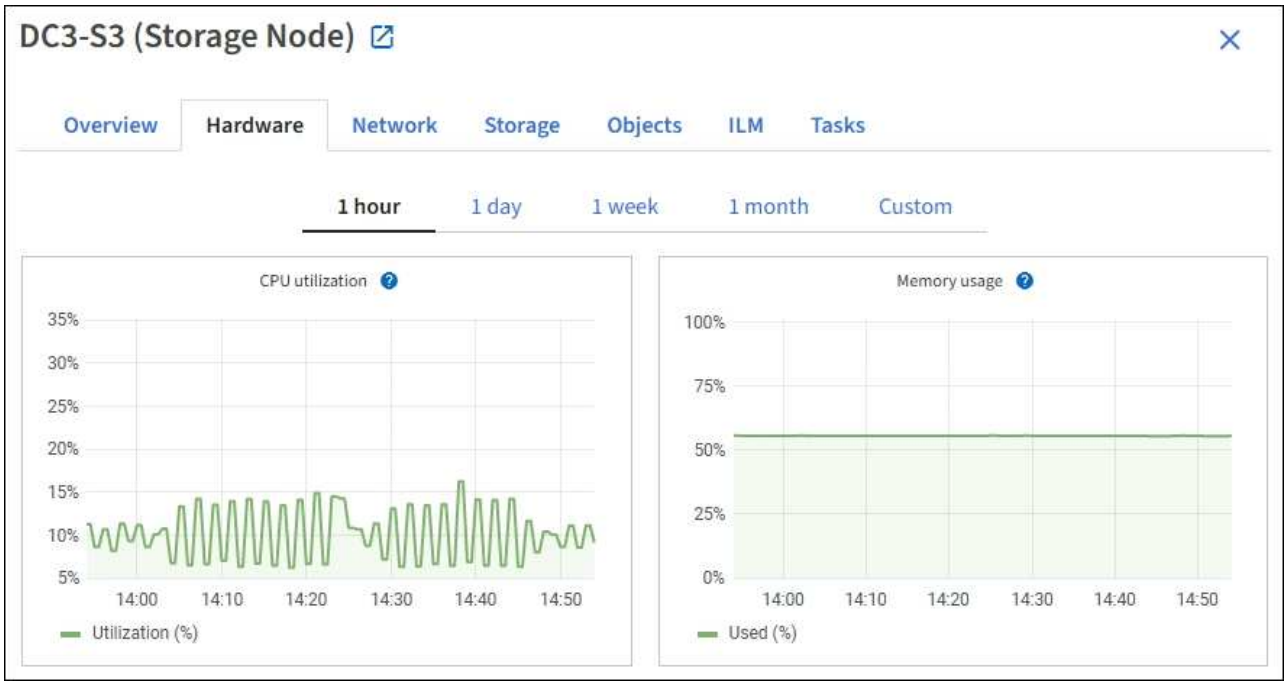
   - **eth**: Rede de Grade, rede Admin ou rede de cliente.
   - **Hic**: Uma das portas físicas de 10, 25 ou 100 GbE no dispositivo. Estas portas podem ser Unidas e ligadas à rede de grelha StorageGRID (eth0) e à rede de clientes (eth2).
   - **mtc**: Uma das portas físicas de 1 GbE no dispositivo. Uma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



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

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

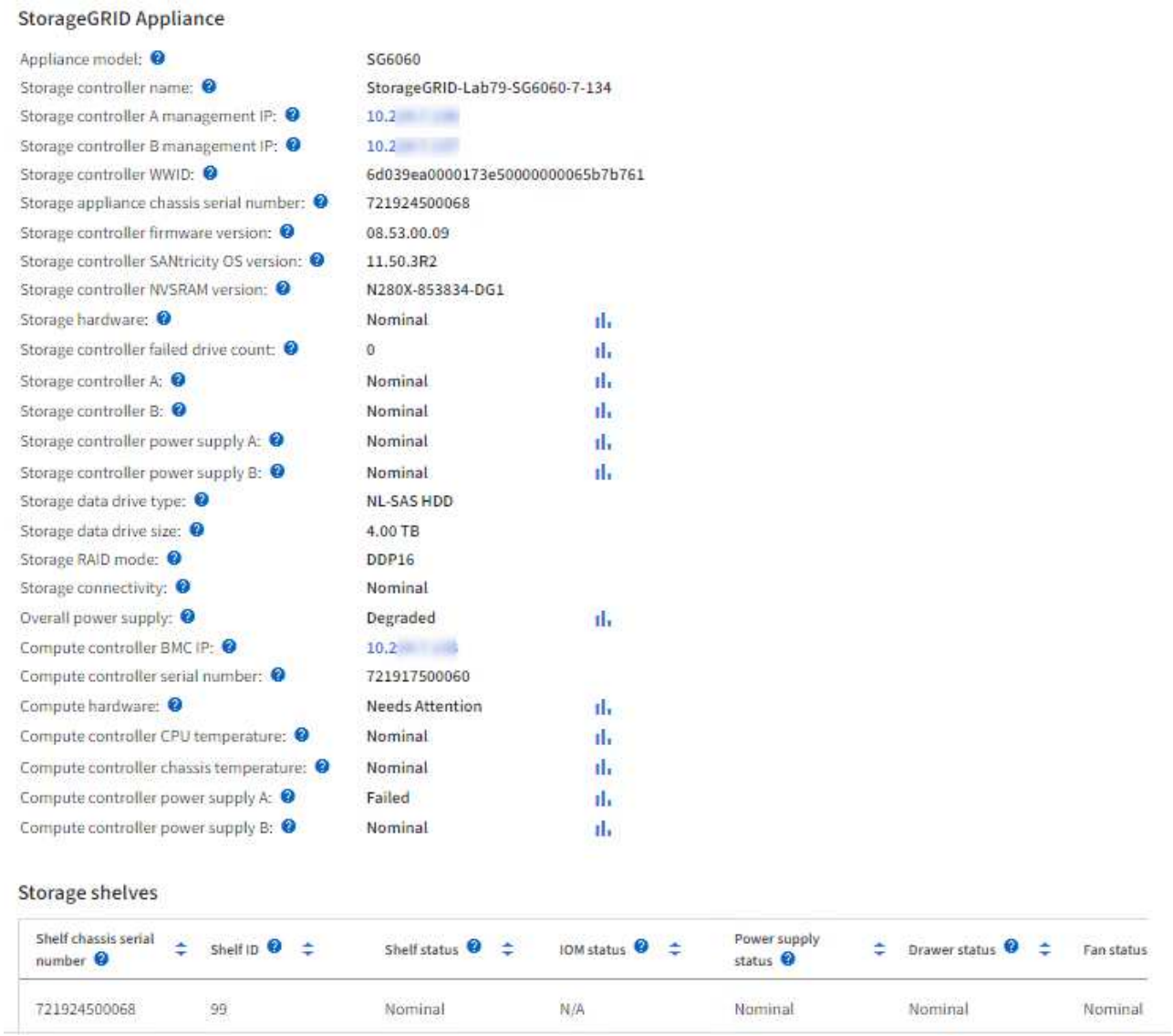
   a. Visualize os gráficos de utilização da CPU e memória para determinar as percentagens de utilização da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico ou gráfico. Você pode exibir as informações disponíveis para intervalos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



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

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

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



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

Campo na mesa do aparelho	Descrição
Controlador de armazenamento WWID	O identificador mundial do controlador de storage mostrado no SANtricity os.
Número de série do chassi do dispositivo de armazenamento	O número de série do chassis do aparelho.
Versão do firmware do controlador de armazenamento	A versão do firmware no controlador de armazenamento para este dispositivo.
Versão do controlador de storage SANtricity os	A versão do SANtricity os do controlador de armazenamento A..
Versão NVSRAM da controladora de storage	Versão NVSRAM da controladora de armazenamento conforme relatado pelo Gerenciador de sistema do SANtricity. Para o SG6060 e SG6160, se houver uma incompatibilidade de versão NVSRAM entre os dois controladores, a versão do controlador A será exibida. Se o controlador A não estiver instalado ou operacional, a versão do controlador B será exibida.
Hardware de storage	O status geral do hardware do controlador de storage. Se o Gerenciador de sistema do SANtricity relatar um status de precisa de atenção para o hardware de storage, o sistema StorageGRID também informará esse valor. Se o status for "precisa de atenção", primeiro verifique o controlador de armazenamento usando o SANtricity os. Em seguida, certifique-se de que não existem outros alertas que se apliquem ao controlador de computação.
Falha na contagem de unidades do controlador de armazenamento	O número de unidades que não são ideais.
Controlador de Storage A	O status do controlador de armazenamento A..
Controlador de armazenamento B	O status do controlador de armazenamento B. alguns modelos de aparelhos não têm um controlador de armazenamento B.
Fonte de Alimentação do controlador de armazenamento A	O estado da fonte de Alimentação A para o controlador de armazenamento.
Fonte de alimentação B do controlador de armazenamento	O estado da fonte de alimentação B para o controlador de armazenamento.
Tipo de unidade de dados de armazenamento	O tipo de unidades no dispositivo, como HDD (disco rígido) ou SSD (unidade de estado sólido).

Campo na mesa do aparelho	Descrição
Tamanho da unidade de dados de armazenamento	O tamanho efetivo de uma unidade de dados. Para o SG6160, o tamanho da unidade de cache também é exibido. **Nota**: Para nós com compartimentos de expansão, use o Tamanho da unidade de dados para cada gaveta em vez disso. O tamanho efetivo da unidade pode ser diferente por gaveta.
Modo RAID de armazenamento	O modo RAID configurado para o dispositivo.
Conectividade de storage	O estado de conetividade de storage.
Fonte de alimentação geral	O estado de todas as fontes de alimentação do aparelho.
Controlador de computação BMC IP	O endereço IP da porta do controlador de gerenciamento de placa base (BMC) no controlador de computação. Você usa esse IP para se conetar à interface do BMC para monitorar e diagnosticar o hardware do dispositivo. Este campo não é apresentado para modelos de aparelhos que não contêm um BMC.
Número de série do controlador de computação	O número de série do controlador de computação.
Hardware de computação	O status do hardware do controlador de computação. Esse campo não é exibido para modelos de dispositivo que não têm hardware de computação e hardware de armazenamento separados.
Temperatura da CPU do controlador de computação	O status da temperatura da CPU do controlador de computação.
Temperatura do chassi do controlador de computação	O status da temperatura do controlador de computação.

+

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

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

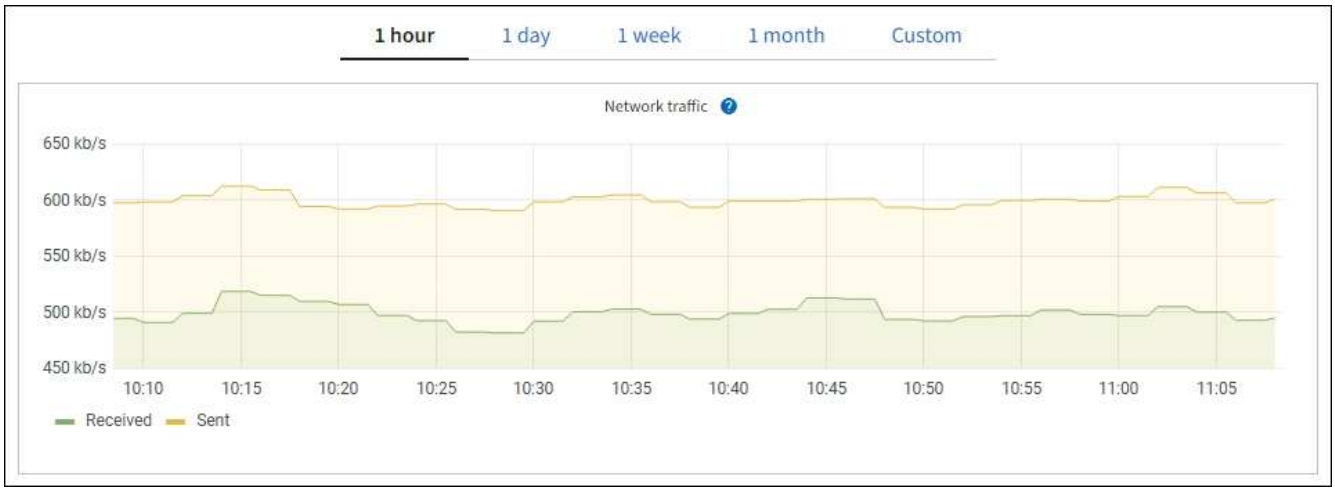
a. Confirmar se todos os Estados são "nominais".

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

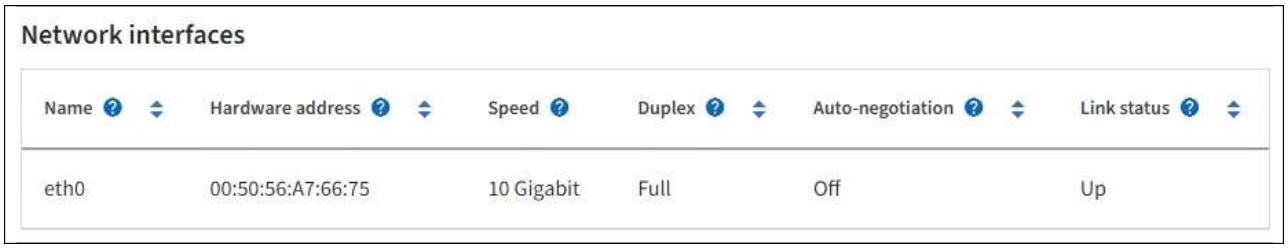
Gerenciador de sistema do SANtricity para saber mais sobre alguns desses valores de hardware. Consulte as instruções para instalar e manter o seu aparelho.

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

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



   a. Reveja a secção interfaces de rede.



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

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

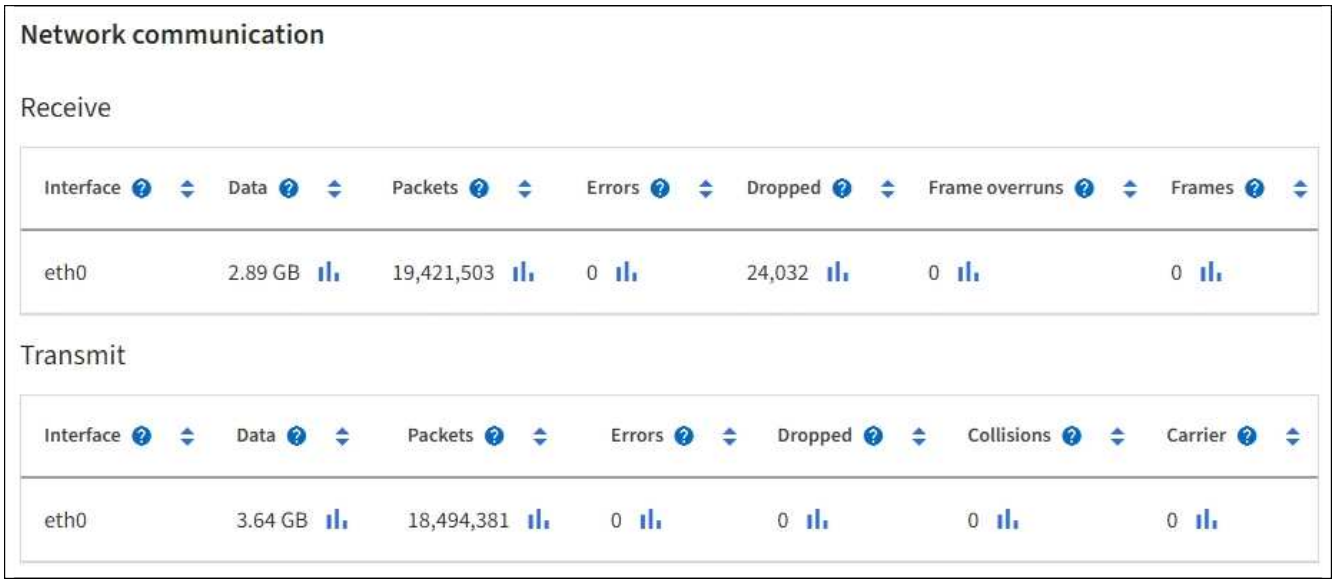
Modo de ligação	Modo Bond	Velocidade de ligação HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede do cliente/grade (eth0,eth2)
Agregado	LACP	25	100
Fixo	LACP	25	50
Fixo	Ativo/Backup	25	25
Agregado	LACP	10	40
Fixo	LACP	10	20

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

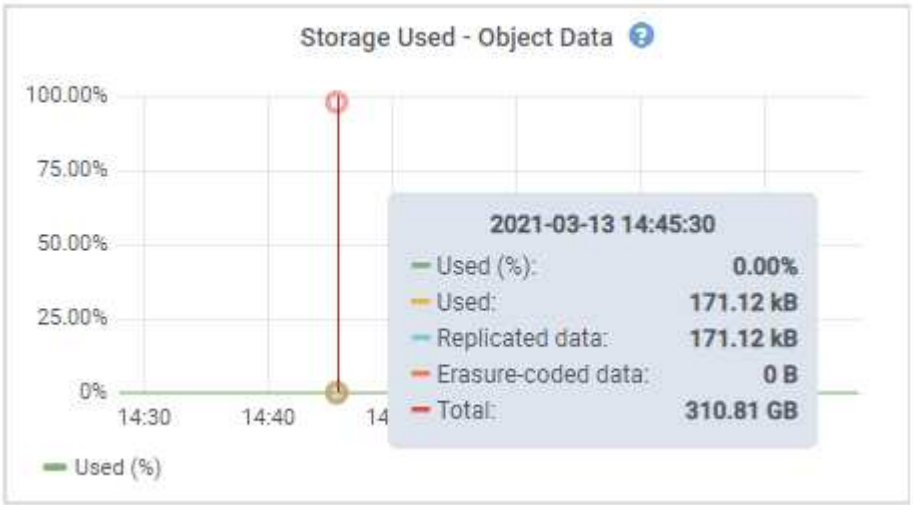
Consulte "Configurar ligações de rede" para obter mais informações sobre como configurar as portas 10/25-GbE.

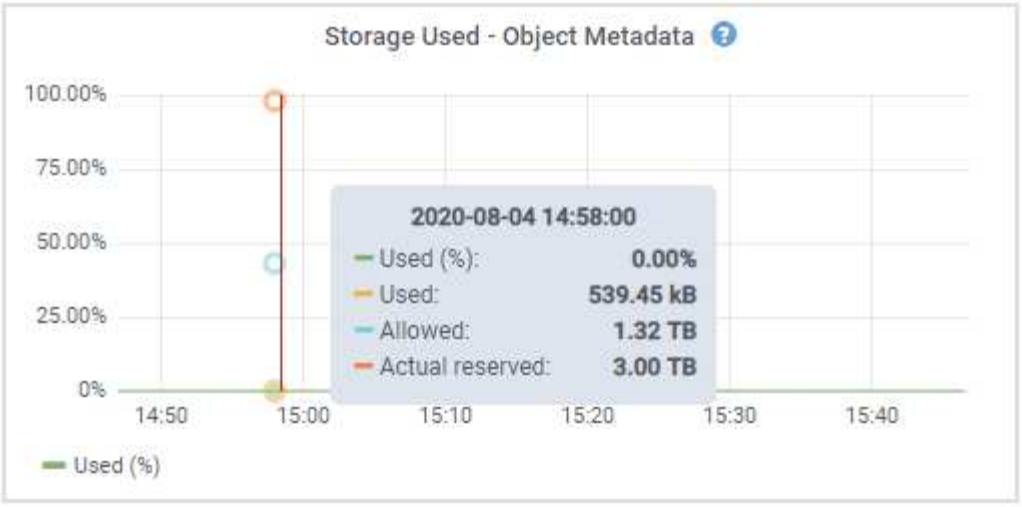
b. Reveja a secção Comunicação de rede.

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



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

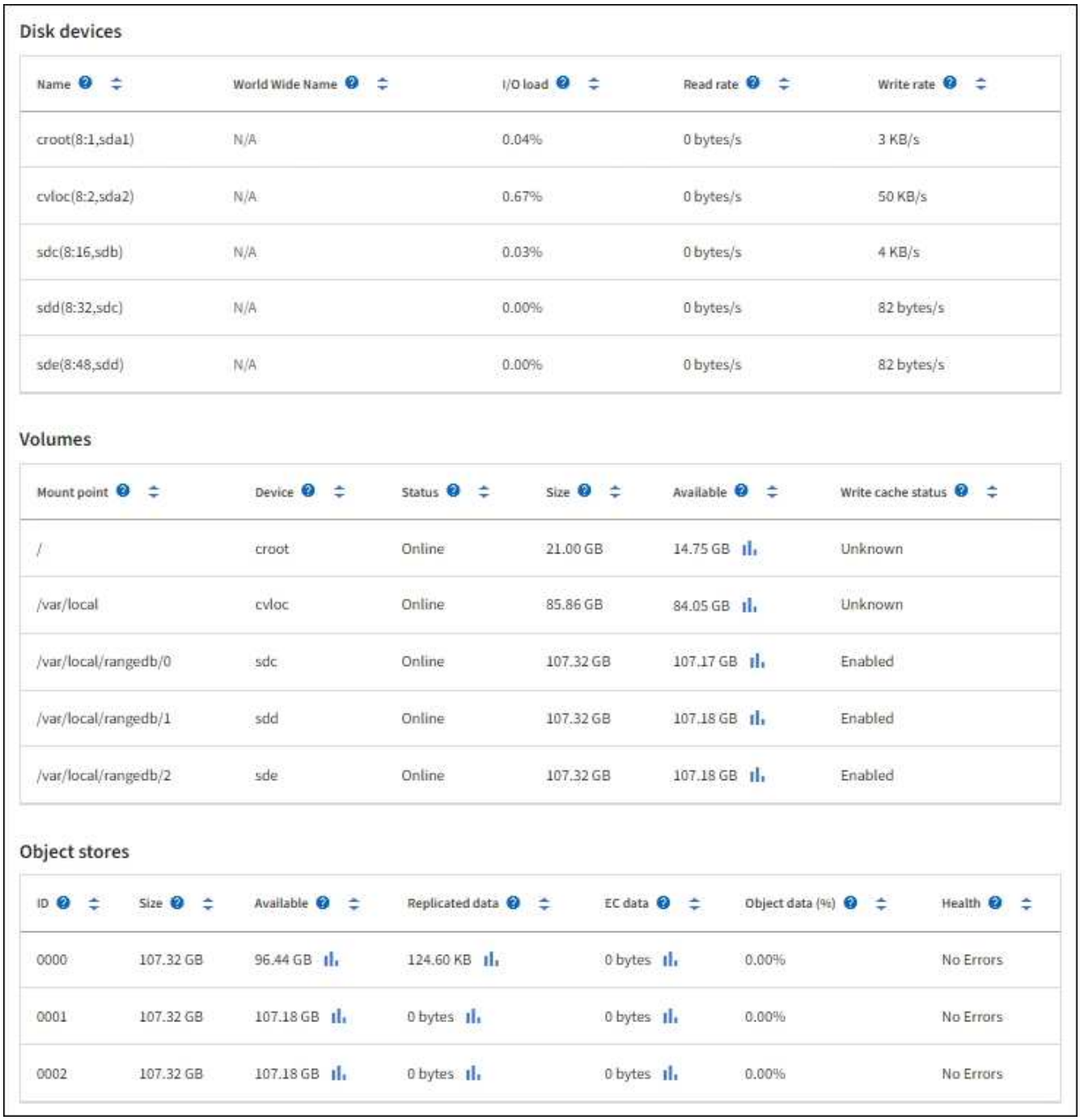




a. Role para baixo para ver as quantidades de armazenamento disponível para cada volume e armazenamento de objetos.

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

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



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

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

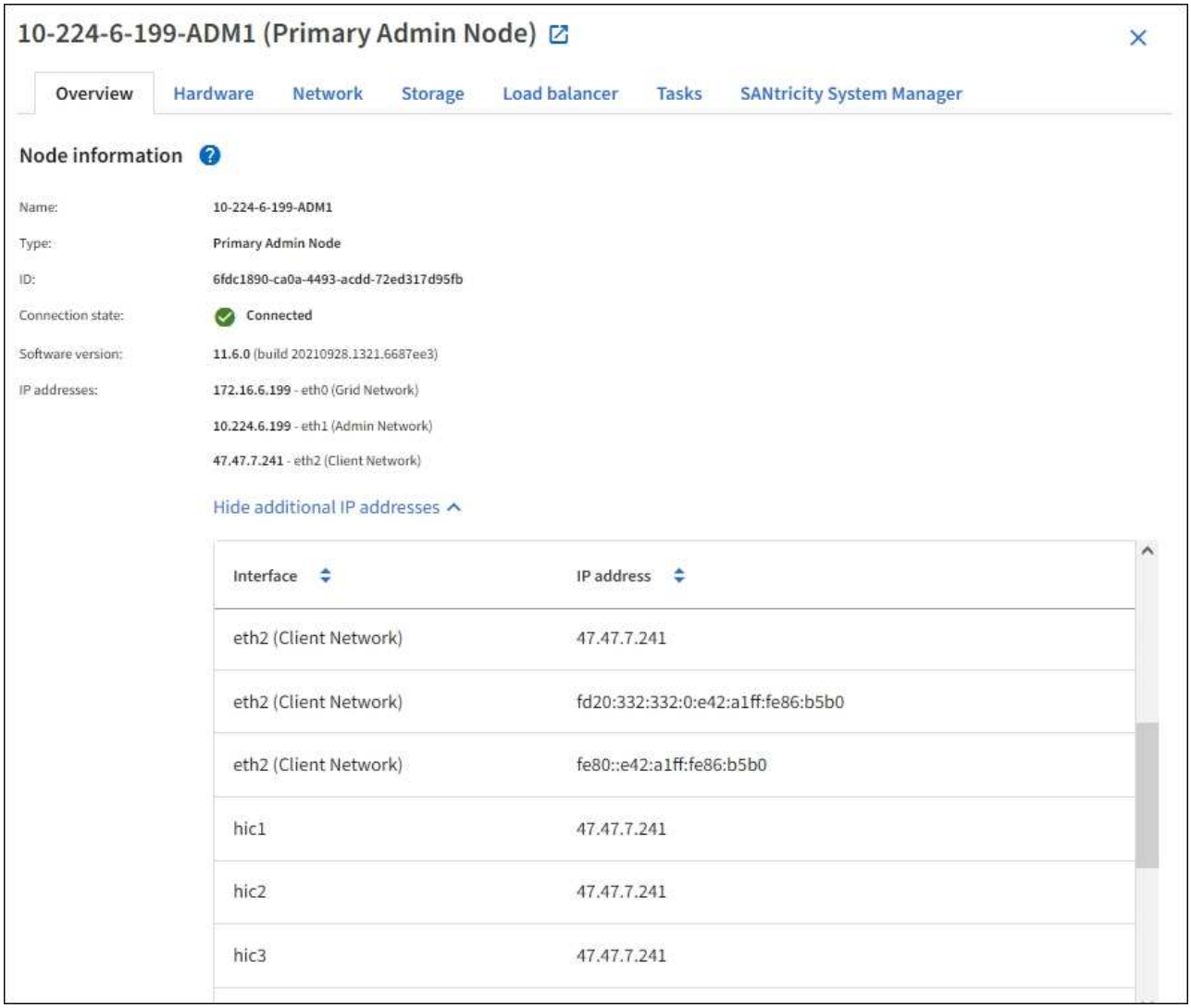
Passos

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

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

seguinte forma:

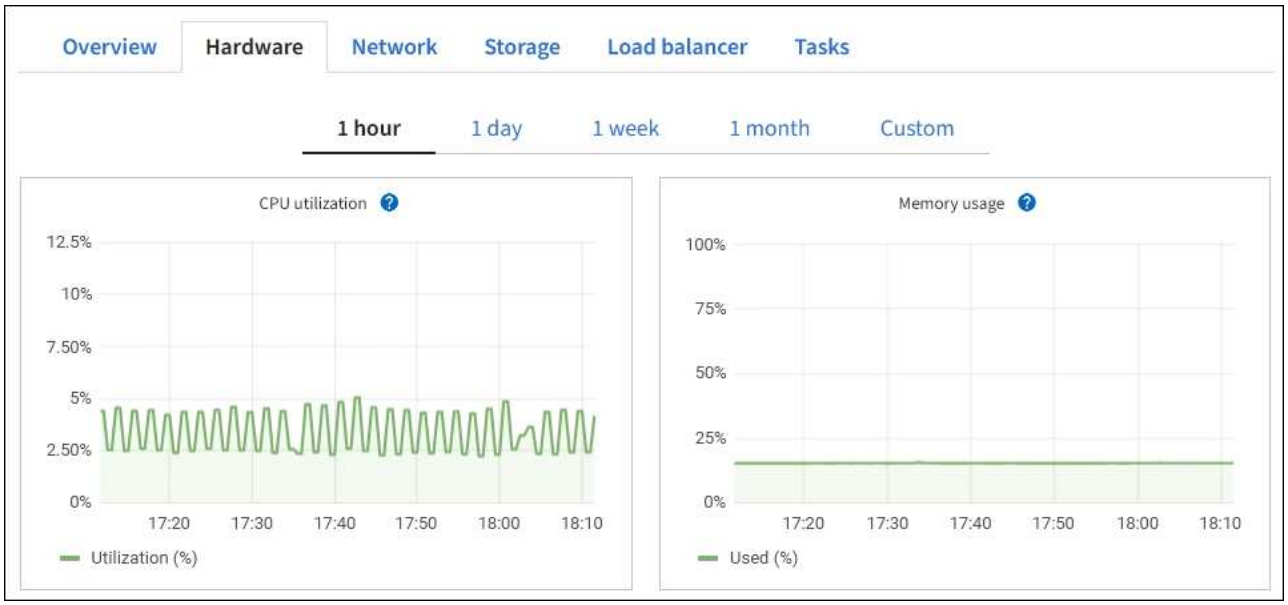
- **Adllb** e **adlli**: Mostrado se a ligação ativa/backup é usada para a interface Admin Network
- **eth**: Rede de Grade, rede Admin ou rede de cliente.
- **Hic**: Uma das portas físicas de 10, 25 ou 100 GbE no dispositivo. Estas portas podem ser Unidas e ligadas à rede de grelha StorageGRID (eth0)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



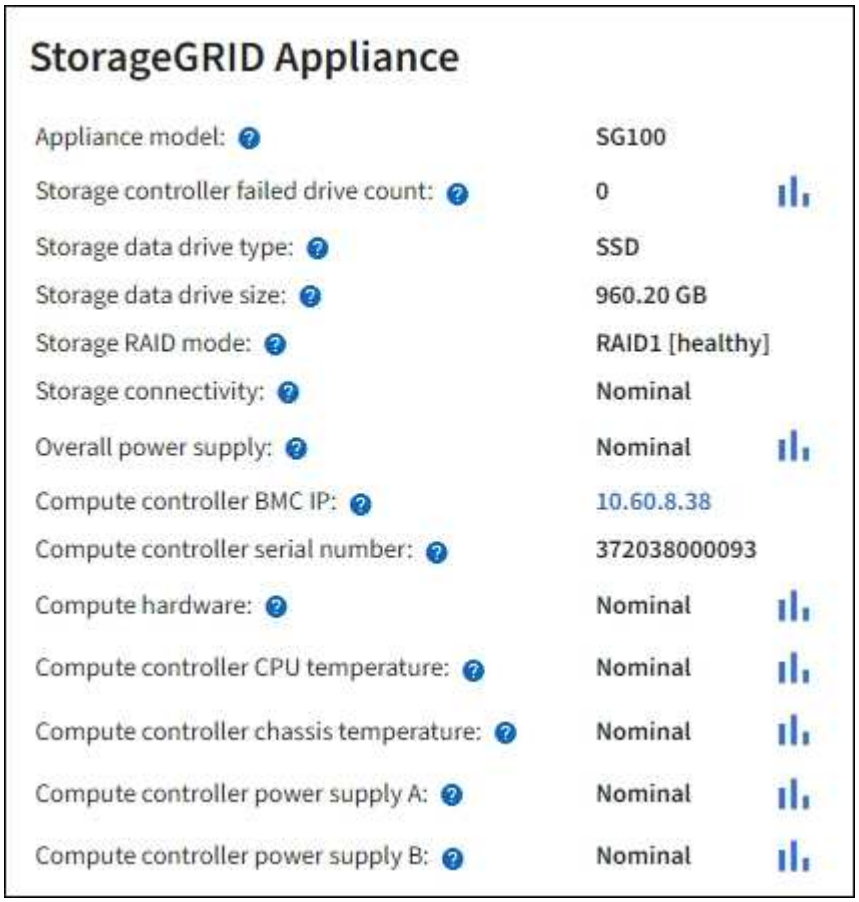
A seção Alertas da guia Visão geral exibe quaisquer alertas ativos para o nó.

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

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



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



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

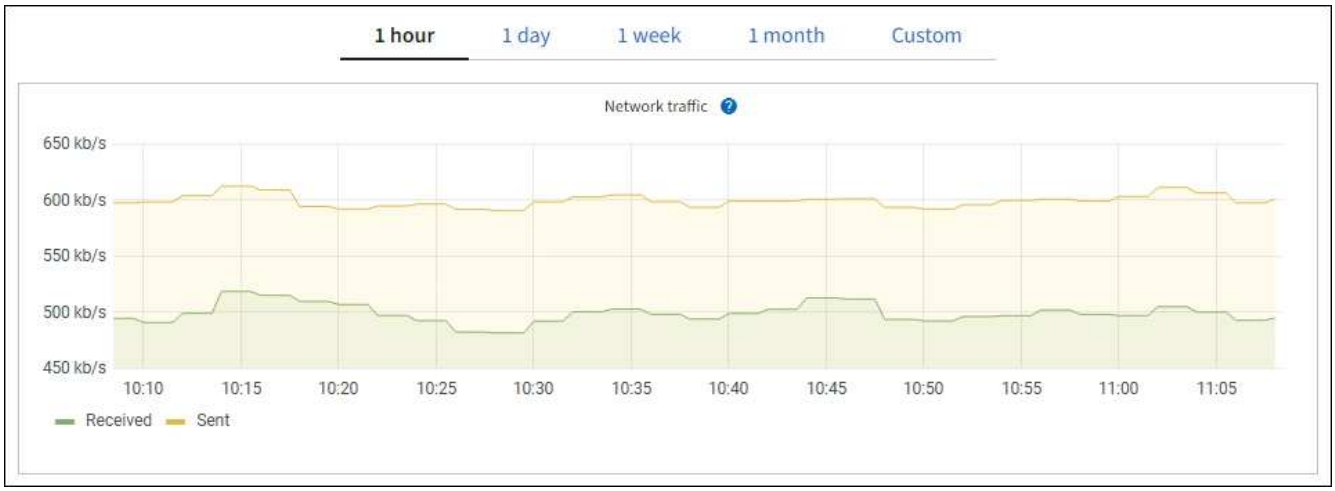
Campo na mesa do aparelho	Descrição
Falha na contagem de unidades do controlador de armazenamento	O número de unidades que não são ideais.
Tipo de unidade de dados de armazenamento	O tipo de unidades no dispositivo, como HDD (disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de dados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

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

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

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

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



a. Reveja a secção interfaces de rede.

Network interfaces

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

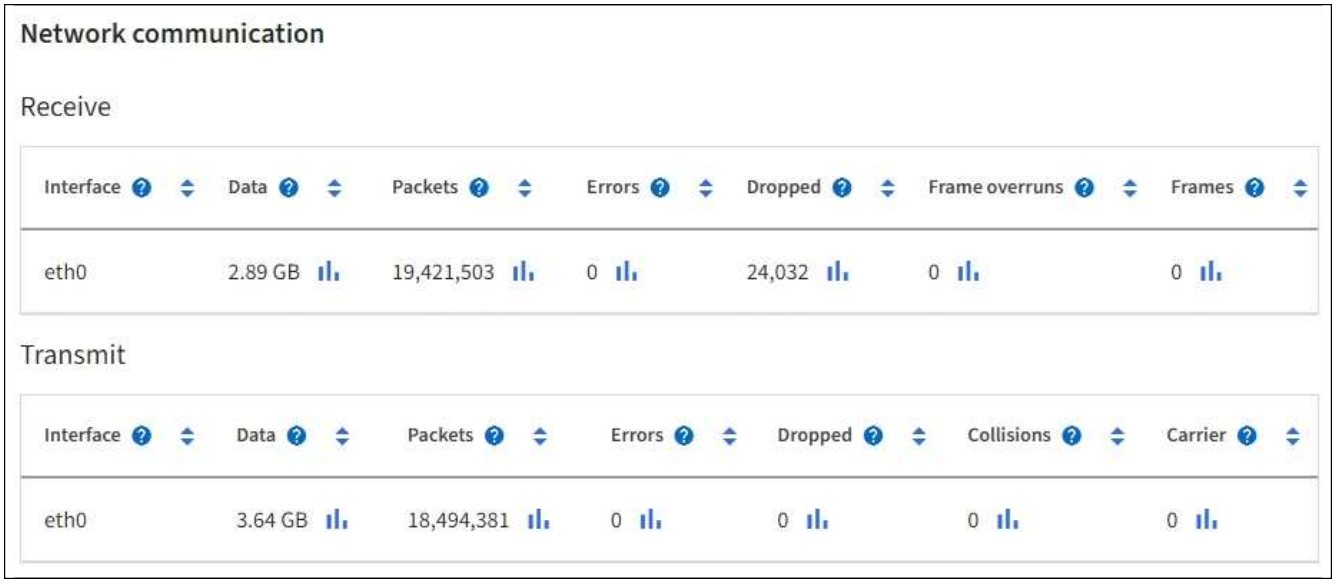
Use a tabela a seguir com os valores na coluna **velocidade** na tabela interfaces de rede para determinar se as quatro portas de rede 40/100-GbE no dispositivo foram configuradas para usar o modo ativo/backup ou o modo LACP.

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

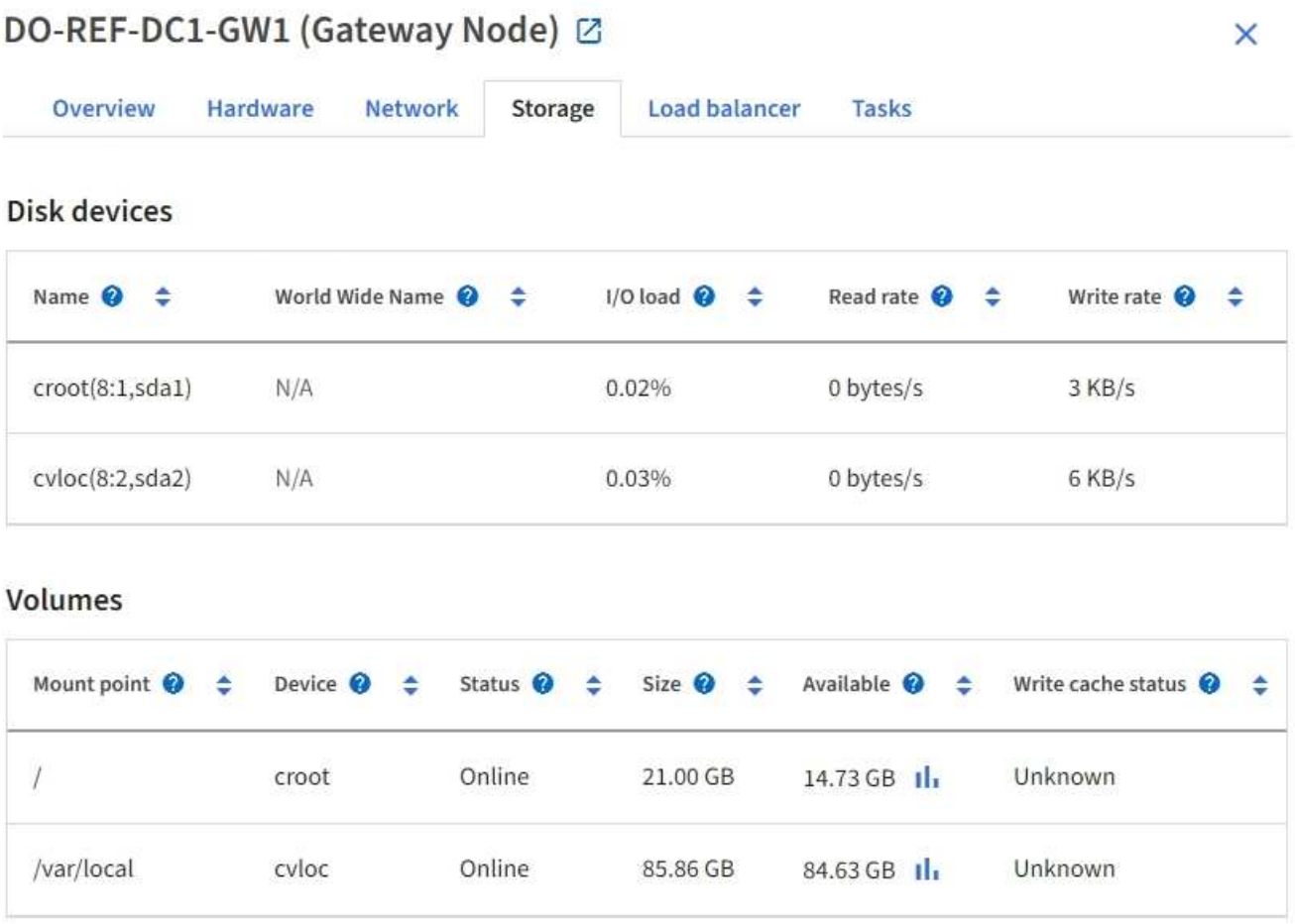
Modo de ligação	Modo Bond	Velocidade de ligação HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede do cliente/grade (eth0, eth2)
Agregado	LACP	100	400
Fixo	LACP	100	200
Fixo	Ativo/Backup	100	100
Agregado	LACP	40	160
Fixo	LACP	40	80
Fixo	Ativo/Backup	40	40

b. Reveja a secção Comunicação de rede.

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



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



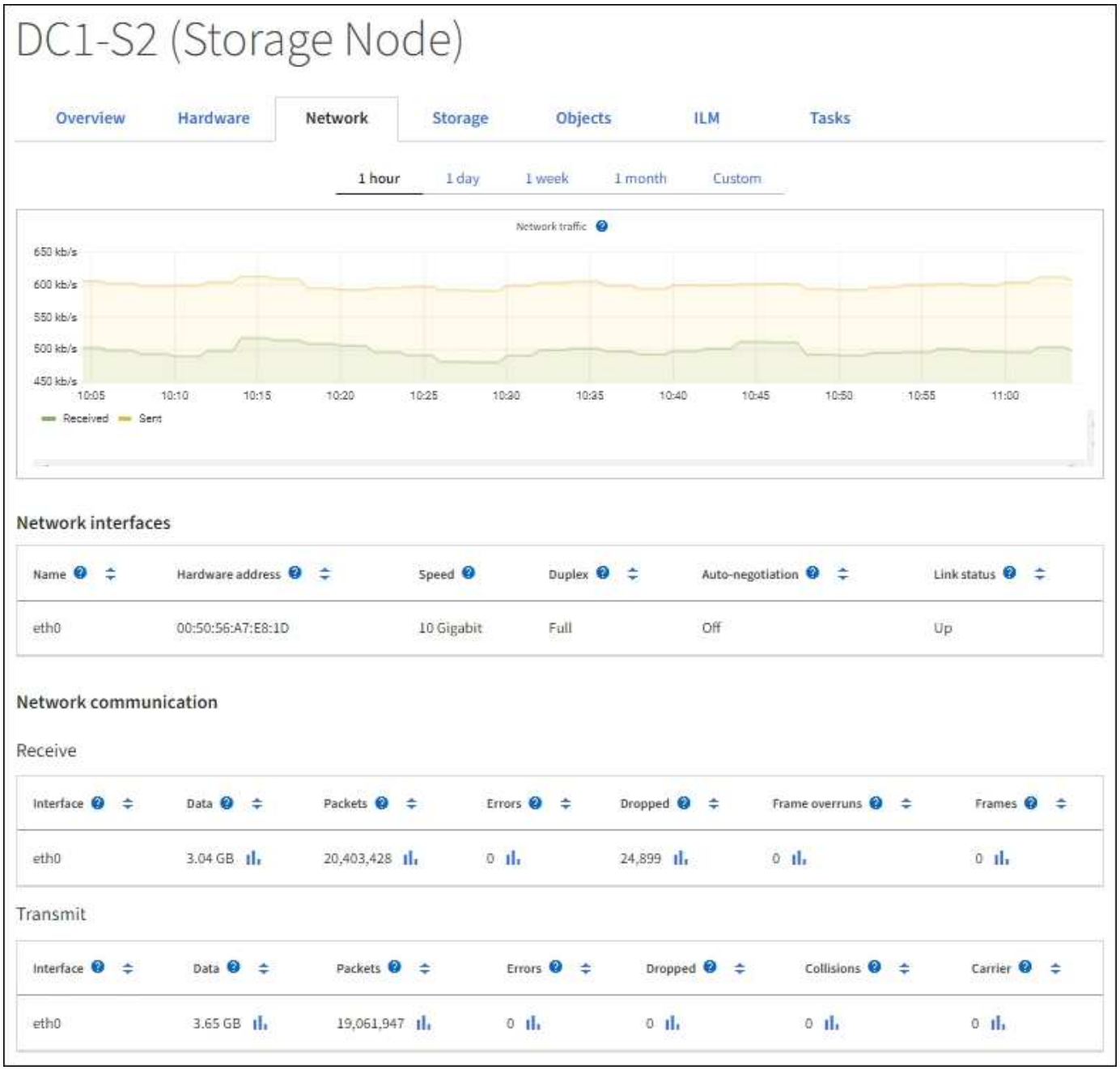
Veja a guia rede

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

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

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

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



Informações relacionadas

"Monitorar conexões de rede e desempenho"

Exibir a guia armazenamento

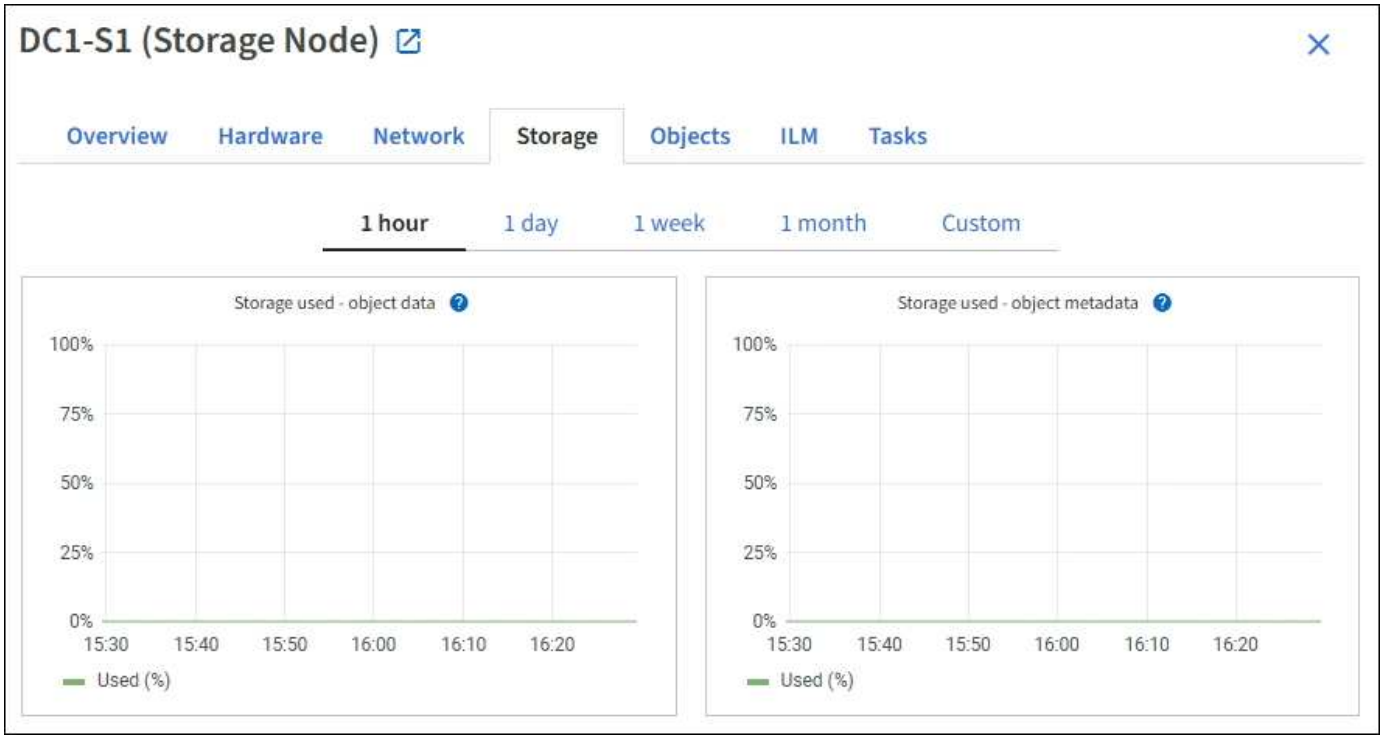
A guia armazenamento resume a disponibilidade de armazenamento e outras métricas de armazenamento.

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

Armazenamento de gráficos usados

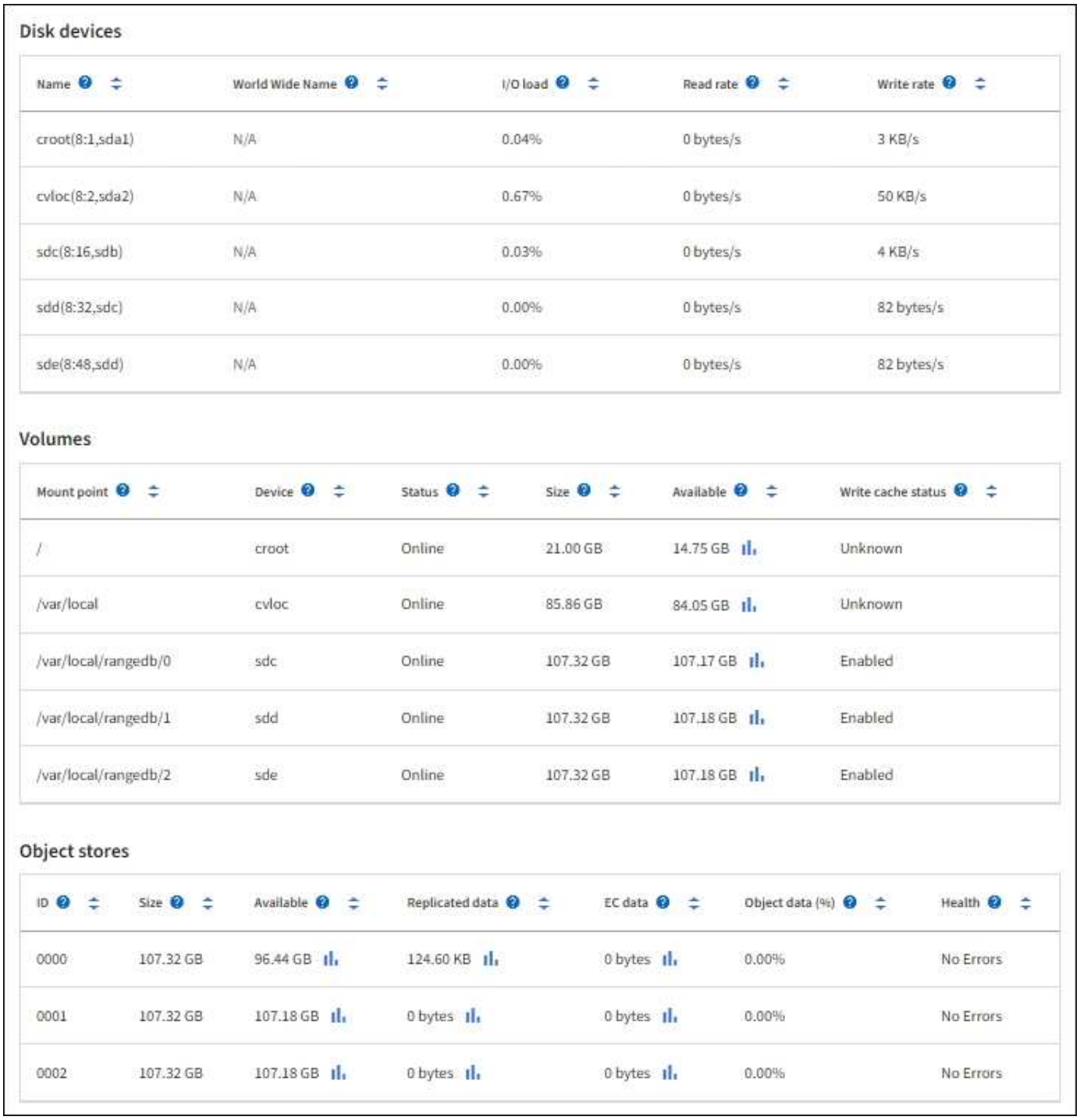
Para nós de storage, cada local e toda a grade, a guia Storage inclui gráficos mostrando quanto de storage foi usado pelos dados de objeto e metadados de objeto ao longo do tempo.

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



Dispositivos de disco, volumes e objetos armazenam tabelas

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



Disk devices

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

Volumes

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

Object stores

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

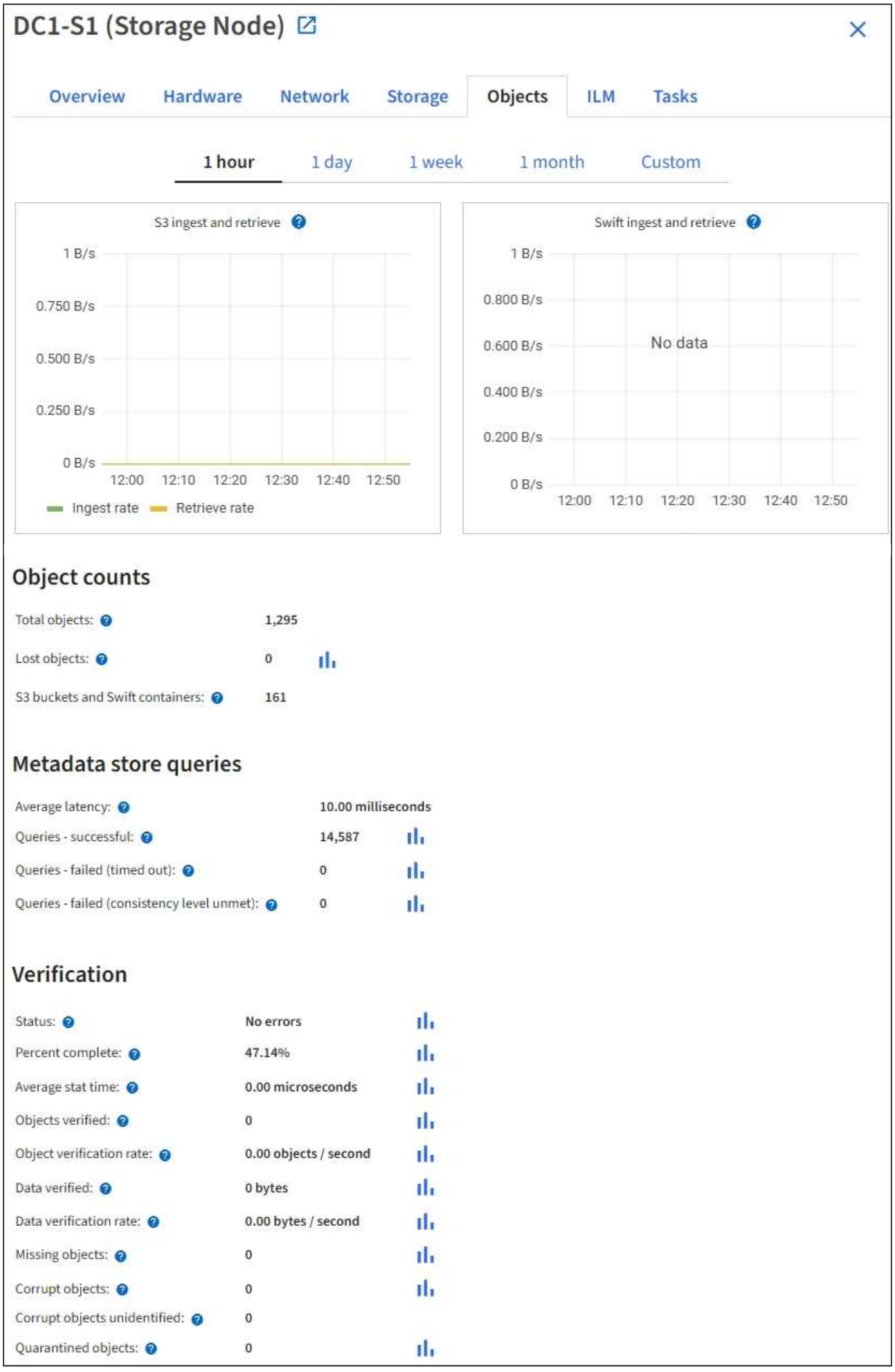
Informações relacionadas

"Monitorar a capacidade de armazenamento"

Exibir a guia objetos

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

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

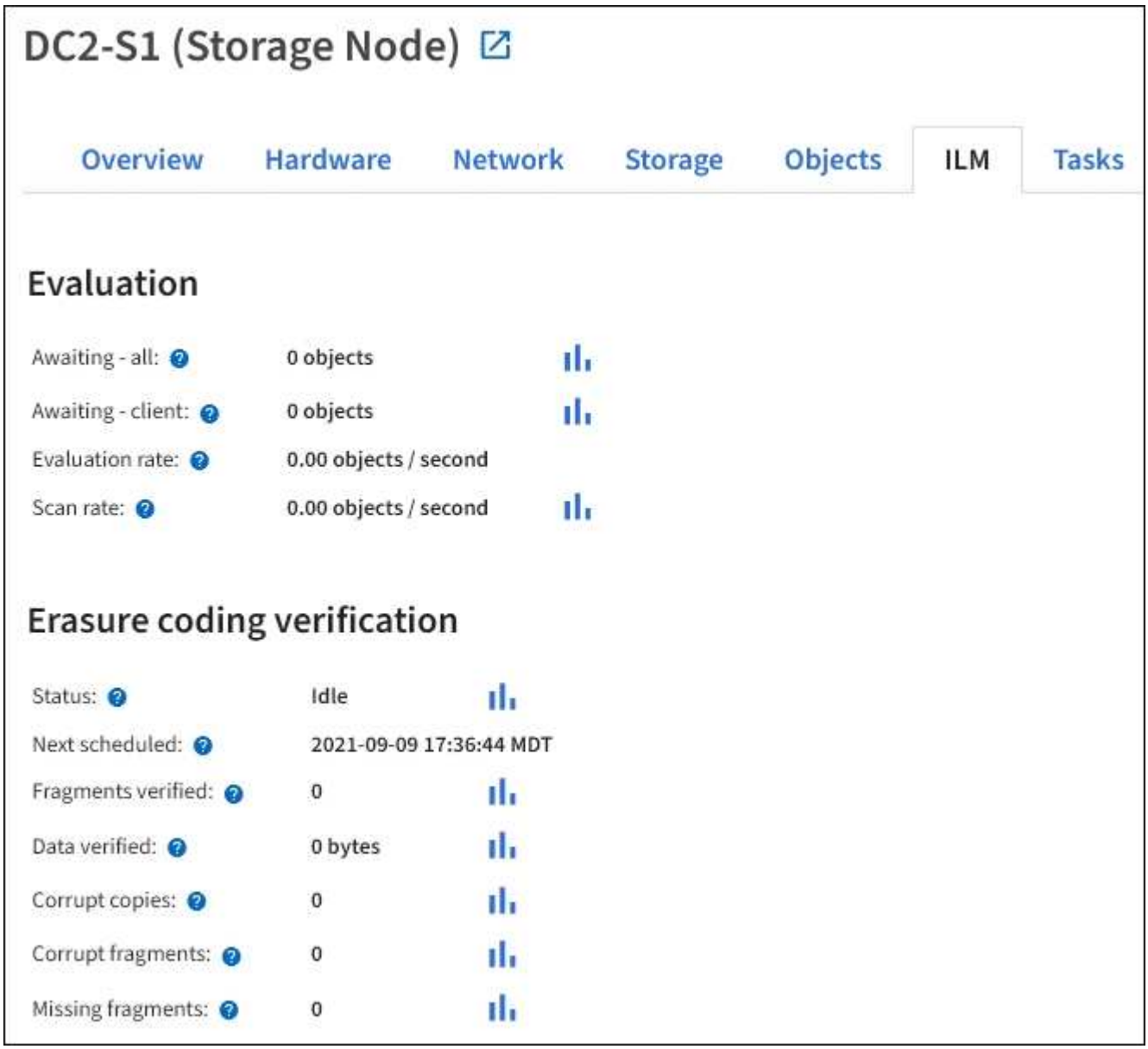

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

Veja a guia ILM

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

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

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



Informações relacionadas

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

Use a guia tarefas

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

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

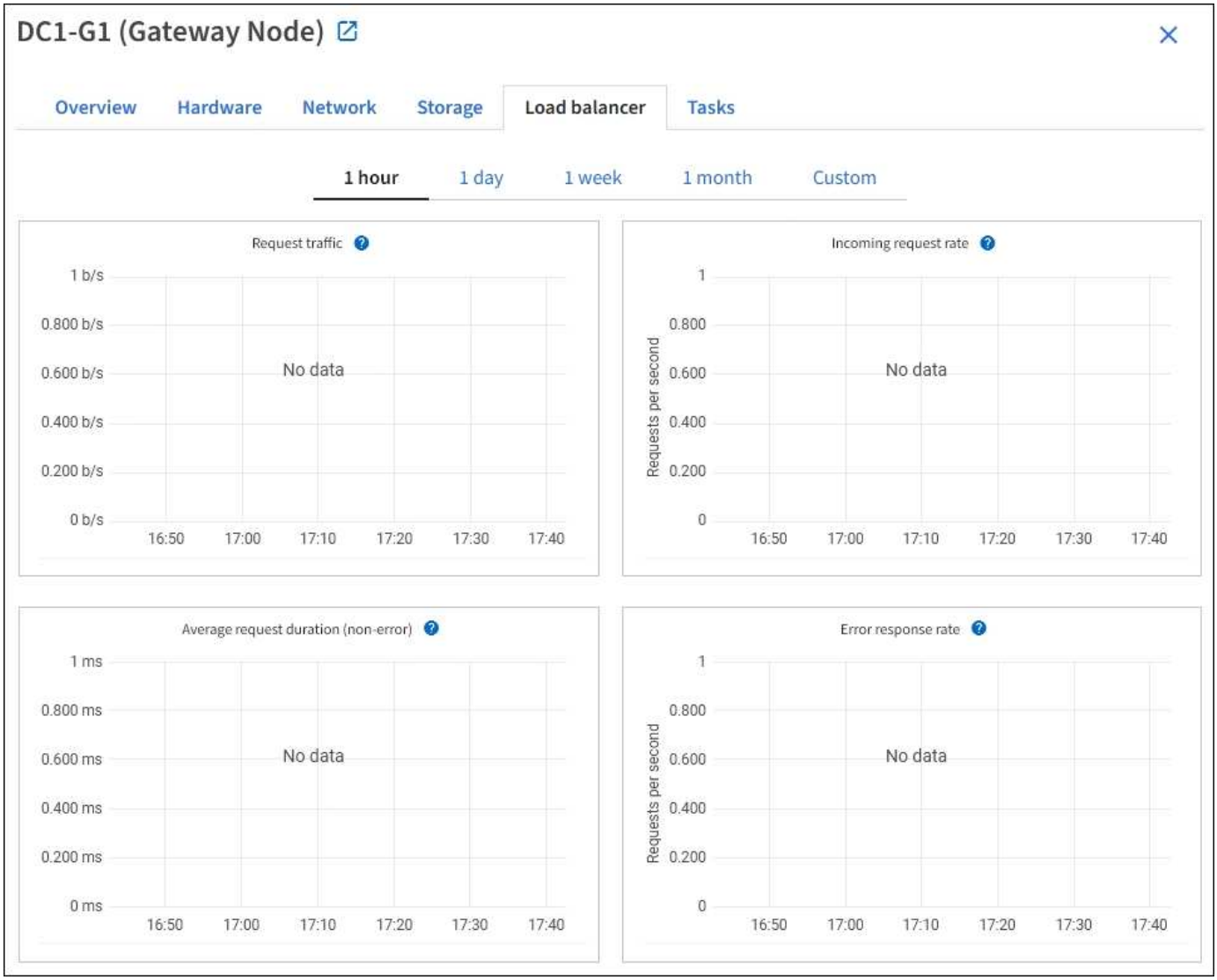
- "Renomeie grade, sites e nós"
- "Reinicie o nó da grade"
- "Coloque o aparelho no modo de manutenção"

Veja a guia balanceador de carga

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

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

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



Solicitar tráfego

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

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

Taxa de solicitação recebida

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

Duração média da solicitação (sem erro)

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

completo é retornado ao cliente.

Taxa de resposta de erro

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

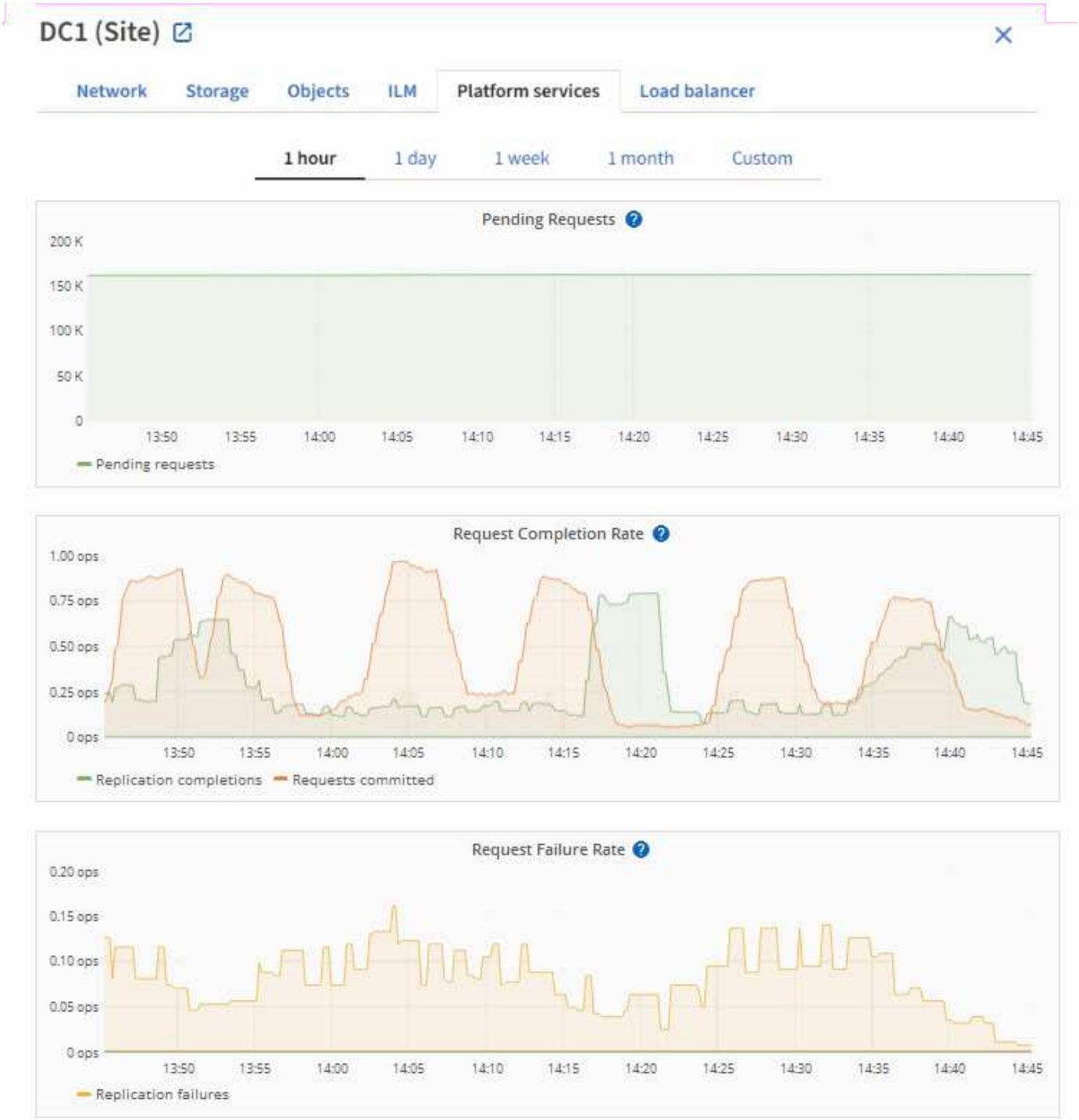
Informações relacionadas

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

Veja a guia Serviços da Plataforma

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

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



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

Veja a guia Gerenciar unidades

A guia Gerenciar unidades permite acessar detalhes e executar tarefas de solução de problemas e manutenção em unidades nos dispositivos que suportam esse recurso.

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

- Exiba um layout das unidades de armazenamento de dados no dispositivo

- Exiba uma tabela que lista cada local, tipo, status, versão do firmware e número de série da unidade
- Execute as funções de solução de problemas e manutenção em cada unidade

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

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

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

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

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

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

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

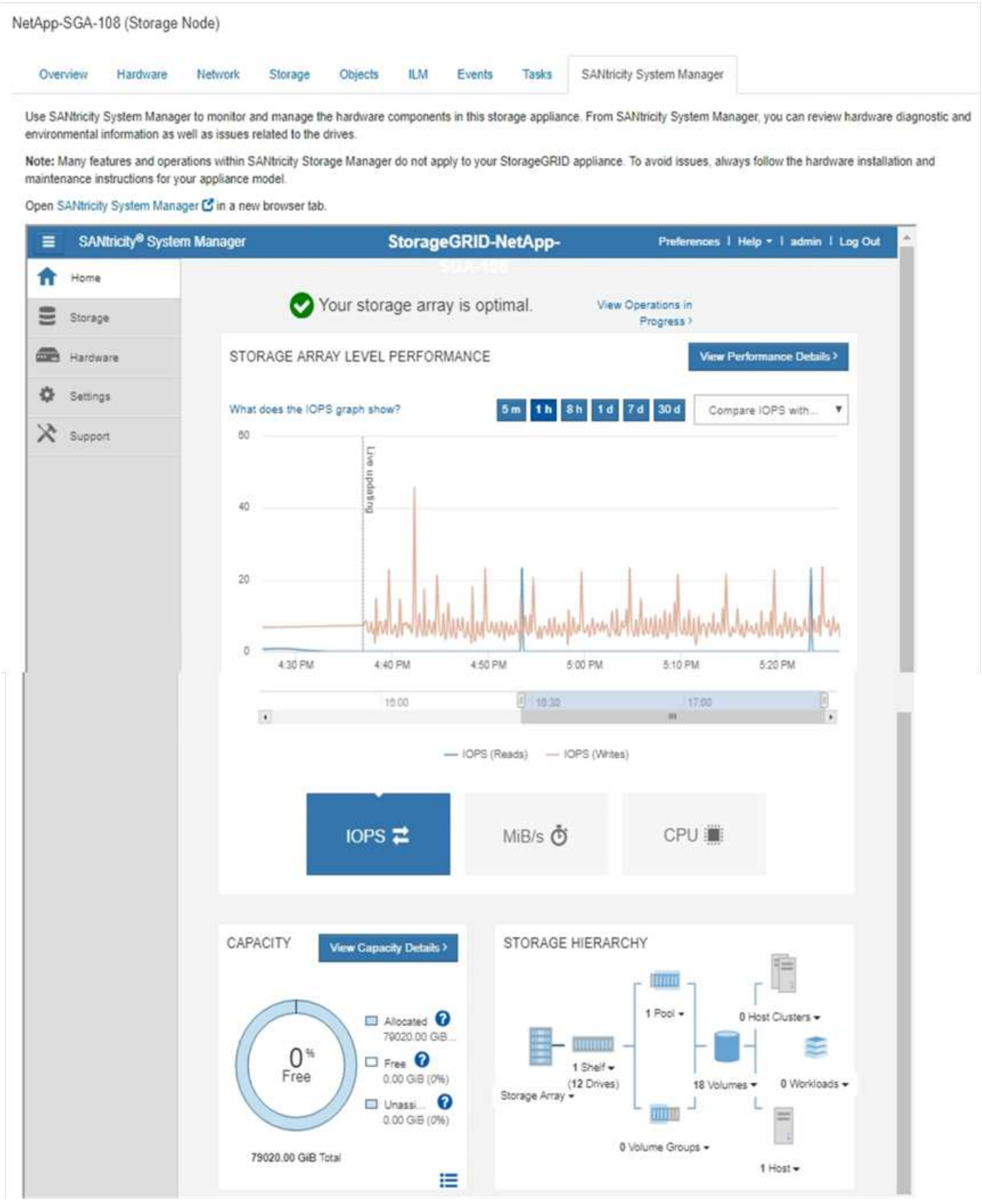
- Visualize dados de performance, como performance em nível de array de storage, latência de e/S, utilização de CPU com controladora de storage e taxa de transferência.
- Verifique o status do componente do hardware.
- Execute funções de suporte, incluindo visualização de dados de diagnóstico e configuração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

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

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

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

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



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

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

cada gráfico.

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

Informações para monitorar regularmente

O que e quando monitorar

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

Antes de começar

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

Sobre tarefas de monitoramento

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

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

Monitorar a integridade do sistema

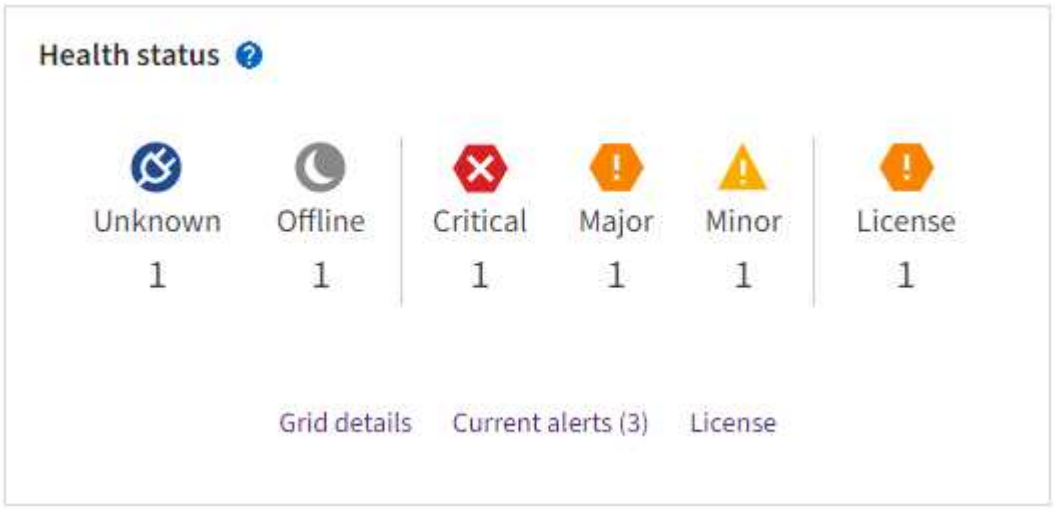
Monitore diariamente a integridade geral do seu sistema StorageGRID.

Sobre esta tarefa

O sistema StorageGRID pode continuar a funcionar quando partes da grelha não estiverem disponíveis. Possíveis problemas indicados por alertas não são necessariamente problemas com as operações do

sistema. Investigue problemas resumidos na placa de estado de funcionamento do Painel do Grid Manager.

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



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

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

Monitorar os estados de conexão do nó

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

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

Ver alertas atuais e resolvidos

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

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

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

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

Cabeçalho da coluna	Descrição
Nome ou título	O nome do alerta e sua descrição.
Gravidade	A gravidade do alerta. Para alertas atuais, se vários alertas forem agrupados, a linha de título mostra quantas instâncias desse alerta estão ocorrendo em cada gravidade. **Crítico**: Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido. **Major**: Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não pare a operação normal de um nó ou serviço StorageGRID. **Menor**: O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.
Tempo acionado	**Alertas atuais**: A data e a hora em que o alerta foi acionado na sua hora local e em UTC. Se vários alertas forem agrupados, a linha de título mostrará horas para a instância mais recente do alerta (*newest*) e a instância mais antiga do alerta (*older*). **Alertas resolvidos**: Há quanto tempo o alerta foi acionado.
Local/nó	O nome do site e do nó onde o alerta está ocorrendo ou ocorreu.

Cabeçalho da coluna	Descrição
Estado	Se o alerta está ativo, silenciado ou resolvido. Se vários alertas forem agrupados e **todos os alertas** estiverem selecionados na lista suspensa, a linha de título mostrará quantas instâncias desse alerta estão ativas e quantas instâncias foram silenciadas.
Tempo resolvido (apenas alertas resolvidos)	Há quanto tempo o alerta foi resolvido.
Valores atuais ou *valores de dados*	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta **armazenamento de dados de objeto baixo** incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado. **Nota:** se vários alertas atuais forem agrupados, os valores atuais não serão exibidos na linha de título.
Valores acionados (apenas alertas resolvidos)	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta **armazenamento de dados de objeto baixo** incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado.

Passos

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

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

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

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

2. Para expandir grupos de alertas, selecione o cursor para baixo . Para recolher alertas individuais num grupo, selecione o cursor para cima ou selecione o nome do grupo.
3. Para exibir alertas individuais em vez de grupos de alertas, desmarque a caixa de seleção **alertas de grupo**.
4. Para classificar os alertas atuais ou grupos de alertas, selecione as setas para cima/para baixo em cada cabeçalho de coluna.
   - Quando **alertas de grupo** é selecionado, tanto os grupos de alerta quanto os alertas individuais dentro de cada grupo são classificados. Por exemplo, você pode querer classificar os alertas em um grupo por **tempo disparado** para encontrar a instância mais recente de um alerta específico.

- Quando **alertas de grupo** é limpo, toda a lista de alertas é classificada. Por exemplo, você pode querer classificar todos os alertas por **nó/Site** para ver todos os alertas que afetam um nó específico.

5. Para filtrar os alertas atuais por status (**todos os alertas**, **Ativo** ou **silenciado**, use o menu suspenso na parte superior da tabela.

   "Silenciar notificações de alerta"Consulte .

6. Para classificar alertas resolvidos:
   - Selecione um período de tempo a partir do menu pendente **When Triggered**.
   - Selecione uma ou mais severidades no menu suspenso **severidade**.
   - Selecione uma ou mais regras de alerta padrão ou personalizadas no menu suspenso **regra de alerta** para filtrar os alertas resolvidos relacionados a uma regra de alerta específica.
   - Selecione um ou mais nós no menu suspenso **Node** para filtrar os alertas resolvidos relacionados a um nó específico.
7. Para ver detalhes de um alerta específico, selecione o alerta. Uma caixa de diálogo fornece detalhes e ações recomendadas para o alerta selecionado.
8. (Opcional) para um alerta específico, selecione Silenciar este alerta para silenciar a regra de alerta que fez com que esse alerta fosse acionado.

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

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

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

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

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

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

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

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

Monitorar a capacidade de armazenamento

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

O StorageGRID armazena os dados de objeto e os metadados de objeto separadamente e reserva uma quantidade específica de espaço para um banco de dados Cassandra distribuído que contém metadados de

objeto. Monitore a quantidade total de espaço consumida para objetos e metadados de objetos, bem como tendências na quantidade de espaço consumida para cada um. Isso permitirá que você se Planeje com antecedência para a adição de nós e evite interrupções de serviço.

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

Monitore a capacidade de armazenamento de toda a grade

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

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

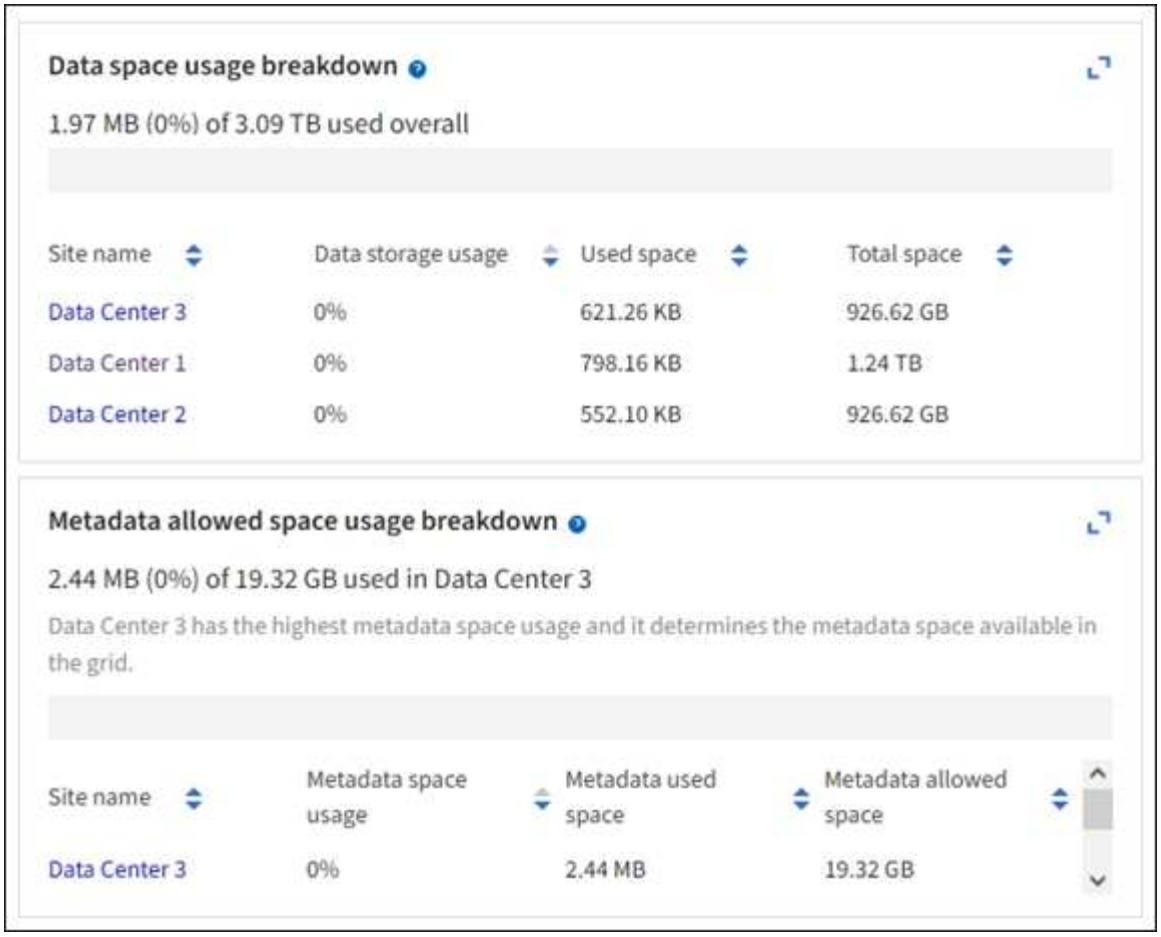
Passos

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

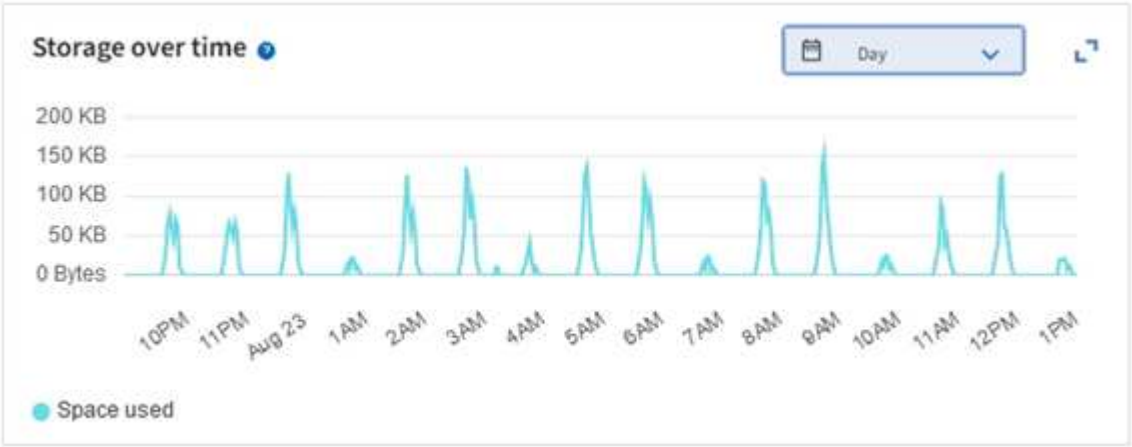
   a. Selecione **Painel > Visão geral**.

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

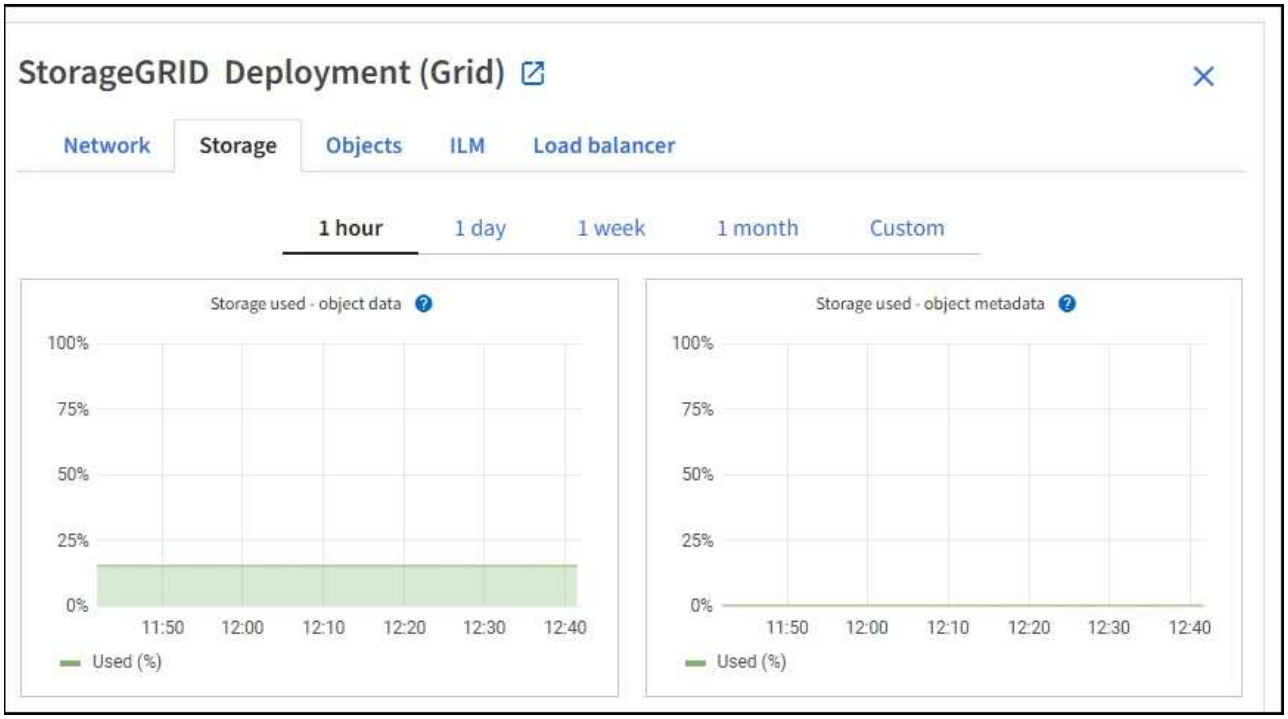
      O resumo não inclui Mídia de arquivamento.



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



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



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

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

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

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

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

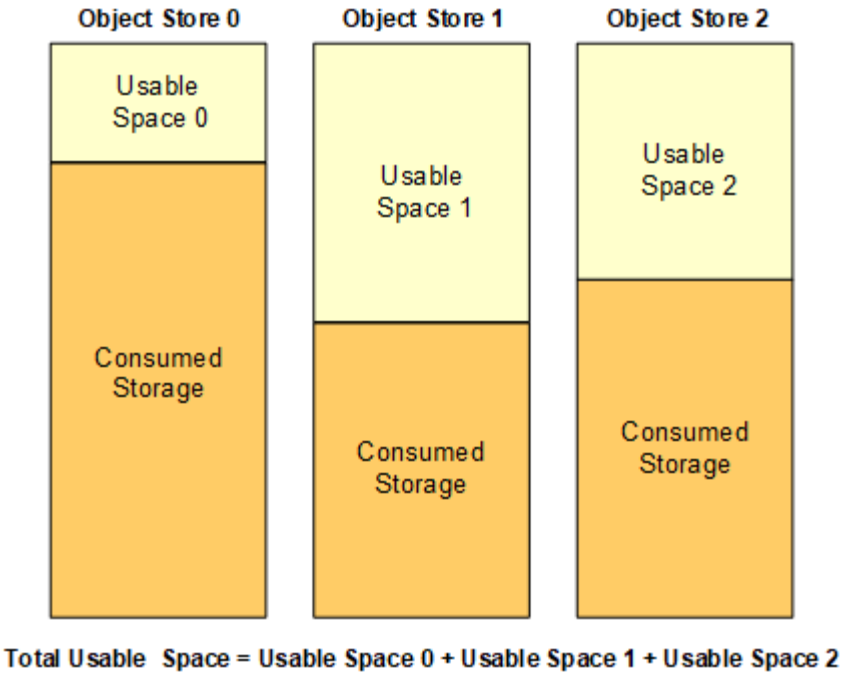
   Para obter mais informações sobre como Planejar uma expansão de armazenamento, consulte o "Instruções para expandir StorageGRID".

Monitore a capacidade de storage para cada nó de storage

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

Sobre esta tarefa

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



Passos

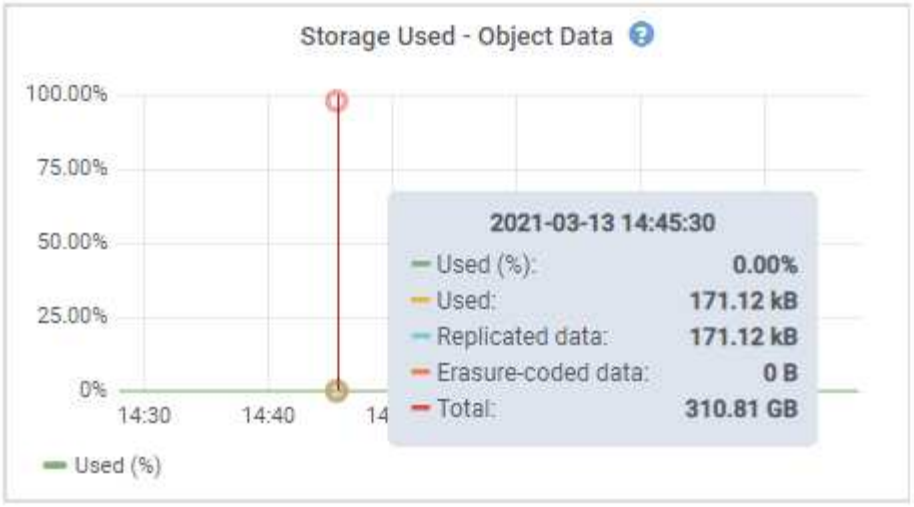
1. Selecione **NÓS** > ***Storage Node*** > **Storage**.

   Os gráficos e tabelas para o nó aparecem.

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

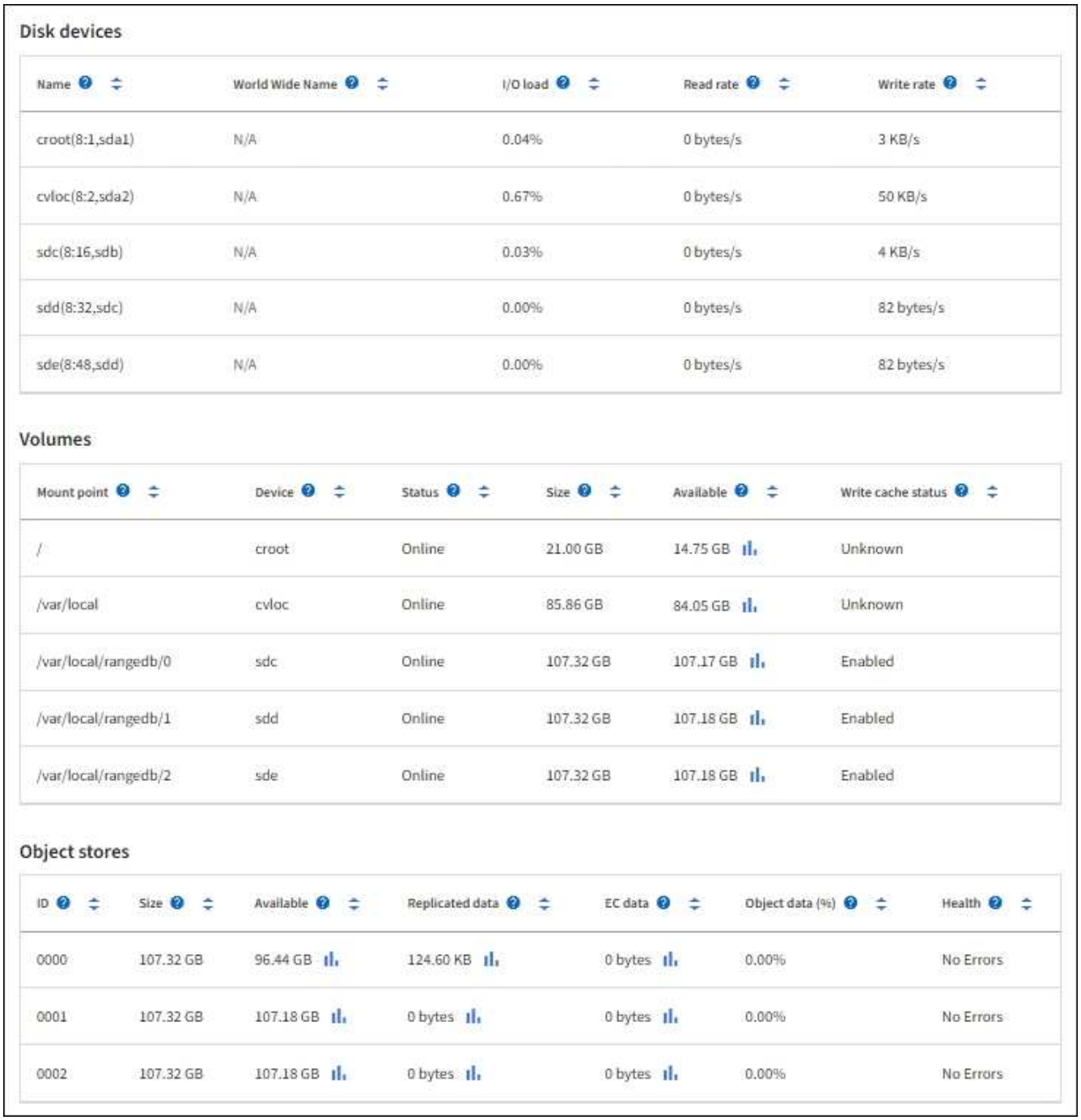
   São apresentados os seguintes valores:

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



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

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



Disk devices

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

Volumes

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

Object stores

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

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

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

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

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

"Instruções para expandir StorageGRID".

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

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

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

Sobre esta tarefa

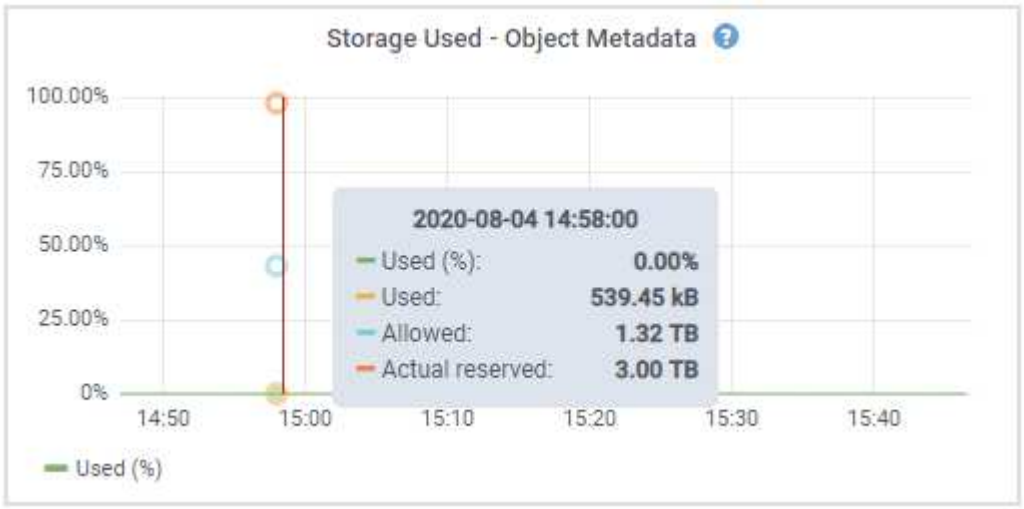
O StorageGRID mantém três cópias de metadados de objetos em cada local para fornecer redundância e proteger os metadados de objetos da perda. As três cópias são distribuídas uniformemente por todos os nós de storage em cada local, usando o espaço reservado para metadados no volume de storage 0 de cada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

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

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

Passos

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



Usado (%)

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

Métricas de Prometheus: `storagegrid_storage_utilization_metadata_bytes` E `storagegrid_storage_utilization_metadata_allowed_bytes`

Usado

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

Métrica Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Permitido

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

Métrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Real reservado

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

Prometheus métrica será adicionada em uma versão futura.

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

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

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

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

Monitorar previsões de uso de espaço

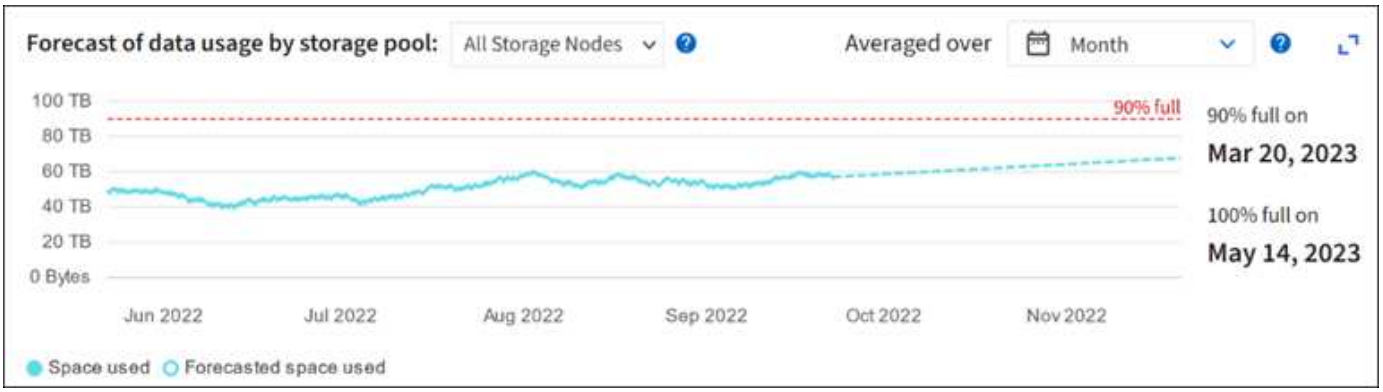
Monitore as previsões de uso de espaço para dados e metadados do usuário para estimar quando será "expanda uma grade"necessário .

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

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

Passos

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



Monitorar o gerenciamento do ciclo de vida das informações

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

Sobre esta tarefa

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

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

Use a guia Painel do Gerenciador de Grade

Passos

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

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

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

Use a página NÓS

Passos

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

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

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

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

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

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

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

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

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

Monitorar recursos de rede e do sistema

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

Monitorar conexões de rede e desempenho

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

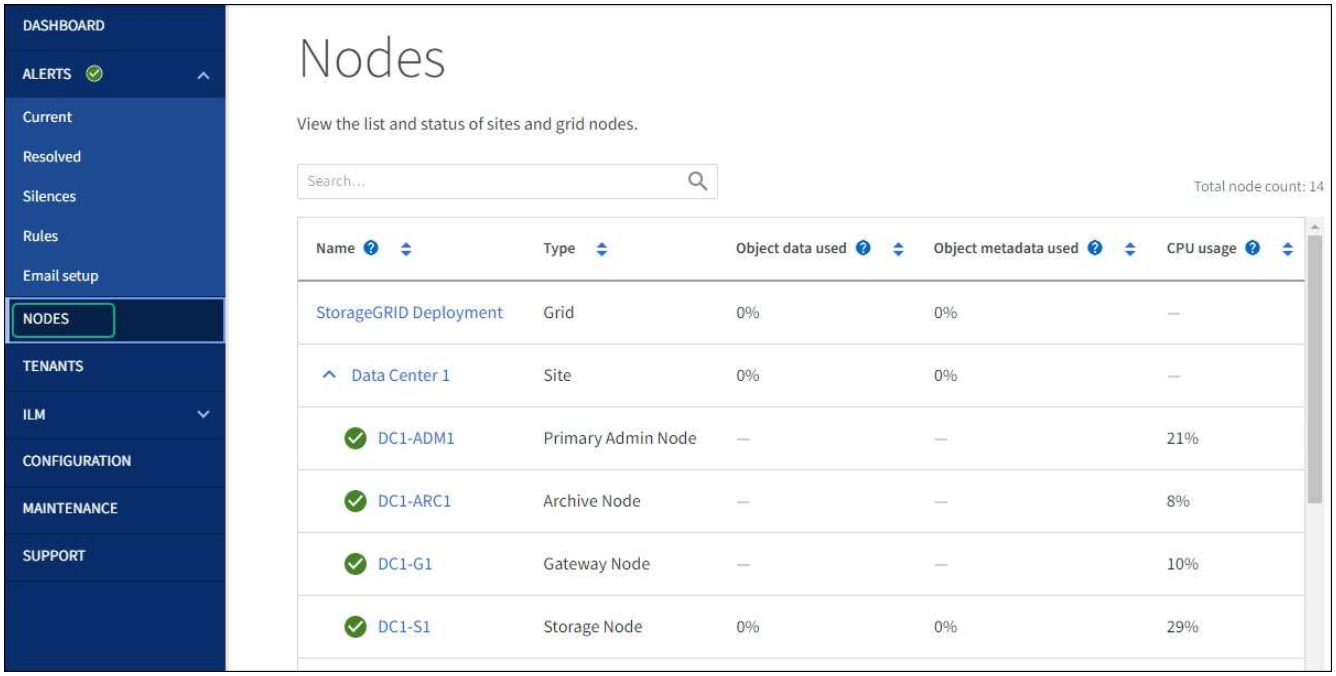
Use o Gerenciador de Grade para monitorar a conetividade e o desempenho da rede, para que você possa resolver quaisquer problemas imediatamente.

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

Passos

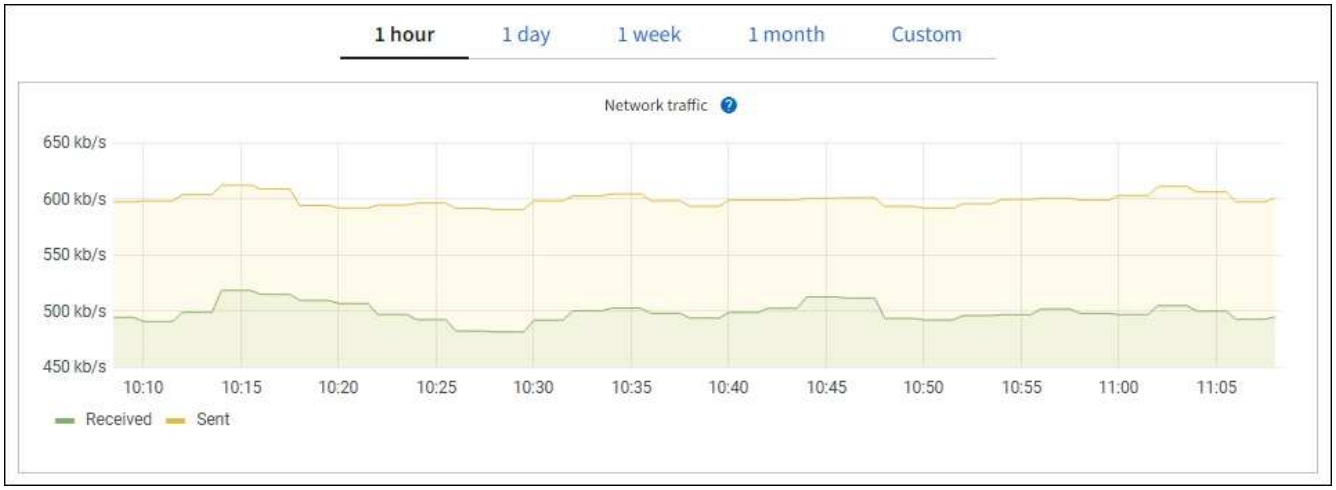
1. Selecione **NODES**.

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

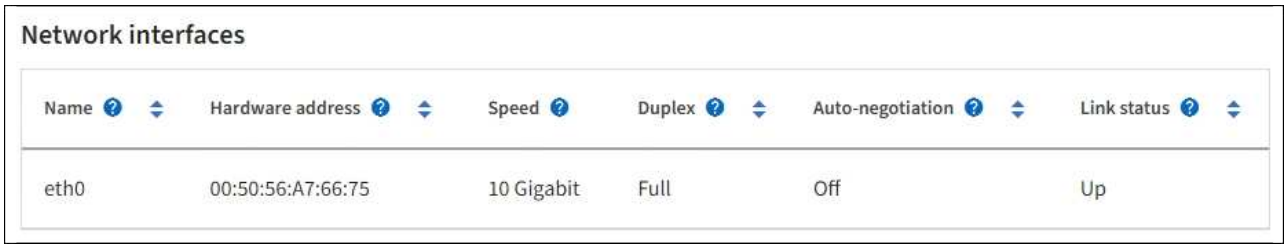


2. Selecione o nome da grade, um site específico de data center ou um nó de grade e, em seguida, selecione a guia **rede**.

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

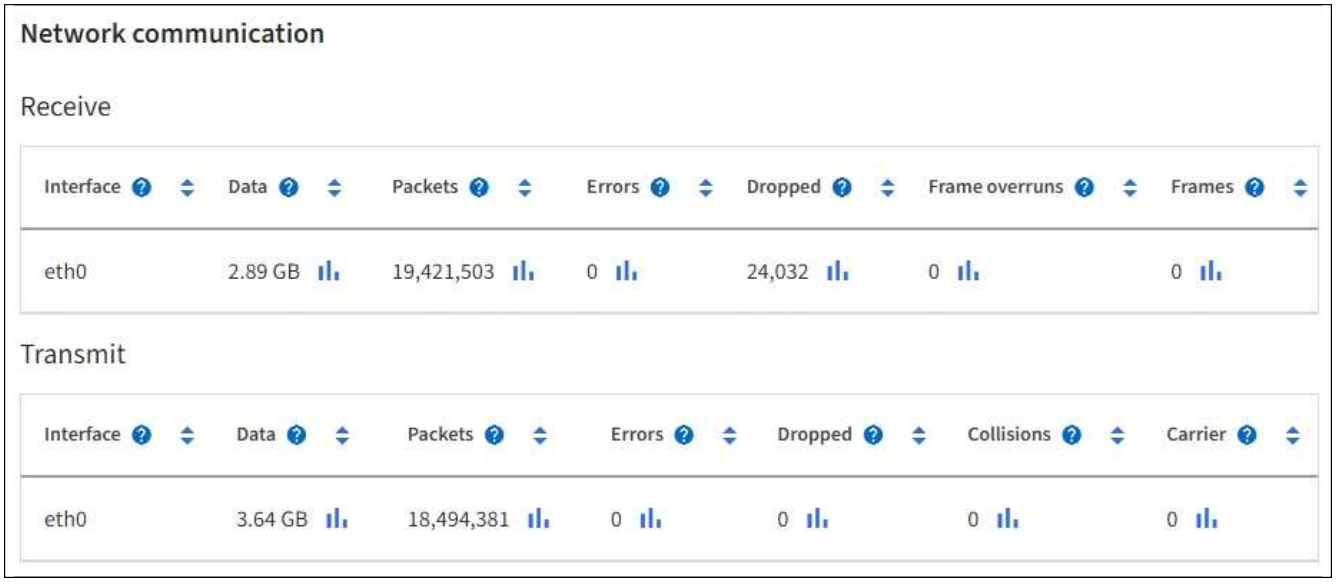


   a. Se você selecionou um nó de grade, role para baixo para revisar a seção **interfaces de rede** da página.



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

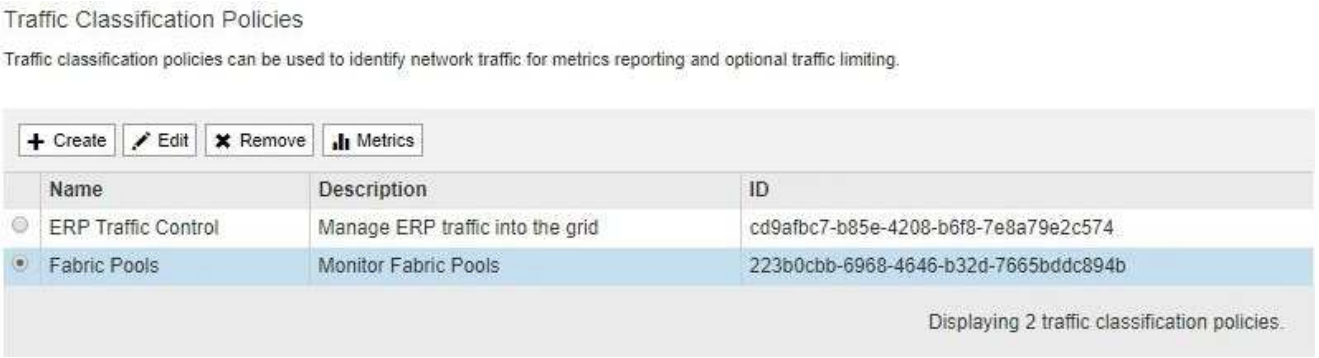
   As tabelas de receção e transmissão mostram quantos bytes e pacotes foram recebidos e enviados através de cada rede, bem como outras métricas de receção e transmissão.



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

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

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



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

   b. Reveja os gráficos para compreender o tráfego de rede associado à política.

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

necessário", .

Informações relacionadas

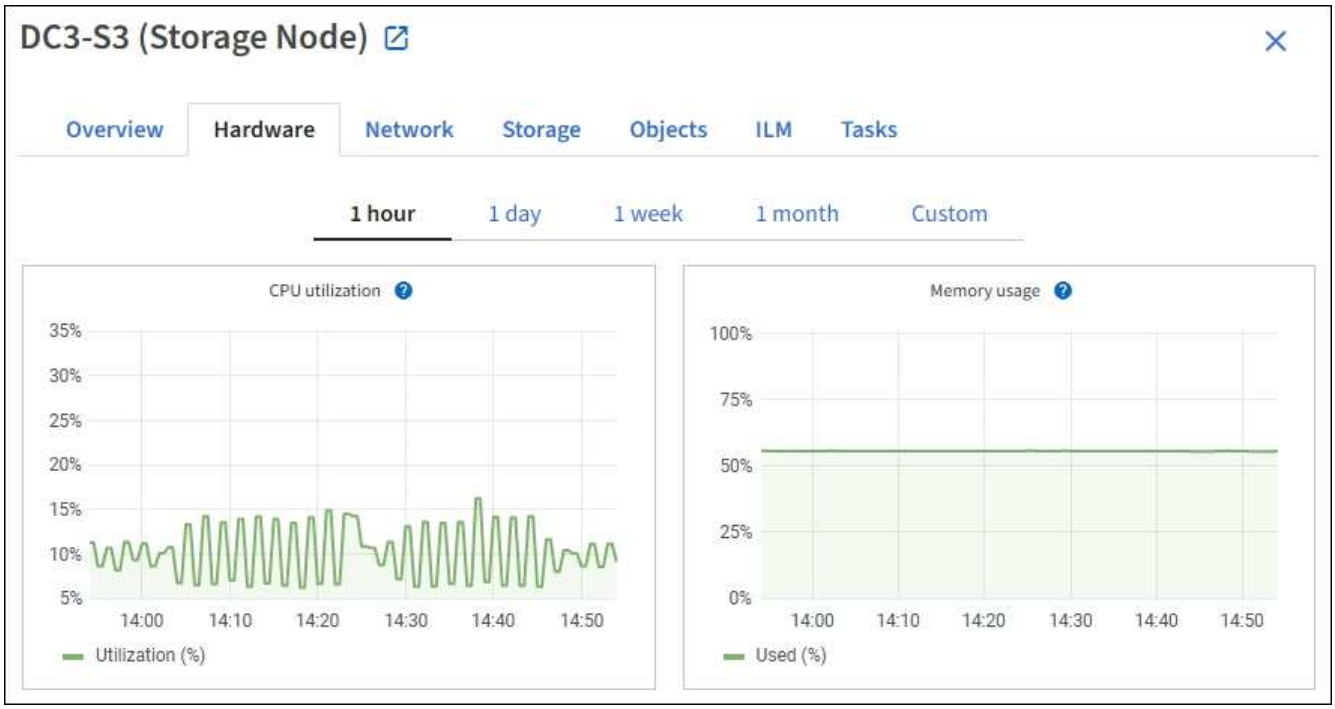
- "Veja a guia rede"
- "Monitorar os estados de conexão do nó"

Monitore os recursos no nível do nó

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

Passos

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



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

Informações relacionadas

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

Monitorar a atividade do locatário

Todas as atividades do cliente S3 estão associadas às contas de inquilino do StorageGRID. Você pode usar o Gerenciador de Grade para monitorar o uso do

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

Antes de começar

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

Ver todos os inquilinos

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

Passos

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

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

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

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

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

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

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

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

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

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

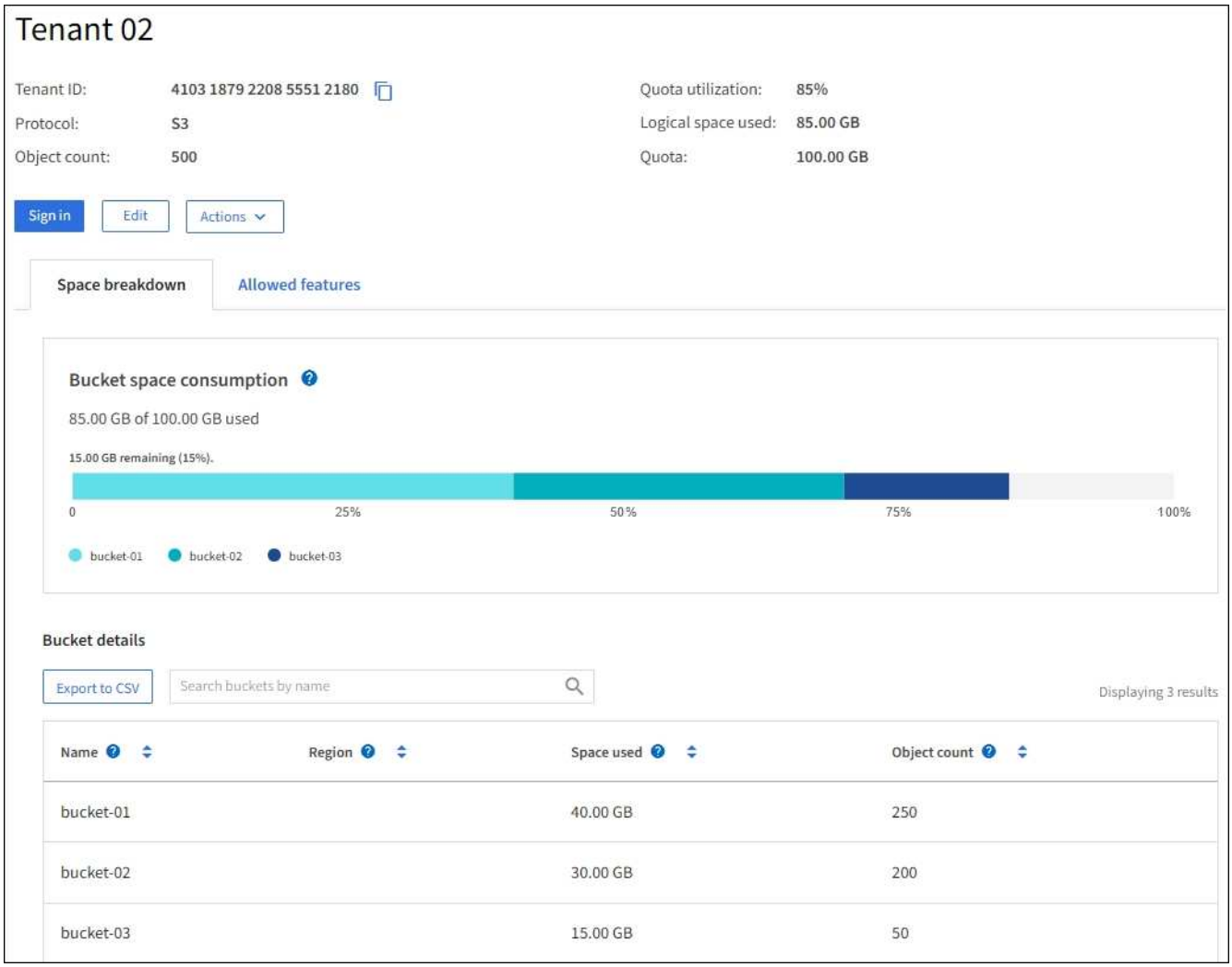
Exibir um locatário específico

Você pode exibir detalhes de um locatário específico.

Passos

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

   A página de detalhes do locatário é exibida.



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

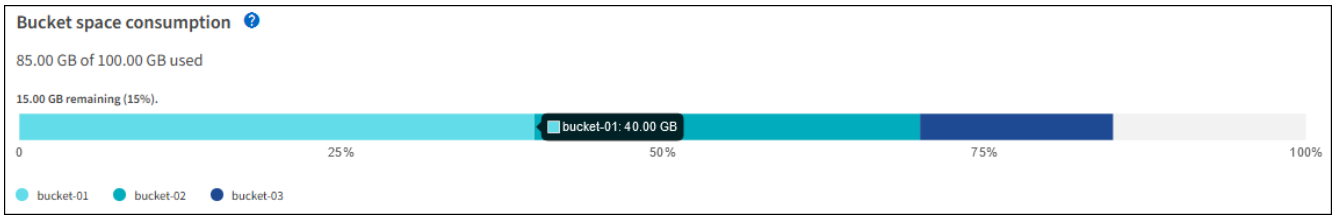
   Esta seção da página de detalhes fornece informações resumidas para o locatário, incluindo a contagem de objetos do locatário, o uso da cota, o espaço lógico usado e a configuração da cota.

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

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

   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.



O uso da cota é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita 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 o uso da cota seja recalculado. Os cálculos de uso de cotas podem levar 10 minutos ou mais.

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

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

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

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

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

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

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

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

6. Opcionalmente, selecione a guia **recursos permitidos** para ver uma lista das permissões e recursos que estão habilitados para o locatário. "Editar conta de locatário"Veja se você precisa alterar qualquer uma dessas configurações.
7. Se o locatário tiver a permissão **usar conexão de federação de grade**, selecione opcionalmente a guia **federação de grade** para saber mais sobre a conexão.

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

Ver o tráfego de rede

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

Passos

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

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

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

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

Use o log de auditoria

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

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

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

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

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

Use métricas Prometheus

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

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

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

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

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

Monitorar S3 operações do cliente

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

Antes de começar

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

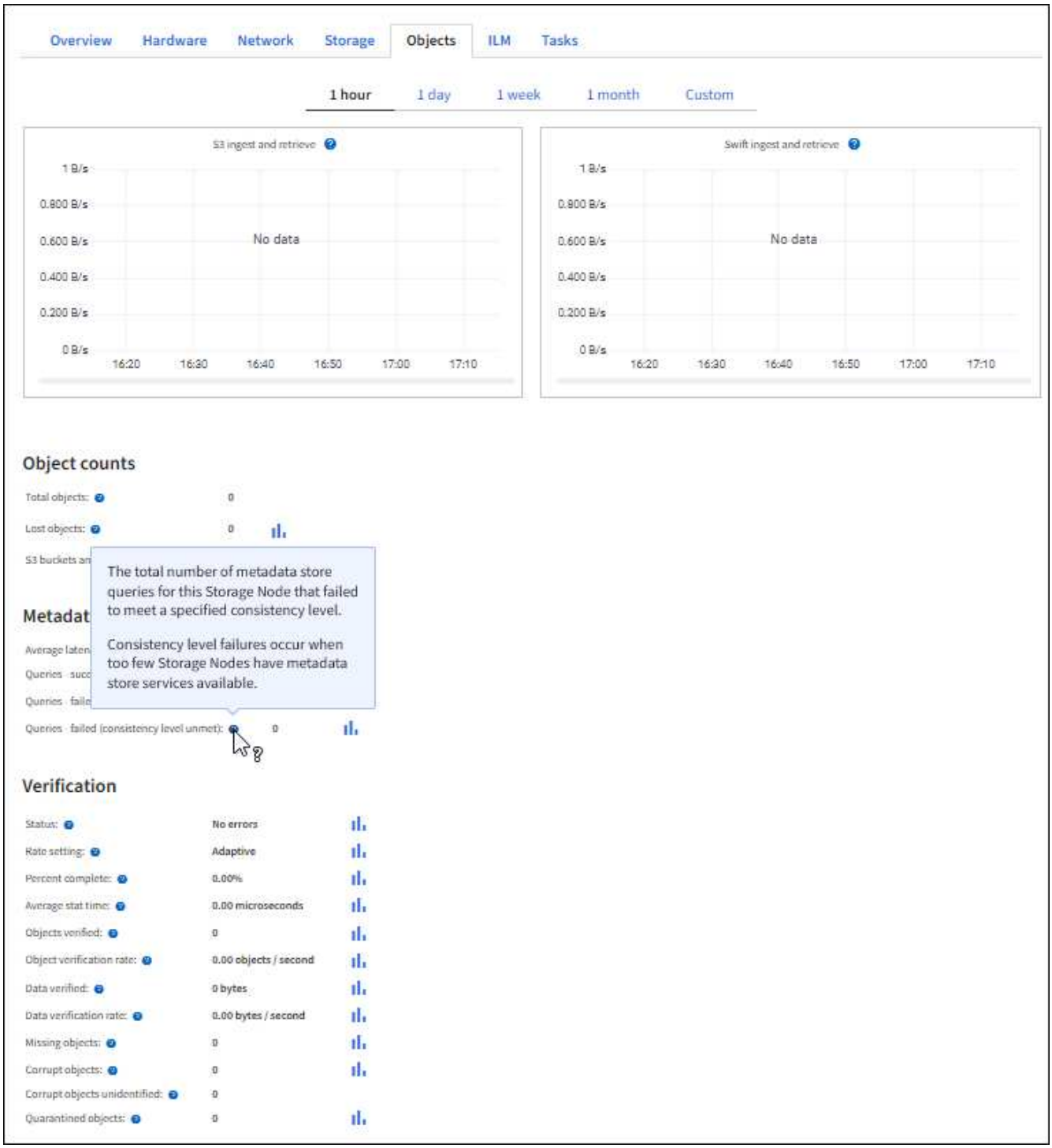
Passos

1. No painel, selecione a guia **desempenho**.
2. Consulte os gráficos S3D, que resumem o número de operações do cliente executadas pelos nós de storage e o número de solicitações de API recebidas pelos nós de storage durante o período de tempo selecionado.
3. Selecione **NÓS** para acessar a página nós.
4. Na página inicial dos nós (nível de grade), selecione a guia **objetos**.

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

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

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



Monitorar operações de balanceamento de carga

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

Sobre esta tarefa

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

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

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

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

Passos

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

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

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

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

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

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

Monitorar conexões de federação de grade

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

Antes de começar

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

Ver todas as ligações

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

Passos

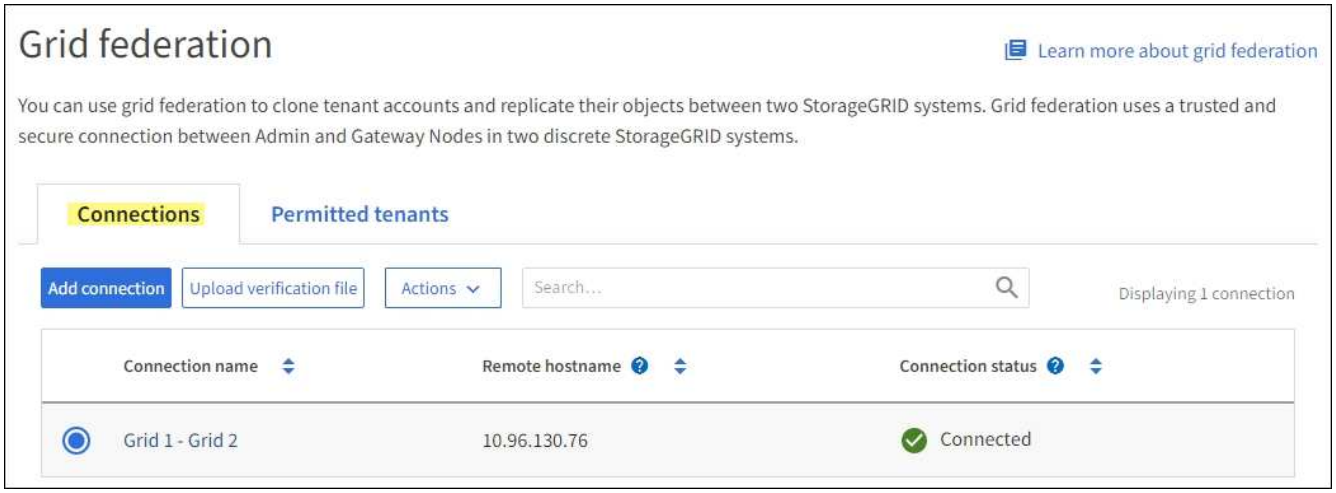
1. Selecione **CONFIGURATION** > **System** > **Grid Federation**.

   A página de federação de grade é exibida.

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

   Nesta guia, você pode:

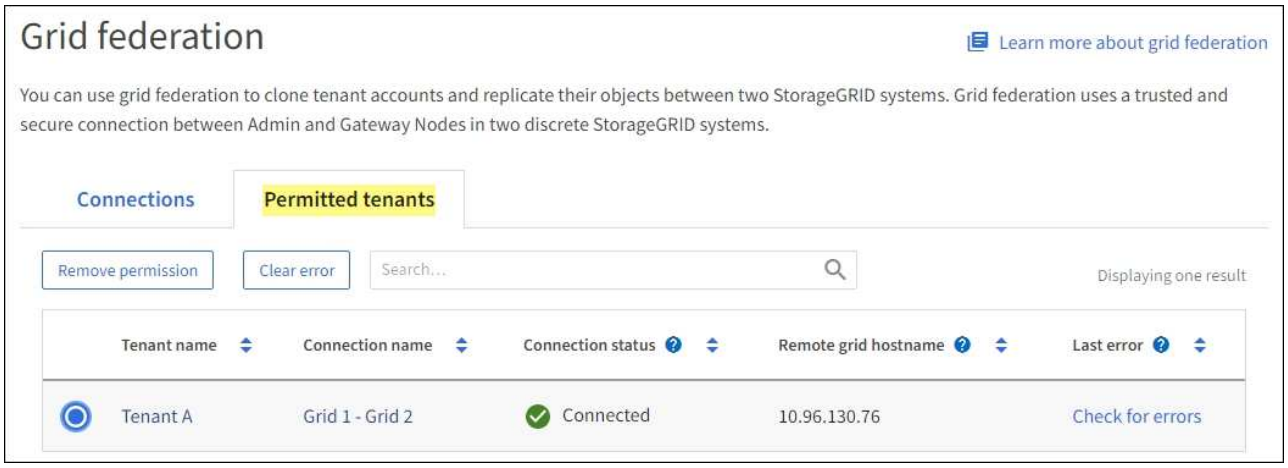
   - "Crie uma nova conexão".
   - Selecione uma conexão existente com "editar ou testar"o .



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

   Nesta guia, você pode:

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



Veja uma conexão específica

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

Passos

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

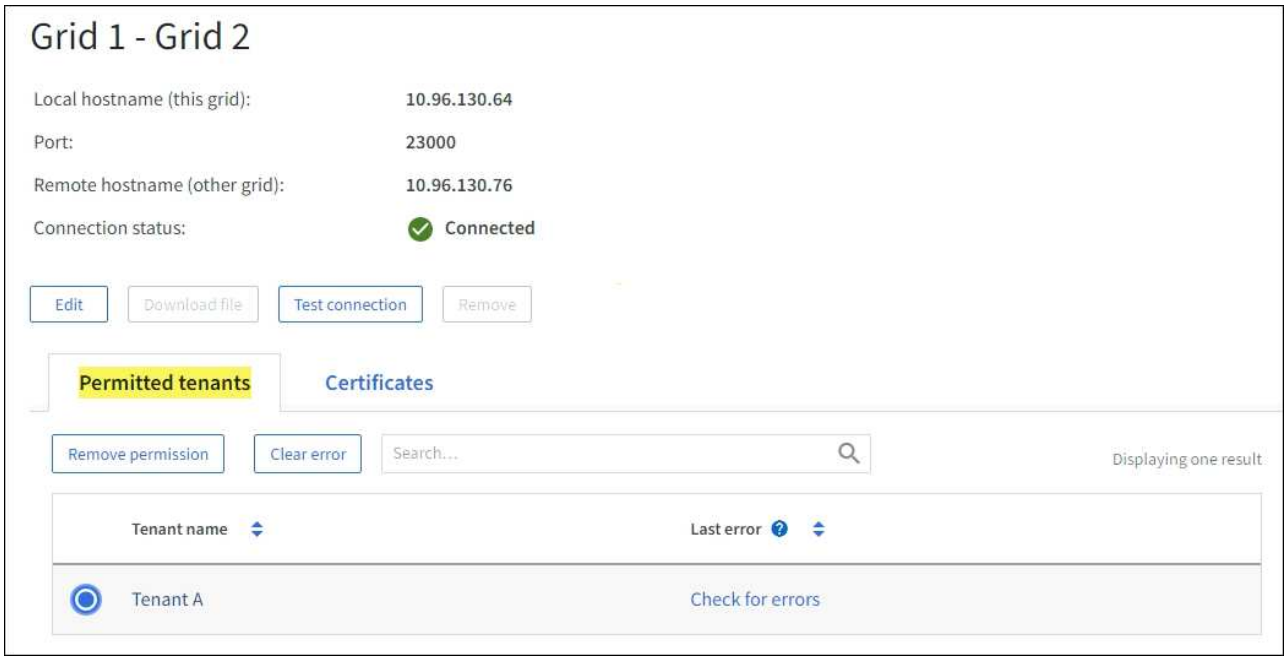
   Na página de detalhes da conexão, você pode:

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

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

   Nesta guia, você pode:

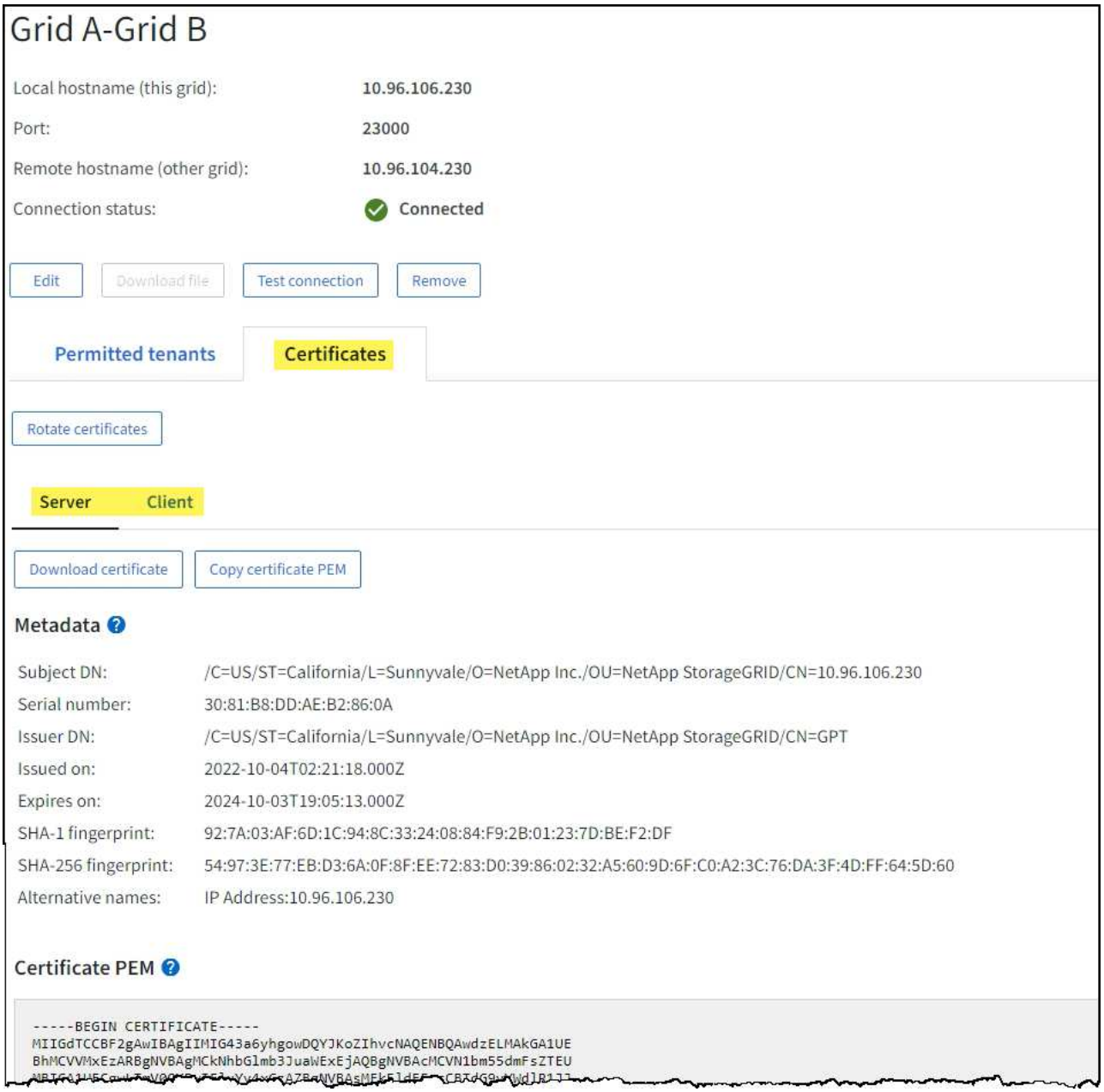
   - "Veja a página de detalhes de cada locatário permitido".
   - "Remova a permissão de um locatário" para utilizar a ligação.
   - Verifique se há erros de replicação entre redes e limpe o último erro. "Solucionar erros de federação de grade"Consulte .



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

   Nesta guia, você pode:

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



Analise as métricas de replicação entre grades

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

Passos

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

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

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

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

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

Gerenciar alertas

Gerenciar alertas

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.

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

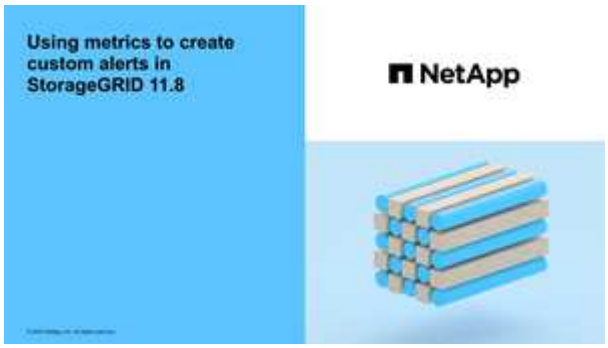
- Um ícone de gravidade de alerta é mostrado no painel do Gerenciador de Grade e a contagem de Alertas atuais é incrementada.
- O alerta é mostrado na página de resumo **NÓS** e na guia **NÓS** > ***node*** > **Visão geral**.
- Uma notificação por e-mail é enviada, supondo que você tenha configurado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

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

Para saber mais:

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

- Reveja o vídeo: "Vídeo: Alertas personalizados"



- Consulte "Referência de alertas".

Ver regras de alerta

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

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

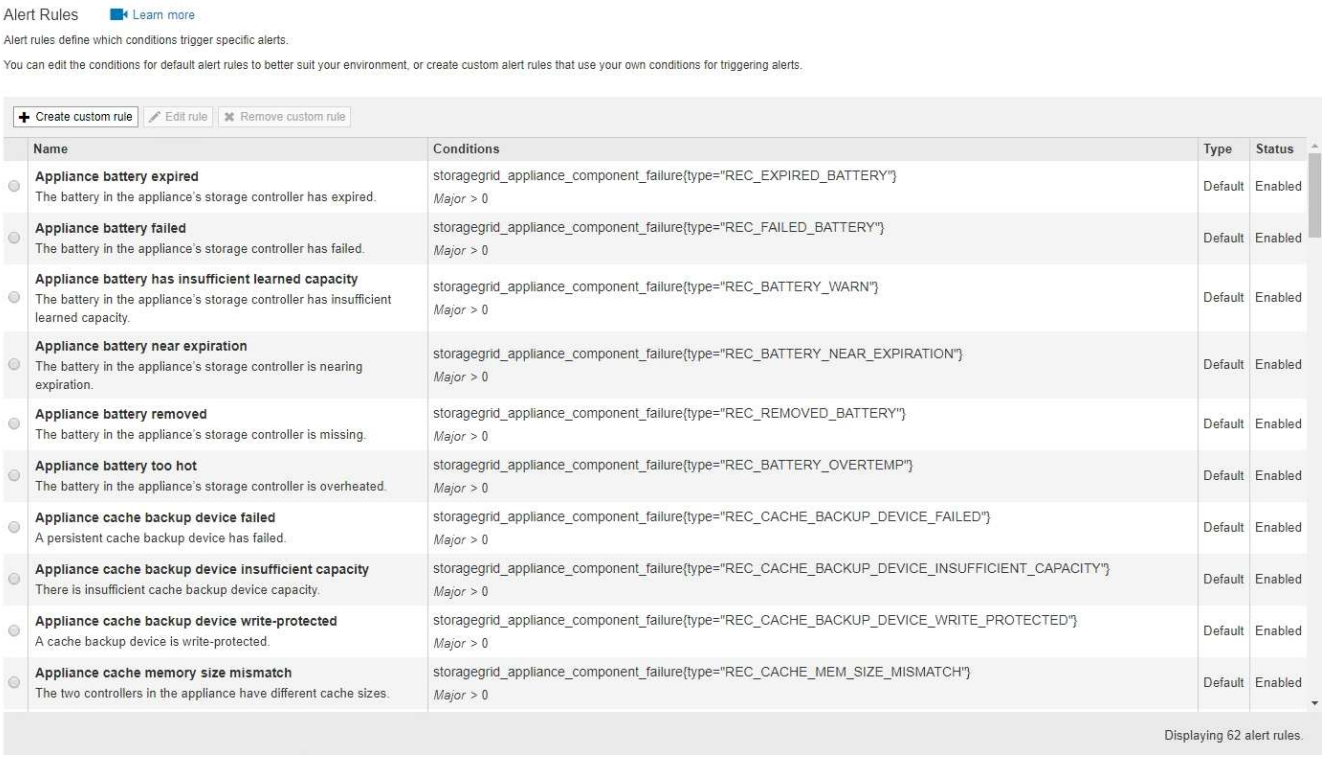
Antes de começar

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

Passos

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

   A página regras de alerta é exibida.



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

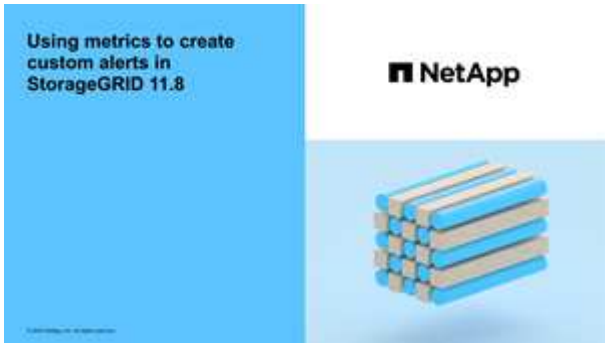
Cabeçalho da coluna	Descrição
Nome	O nome exclusivo e a descrição da regra de alerta. As regras de alerta personalizadas são listadas primeiro, seguidas pelas regras de alerta padrão. O nome da regra de alerta é o assunto das notificações por e-mail.
Condições	As expressões Prometheus que determinam quando esse alerta é acionado. Um alerta pode ser acionado em um ou mais dos seguintes níveis de gravidade, mas não é necessária uma condição para cada gravidade. • **Crítico** : existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido. • **Major** : existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não pare a operação normal de um nó ou serviço StorageGRID. • **Minor** : o sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.
Tipo	O tipo de regra de alerta: • **Default**: Uma regra de alerta fornecida com o sistema. Você pode desativar uma regra de alerta padrão ou editar as condições e a duração de uma regra de alerta padrão. Não é possível remover uma regra de alerta padrão. • **Padrão***: Uma regra de alerta padrão que inclui uma condição ou duração editada. Conforme necessário, você pode reverter facilmente uma condição modificada de volta ao padrão original. • **Custom**: Uma regra de alerta que você criou. Você pode desativar, editar e remover regras de alerta personalizadas.
Estado	Se esta regra de alerta está atualmente ativada ou desativada. As condições para regras de alerta desativadas não são avaliadas, portanto, nenhum alerta é acionado.

Crie regras de alerta personalizadas

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".
- Você está familiarizado com o "Métricas de Prometheus comumente usadas".
- Você entende o "Sintaxe das consultas Prometheus".
- Opcionalmente, você assistiu o vídeo: "Vídeo: 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 "bem-sucedida" pode ser um corpo de resposta vazio (nenhum alerta acionado). Para ver se o alerta é realmente acionado, você pode definir temporariamente um limite para um valor que você espera ser verdadeiro atualmente.

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

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

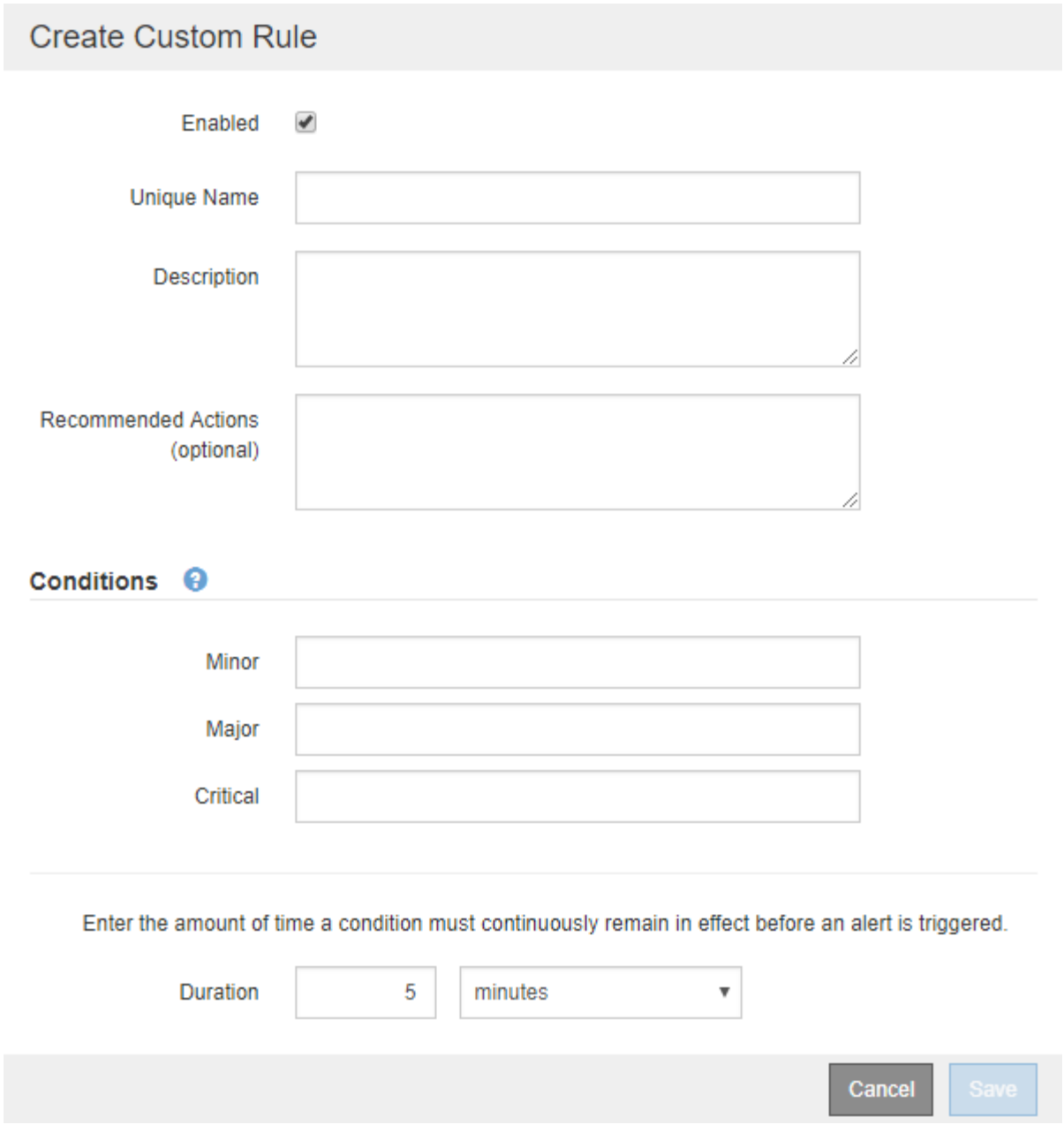
Passos

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

   A página regras de alerta é exibida.

2. Selecione **criar regra personalizada**.

   A caixa de diálogo criar regra personalizada é exibida.



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

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

4. Introduza as seguintes informações:

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

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 carateres.
Ações recomendadas	Opcionalmente, as ações recomendadas a serem tomadas quando esse alerta for acionado. Insira as ações recomendadas como texto simples (sem códigos de formatação). As ações recomendadas para regras de alerta podem ter entre 0 e 1.024 carateres.

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

   Uma expressão básica é geralmente da forma:

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

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

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

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

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

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

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

   O padrão é 5 minutos.

7. Selecione **Guardar**.

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

Editar regras de alerta

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

Antes de começar

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

Sobre esta tarefa

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

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

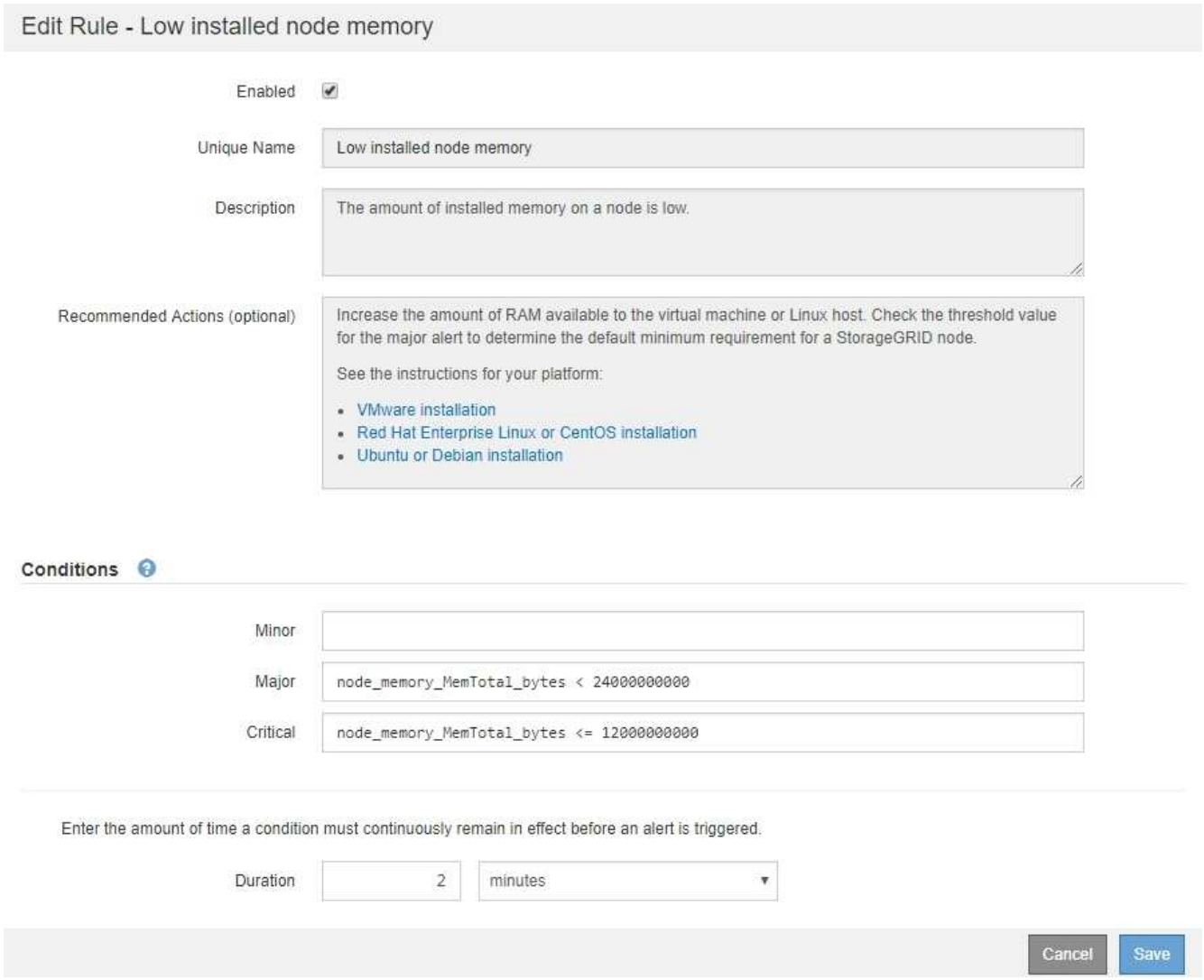
Passos

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

   A página regras de alerta é exibida.

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

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



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

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

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

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

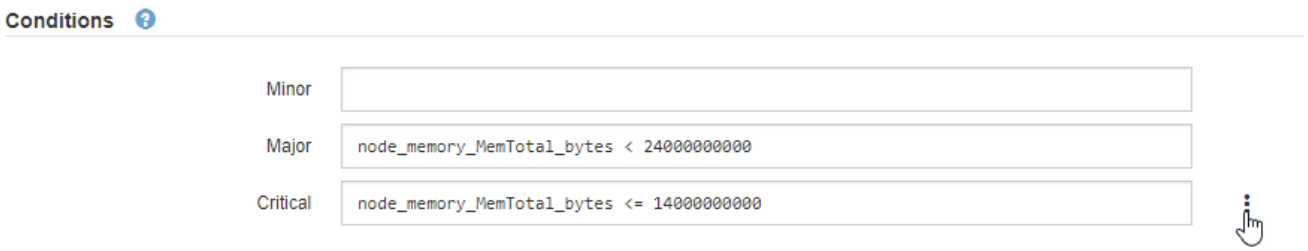
5. Para regras de alerta personalizadas, atualize as seguintes informações conforme necessário.

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

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

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

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



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

Uma expressão básica é geralmente da forma:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

   O padrão é 5 minutos.

8. Selecione **Guardar**.

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

Desativar regras de alerta

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

Antes de começar

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

Sobre esta tarefa

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

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

Passos

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

   A página regras de alerta é exibida.

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

   A caixa de diálogo Editar regra é exibida.

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

no momento.

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

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

5. Selecione **Guardar**.

   Disabled aparece na coluna **Status**.

Remover regras de alerta personalizadas

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

Antes de começar

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

Passos

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

   A página regras de alerta é exibida.

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

   Não é possível remover uma regra de alerta padrão.

3. Selecione **Remover regra personalizada**.

   É apresentada uma caixa de diálogo de confirmação.

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

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

Gerenciar notificações de alerta

Configurar notificações SNMP para alertas

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

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

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

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

ser enviados:

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

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

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

Configurar notificações por e-mail para alertas

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

Antes de começar

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

Sobre esta tarefa

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

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

Passos

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

   A página Configuração de e-mail é exibida.

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

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

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

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

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

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

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

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

      Selecione o ícone de mais ➕para adicionar destinatários.

5. Se a TLS (Transport Layer Security) for necessária para comunicações com o servidor SMTP, selecione **Require TLS** na seção TLS (Transport Layer Security).
   a. No campo **certificado CA**, forneça o certificado CA que será usado para verificar a identificação do servidor SMTP.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Selecione **Guardar**.

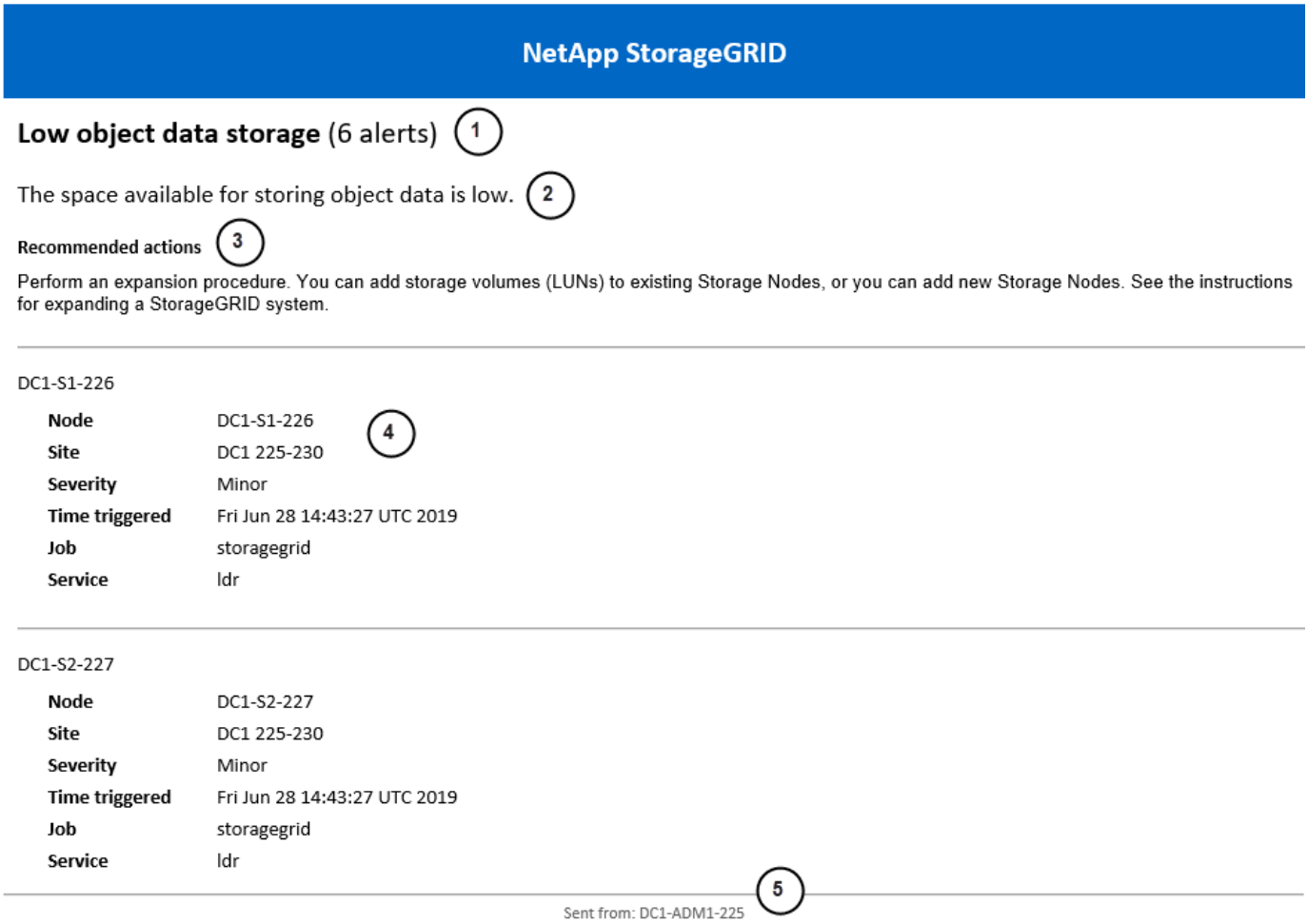
   Enviar um e-mail de teste não salva suas configurações. Você deve selecionar **Salvar**.

   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:



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

Como os alertas são agrupados

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

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

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

Solucionar problemas de notificações por e-mail de alerta

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

Antes de começar

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

Passos

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

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

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

Silenciar notificações de alerta

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

Antes de começar

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

Sobre esta tarefa

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

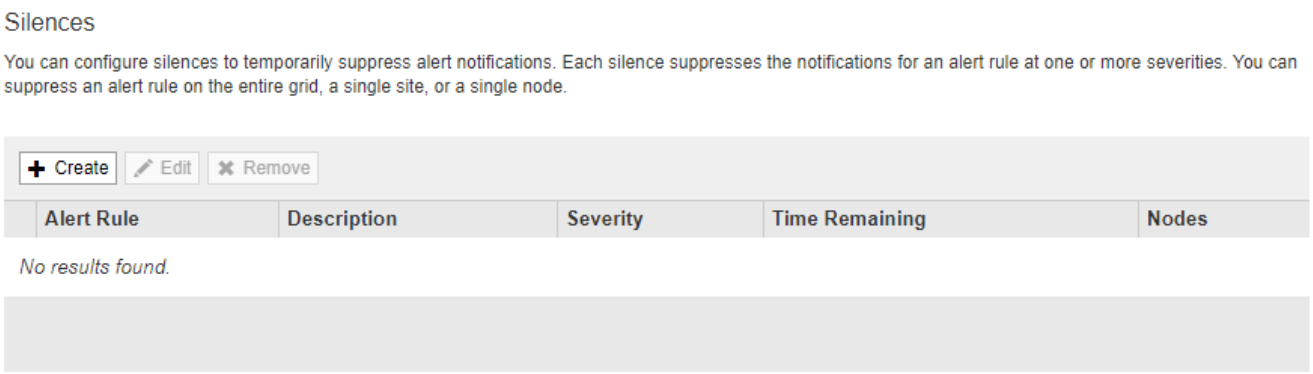
Se tiver ativado o agente SNMP, os silêncios também suprimem traps SNMP e informam.

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

Passos

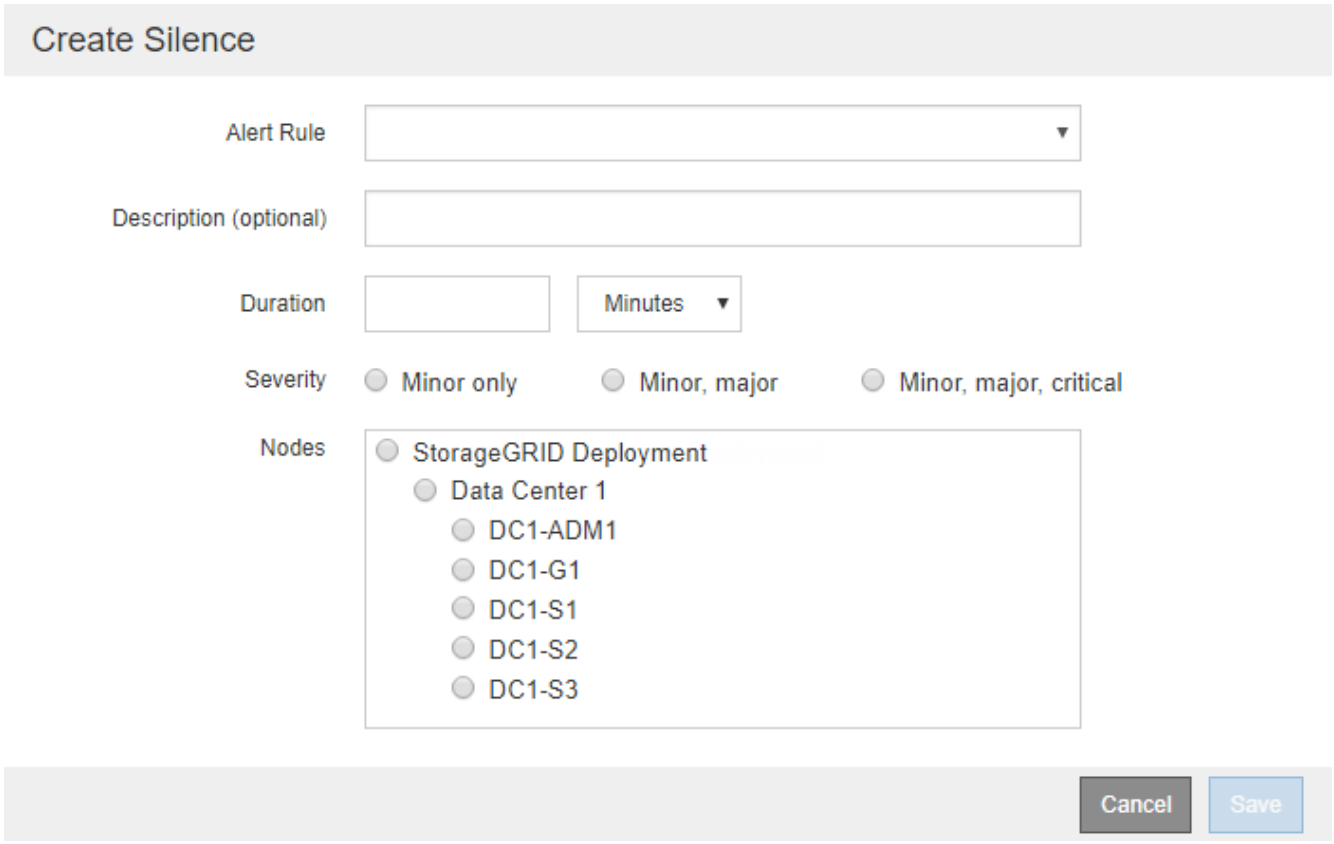
1. Selecione **ALERTAS** > **silêncios**.

   É apresentada a página silêncios.



2. Selecione **criar**.

   A caixa de diálogo criar Silêncio é exibida.



3. Selecione ou introduza as seguintes informações:

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

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

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

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

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

Informações relacionadas

"Configure o agente SNMP"

Referência de alertas

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

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

Alguns dos alertas padrão usam "Métricas Prometheus"o .

Alertas de dispositivo

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

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

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

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

Alertas de auditoria e syslog

Nome do alerta	Descrição
Os logs de auditoria estão sendo adicionados à fila na memória	O nó não pode enviar logs para o servidor syslog local e a fila na memória está sendo preenchida.

Nome do alerta	Descrição
Erro de encaminhamento do servidor syslog externo	O nó não pode encaminhar logs para o servidor syslog externo.
Fila de auditoria grande	A fila de discos para mensagens de auditoria está cheia. Se esta condição não for resolvida, as operações S3 ou Swift podem falhar.
Os logs estão sendo adicionados à fila no disco	O nó não pode encaminhar logs para o servidor syslog externo e a fila no disco está sendo preenchida.

Alertas de intervalo

Nome do alerta	Descrição
O balde FabricPool tem uma definição de consistência do balde não suportada	Um bucket do FabricPool usa o nível de consistência disponível ou de sites fortes, que não é suportado.
O bucket do FabricPool não tem configuração de controle de versão sem suporte	Um bucket do FabricPool tem controle de versão ou bloqueio de objeto S3 habilitado, que não são suportados.

Alertas do Cassandra

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

Nome do alerta	Descrição
O serviço de reparação Cassandra não está disponível	O serviço de reparação Cassandra não está disponível.
Corrupção da tabela Cassandra	Cassandra detetou corrupção de tabela. O Cassandra reinicia automaticamente se detetar corrupção de tabela.

Alertas do Cloud Storage Pool

Nome do alerta	Descrição
Erro de conetividade do Cloud Storage Pool	A verificação de integridade dos pools de armazenamento em nuvem detetou um ou mais erros novos.
Expiração da certificação de entidade final em qualquer lugar	O certificado de entidade final está prestes a expirar em qualquer lugar.

Alertas de replicação entre grades

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

Alertas DHCP

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

Depurar e rastrear alertas

Nome do alerta	Descrição
Impacto no desempenho de depuração	Quando o modo de depuração está ativado, o desempenho do sistema pode ser afetado negativamente.

Nome do alerta	Descrição
Configuração do traçado ativada	Quando a configuração de rastreamento está ativada, o desempenho do sistema pode ser afetado negativamente.

Alertas de e-mail e AutoSupport

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

Alertas de codificação de apagamento (EC)

Nome do alerta	Descrição
Falha no rebalanceamento EC	O procedimento de reequilíbrio CE falhou ou foi interrompido.
Falha na reparação EC	Um trabalho de reparação para dados EC falhou ou foi interrompido.
A reparação CE parou	Um trabalho de reparação para dados CE parou.
Erro de verificação de fragmentos codificados por apagamento	Fragmentos codificados por apagamento não podem mais ser verificados. Fragmentos corrompidos podem não ser reparados.

Expiração de alertas de certificados

Nome do alerta	Descrição
Expiração do certificado CA do Proxy Admin	Um ou mais certificados no pacote de CA do servidor proxy administrativo está prestes a expirar.
Expiração do certificado do cliente	Um ou mais certificados de cliente estão prestes a expirar.
Expiração do certificado de servidor global para S3 e Swift	O certificado de servidor global para S3 e Swift está prestes a expirar.

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

Alertas da rede de grelha

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

Alertas de federação de grade

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

Alertas de alta utilização ou alta latência

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

Alertas de federação de identidade

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

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

Nome do alerta	Descrição
Colocação de ILM inalcançável	Uma instrução de colocação em uma regra ILM não pode ser alcançada para determinados objetos.
Taxa de digitalização ILM baixa	A taxa de digitalização ILM é definida para menos de 100 objetos/segundo.

Alertas de servidor de gerenciamento de chaves (KMS)

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

Nome do alerta	Descrição
Expiração do certificado do servidor DE KMS	O certificado do servidor usado pelo KMS (Key Management Server) está prestes a expirar.
Falha de conetividade do servidor KMS	Um nó de dispositivo não pôde se conetar a um ou mais servidores no cluster do servidor de gerenciamento de chaves para seu site.

Alertas do balanceador de carga

Nome do alerta	Descrição
Conexões elevadas do balanceador de carga de solicitação zero	Uma porcentagem elevada de conexões para terminais do balanceador de carga desconetados sem a realização de solicitações.

Alertas de desvio do relógio local

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

Alertas de memória baixa ou de espaço reduzido

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

Nome do alerta	Descrição
Baixa sobreposição de marca d'água somente leitura	A substituição suave da marca d'água somente leitura do volume de armazenamento é menor do que a marca d'água mínima otimizada para um nó de armazenamento.
Baixa capacidade de disco raiz	O espaço disponível no disco raiz é baixo.
Baixa capacidade de dados do sistema	O espaço disponível para /var/local é baixo. Se esta condição não for resolvida, as operações S3 ou Swift podem falhar.
Espaço livre do diretório de baixa tmp	O espaço disponível no diretório /tmp é baixo.

Alertas de rede de nós ou nós

Nome do alerta	Descrição
Admin Network receber uso	O uso de receção na rede Admin é alto.
Utilização de transmissão de rede Admin	A utilização de transmissão na rede de administração é elevada.
Falha na configuração do firewall	Falha ao aplicar a configuração da firewall.
Endpoints de interface de gerenciamento no modo fallback	Todos os endpoints de interface de gerenciamento têm voltado para as portas padrão por muito tempo.
Erro de conetividade de rede do nó	Ocorreram erros durante a transferência de dados entre nós.
Erro de quadro de receção de rede do nó	Uma alta porcentagem dos quadros de rede recebidos por um nó teve erros.
Nó não sincronizado com o servidor NTP	O nó não está em sincronia com o servidor NTP (Network Time Protocol).
Nó não bloqueado com servidor NTP	O nó não está bloqueado para um servidor NTP (Network Time Protocol).
Rede de nós que não são do dispositivo inativa	Um ou mais dispositivos de rede estão inativos ou desconetados.
Link do utilitário de serviços para baixo na rede de administração	A interface do dispositivo para a rede de administração (eth1) está inativa ou desligada.
Link do utilitário de serviços para baixo na porta de rede Admin 1	A porta Admin Network 1 do aparelho está inativa ou desconetada.

Nome do alerta	Descrição
Link do utilitário de serviços para baixo na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 1	A porta de rede 1 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 2	A porta de rede 2 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 3	A porta de rede 3 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 4	A porta de rede 4 do aparelho está inativa ou desligada.
Link do dispositivo de armazenamento na rede Admin	A interface do dispositivo para a rede de administração (eth1) está inativa ou desligada.
Link do dispositivo de armazenamento na porta Admin Network 1	A porta Admin Network 1 do aparelho está inativa ou desconetada.
Ligação do dispositivo de armazenamento na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 1	A porta de rede 1 do aparelho está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 2	A porta de rede 2 do aparelho está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 3	A porta de rede 3 do aparelho está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 4	A porta de rede 4 do aparelho está inativa ou desligada.
Nó de storage não no estado de storage desejado	O serviço LDR em um nó de armazenamento não pode fazer a transição para o estado desejado devido a um erro interno ou problema relacionado ao volume
Utilização da ligação TCP	O número de conexões TCP neste nó está se aproximando do número máximo que pode ser rastreado.
Não é possível comunicar com o nó	Um ou mais serviços não respondem ou o nó não pode ser alcançado.

Nome do alerta	Descrição
Reinicialização inesperada do nó	Um nó reinicializou inesperadamente nas últimas 24 horas.

Alertas de objetos

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

Alertas de serviços de plataforma

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

Alertas de volume de storage

Nome do alerta	Descrição
O volume de armazenamento precisa de atenção	Um volume de armazenamento está offline e precisa de atenção.
O volume de storage precisa ser restaurado	Um volume de armazenamento foi recuperado e precisa ser restaurado.
Volume de armazenamento offline	Um volume de armazenamento está offline por mais de 5 minutos.
Tentativa de remontagem do volume de storage	Um volume de storage estava off-line e acionou uma remontagem automática. Isso pode indicar um problema de unidade ou erros de sistema de arquivos.

Nome do alerta	Descrição
Falha ao iniciar o reparo de dados replicados	O reparo de dados replicados para um volume reparado não pôde ser iniciado automaticamente.

Alertas dos serviços do StorageGRID

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

Alertas do locatário

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

Métricas de Prometheus comumente usadas

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

Você também obtenha uma lista completa de todas as métricaspode .

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

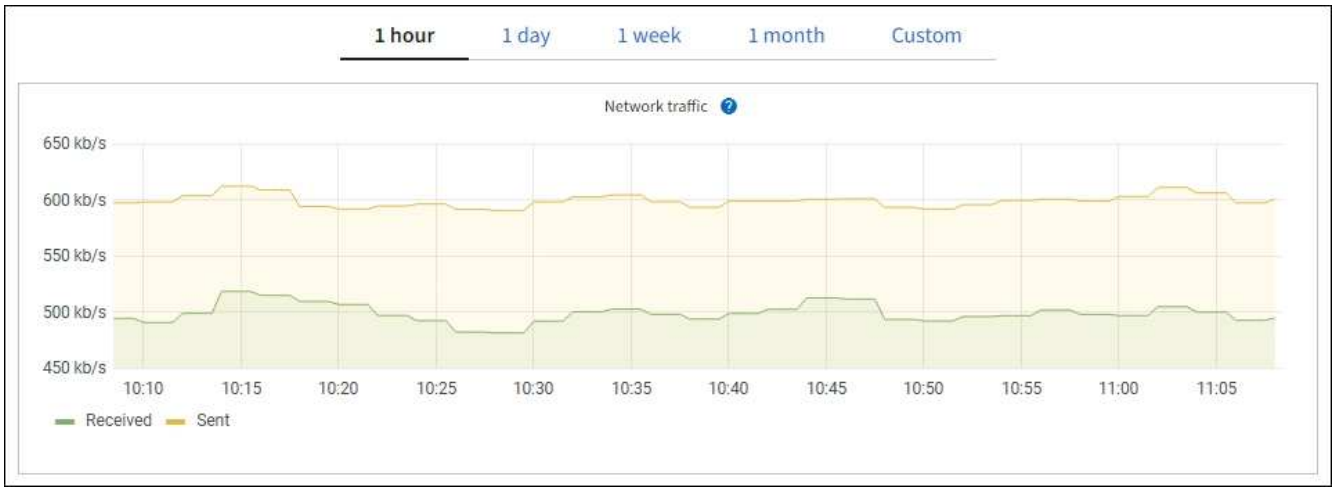
O que são métricas Prometheus?

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

Onde são usadas as métricas do Prometheus?

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

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



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

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

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

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

Lista das métricas mais comuns

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

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

alertmanager_notifications_failed_total

O número total de notificações de alerta com falha.

node_filesystem_avail_bytes

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

Node_Memory_MemAvailable_bytes

Campo de informações de memória MemAvailable_bytes.

node_network_carrier

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

node_network_receive_errs_total

Estatística do dispositivo de rede `receive_errs` .

node_network_transmit_errs_total

Estatística do dispositivo de rede `transmit_errs` .

StorageGRID_administrativamente_down

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

StorageGRID_appliance_compute_controller_hardware_status

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

StorageGRID_appliance_failed_disks

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

StorageGRID_appliance_storage_controller_hardware_status

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

StorageGRID_content_buckets_and_containers

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

StorageGRID_content_objects

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

StorageGRID_content_objects_lost

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

"Solucionar problemas de dados de objetos perdidos e ausentes"

StorageGRID_http_sessions_incoming_tented

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

StorageGRID_http_sessions_incoming_currently_established

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

StorageGRID_http_sessions_incoming_failed

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

StorageGRID_http_sessions_incoming_successful

O número total de sessões HTTP concluídas com êxito.

StorageGRID_ilm_awaiting_background_objects

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

StorageGRID_ilm_awaiting_client_evaluation_objects_per_second

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

StorageGRID_ilm_awaiting_client_objects

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

StorageGRID_ilm_awaiting_total_objects

O número total de objetos aguardando avaliação ILM.

StorageGRID_ilm_scan_objects_per_second

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

StorageGRID_ilm_scan_period_estimated_minutes

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

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

StorageGRID_load_balancer_endpoint_cert_expiry_time

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

StorageGRID_metadata_queries_average_latency_milésimos de segundo

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

StorageGRID_network_received_bytes

A quantidade total de dados recebidos desde a instalação.

StorageGRID_network_transmitted_bytes

A quantidade total de dados enviados desde a instalação.

StorageGRID_node_cpu_utilization_percentage

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

StorageGRID_ntp_chosen_time_source_offset_milissegundos

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

StorageGRID_ntp_locked

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

storagegrid_s3_data_transfers_bytes_ingested

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

storagegrid_s3_data_transfers_bytes_retrieved

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

storagegrid_s3_operations_failed

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

storagegrid_s3_operations_successful

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

storagegrid_s3_operations_unauthorized

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

StorageGRID_servercertificate_management_interface_cert_expiry_days

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

StorageGRID_servercertificate_storage_api_endpoints_cert_expiry_days

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

StorageGRID_service_cpu_seconds

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

StorageGRID_service_memory_usage_bytes

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

StorageGRID_service_network_received_bytes

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

StorageGRID_service_network_transmitted_bytes

A quantidade total de dados enviados por este serviço.

StorageGRID_service_restarts

O número total de vezes que o serviço foi reiniciado.

StorageGRID_service_runtime_seconds

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

StorageGRID_service_uptime_seconds

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

StorageGRID_storage_state_current

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

- 10: Offline
- 15: Manutenção

- 20 - somente leitura
- 30 - Online

StorageGRID_storage_status

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

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

StorageGRID_storage_utilization_data_bytes

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

StorageGRID_storage_utilization_metadata_allowed_bytes

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

StorageGRID_storage_utilization_metadata_bytes

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

StorageGRID_storage_utilization_total_space_bytes

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

StorageGRID_storage_utilization_usable_space_bytes

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

StorageGRID_swift_data_transfers_bytes_ingerido

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

StorageGRID_swift_data_transfers_bytes_recuperados

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

StorageGRID_swift_operations_failed

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

StorageGRID_swift_operations_successful

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

StorageGRID_swift_operations_unauthorized

O número total de operações Swift falhadas que são o resultado de uma falha de autorização (códigos de

status HTTP 401, 403, 405).

StorageGRID_tenant_usage_data_bytes
O tamanho lógico de todos os objetos para o locatário.

StorageGRID_tenant_use_object_count
O número de objetos para o inquilino.

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

Obtenha uma lista de todas as métricas

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

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

Referência de ficheiros de registo

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"
- "Sobre o bycast.log"

> Os detalhes fornecidos para cada tipo de log são apenas para referência. Os registos destinam-se à resolução de problemas avançada por suporte técnico. Técnicas avançadas que envolvem a reconstrução do histórico de problemas usando os logs de auditoria e os arquivos de log do aplicativo estão além do escopo dessas instruções.

Aceder aos registos

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

1. Introduza o seguinte comando: `ssh admin@grid_node_IP`
2. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

3. Digite o seguinte comando para mudar para root: `su -`
4. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Exporte logs para o servidor syslog

Exportar os logs para o servidor syslog fornece estes recursos:

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

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

Categorias de ficheiros de registo

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

Localização do arquivo	Descrição
auditoria	Mensagens de auditoria geradas durante a operação normal do sistema.
base-os-logs	Informações básicas do sistema operacional, incluindo versões de imagem StorageGRID.
pacotes	Informações de configuração global (pacotes).
cassandra	Informações do banco de dados Cassandra e Registros de reparo do Reaper.
ce	Informações de VCSs sobre o nó atual e as informações de grupo EC por ID de perfil.
grelha	Logs gerais de grade incluindo debug (`bycast.log`) e `servermanager` logs.
grid.json	Arquivo de configuração de grade compartilhado em todos os nós. Além disso, `node.json` é específico para o nó atual.
grupos	A alta disponibilidade agrupa métricas e logs.
instale	`Gdu-server` e instalar logs.
Lambda-árbitro	Logs relacionados à solicitação de proxy S3 Select.

Localização do arquivo	Descrição
lumberjack.log	Depurar mensagens relacionadas à coleção de logs.
Métricas	Logs de serviço para Grafana, Jaeger, nó exportador e Prometheus.
miscd	Registos de acesso e erro incorretos.
mysql	A configuração do banco de dados MariaDB e logs relacionados.
rede	Logs gerados por scripts relacionados à rede e pelo serviço Dynip.
nginx	Arquivos e logs de configuração de federação de grade e balanceador de carga. Também inclui logs de tráfego do Grid Manager e do Tenant Manager.
nginx-gw	• `access.log`: O Gerenciador de Grade e o Gerenciador do Locatário solicitam mensagens de log. ◦ Essas mensagens são prefixadas com `mgmt:` quando exportadas usando syslog. ◦ O formato destas mensagens de registo é `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: Solicitações de replicação entre grade de entrada. ◦ Essas mensagens são prefixadas com `cgr:` quando exportadas usando syslog. ◦ O formato destas mensagens de registo é `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`: Solicitações S3 e Swift para terminais do balanceador de carga. ◦ Essas mensagens são prefixadas com `endpoint:` quando exportadas usando syslog. ◦ O formato destas mensagens de registo é `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: Relacionado com o novo alerta de verificação de DNS.
ntp	Ficheiro de configuração NTP e registos.
Objetos órfãos	Logs relativos a objetos órfãos.

Localização do arquivo	Descrição
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.
ssh	Logs relacionados à configuração e serviço SSH.
snmp	Configuração do agente SNMP usada 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.
sincronizar-recuperação-pacote	Relacionado a manter a consistência do pacote de recuperação mais recente em todos os nós de administração e nós de storage que hospedam o serviço ADC.

Registos do software StorageGRID

Você pode usar logs do StorageGRID para solucionar problemas.

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

Registos gerais do StorageGRID

Nome do ficheiro	Notas	Encontrado em
/var/local/log/bycast.log	O arquivo primário de solução de problemas do StorageGRID. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***Site*** > ***Node*** > **SSM** > **Eventos**.	Todos os nós

Nome do ficheiro	Notas	Encontrado em
/var/local/log/bycast-err.log	Contém um subconjunto de `bycast.log` (mensagens com ERRO de gravidade e CRÍTICO). Mensagens CRÍTICAS também são exibidas no sistema. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***Site*** > ***Node*** > **SSM** > **Eventos**.	Todos os nós
/var/local/core/	Contém quaisquer arquivos de despejo de núcleo criados se o programa terminar anormalmente. As possíveis causas incluem falhas de asserção, violações ou tempos limite de thread. **Nota**: O arquivo `` `/var/local/core/kexec_cmd `` geralmente existe em nós de appliance e não indica um erro.	Todos os nós

Registos relacionados com cifras

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

Logs de federação de grade

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

Registos NMS

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

Logs do Server Manager

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

Nome do ficheiro	Notas	Encontrado em
/var/local/log/gridstat.errlog	Ficheiro de registo para a GUI do Gestor de servidor.	Todos os nós

Registos de serviços do StorageGRID

Nome do ficheiro	Notas	Encontrado em
/var/local/log/acct.errlog		Nós de storage executando o serviço ADC
/var/local/log/adc.errlog	Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de storage executando o serviço ADC
/var/local/log/ams.errlog		Nós de administração
/var/local/log/cassandra/system.log	Informações para o armazenamento de metadados (banco de dados Cassandra) que podem ser usadas se ocorrerem problemas ao adicionar novos nós de armazenamento ou se a tarefa de reparo nodetool for interrompida.	Nós de storage
/var/local/log/cassandra-reaper.log	Informações para o serviço Cassandra Reaper, que executa reparos dos dados no banco de dados Cassandra.	Nós de storage
/var/local/log/cassandra-reaper.errlog	Informações de erro para o serviço Cassandra Reaper.	Nós de storage
/var/local/log/chunk.errlog		Nós de storage
/var/local/log/cmn.errlog		Nós de administração
/var/local/log/cms.errlog	Esse arquivo de log pode estar presente em sistemas que foram atualizados a partir de uma versão mais antiga do StorageGRID. Ele contém informações legadas.	Nós de storage
/var/local/log/dds.errlog		Nós de storage

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

Nome do ficheiro	Notas	Encontrado em
/var/local/log/miscd/*.log	Contém logs para o serviço MISCd (Information Service Control Daemon), que fornece uma interface para consultar e gerenciar serviços em outros nós e para gerenciar configurações ambientais no nó, como consultar o estado dos serviços em execução em outros nós.	Todos os nós
/var/local/log/nginx/*.log	Contém logs para o serviço nginx, que atua como um mecanismo de autenticação e comunicação segura para vários serviços de grade (como Prometheus e Dynip) para poder falar com serviços em outros nós através de APIs HTTPS.	Todos os nós
/var/local/log/nginx-gw/*.log	Contém logs gerais relacionados ao serviço nginx-gw, incluindo logs de erro e logs para as portas de administração restritas em nós de administração.	Nós de administração e nós de gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contém registos de acesso relacionados com o tráfego de replicação entre redes.	Nós de administração, nós de gateway ou ambos, com base na configuração da federação de grade. Apenas encontrado na grelha de destino para replicação entre grelha.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contém logs de acesso para o serviço Load Balancer, que fornece balanceamento de carga de tráfego S3 de clientes para nós de storage.	Nós de administração e nós de gateway
/var/local/log/persistence*	Contém logs para o serviço Persistence, que gerencia arquivos no disco raiz que precisam persistir durante uma reinicialização.	Todos os nós
/var/local/log/prometheus.log	Para todos os nós, contém o log de serviço de exportador de nós e o log de serviço de métricas ade-exportador. For Admin node, também contém logs para os serviços Prometheus e Alert Manager.	Todos os nós

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

Informações relacionadas

- "Sobre o bycast.log"
- "USE A API REST DO S3"

Logs de implantação e manutenção

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

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

Nome do ficheiro	Notas	Encontrado em
/var/local/log/expansion-progress.log	Criado durante operações de expansão. Contém um Registro dos eventos de expansão.	Nós de storage
/var/local/log/pa-move.log	Criado durante a execução `pa-move.sh` do script.	Nó de administração principal
/var/local/log/pa-move-new_pa.log	Criado durante a execução `pa-move.sh` do script.	Nó de administração principal
/var/local/log/pa-move-old_pa.log	Criado durante a execução `pa-move.sh` do script.	Nó de administração principal
/var/local/log/gdu-server.log	Criado pelo serviço GDU. Contém eventos relacionados aos procedimentos de provisionamento e manutenção gerenciados pelo nó de administração principal.	Nó de administração principal
/var/local/log/send_admin_hw.log	Criado durante a instalação. Contém informações de depuração relacionadas às comunicações de um nó com o nó de administração principal.	Todos os nós
/var/local/log/upgrade.log	Criado durante a atualização de software. Contém um registo dos eventos de atualização de software.	Todos os nós

Sobre o bycast.log

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

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

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

Rotação de ficheiros para bycast.log

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

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

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

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

> Se um arquivo de log tiver sido compactado, você não deve descompactá-lo para o mesmo local em que foi escrito. A descompressão do arquivo para o mesmo local pode interferir com os scripts de rotação de log.

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

Informações relacionadas

"Colete arquivos de log e dados do sistema"

Mensagens em bycast.log

As mensagens em `bycast.log` são escritas pelo ADE (Asynchronous Distributed Environment). ADE é o ambiente de tempo de execução usado pelos serviços de cada nó de grade.

Exemplo de mensagem ADE:

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

As mensagens ADE contêm as seguintes informações:

Segmento de mensagens	Valor no exemplo
ID de nó	12455685
ID do processo ADE	0357819531
Nome do módulo	SVMR
Identificador da mensagem	EVHR
Hora do sistema UTC	2019-05-05T27T17:10:29,784677 (AAAA-MM-DDTHH:MM:SS.UUUUUUUUUUUU)
Nível de gravidade	ERRO
Número de rastreamento interno	0906
Mensagem	SVMR: A verificação do estado do volume 3 falhou com o motivo "TOUT"

Severidades da mensagem em bycast.log

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

Por exemplo:

- **AVISO** — ocorreu um evento que deve ser gravado. A maioria das mensagens de log estão nesse nível.
- **AVISO** — ocorreu uma condição inesperada.
- **ERROR** — ocorreu Um erro importante que afetará as operações.
- **CRÍTICO** — ocorreu uma condição anormal que parou as operações normais. Você deve abordar a condição subjacente imediatamente.

Códigos de erro em `bycast.log`

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

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

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

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

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

Número de erro	Código de erro	Significado
022	EINVAL	Argumento inválido
023	ENFILE	Estouro da tabela de arquivos
024	EMFILE	Demasiados ficheiros abertos
025	ENOTTY	Não é uma máquina de escrever
026	ETXTBSY	Ficheiro de texto ocupado
027	EFBIG	Ficheiro demasiado grande
028	ENOSPC	Nenhum espaço restante no dispositivo
029	ESPIPE	Procura ilegal
030	EROFS	Sistema de arquivos somente leitura
031	EMLINK	Demasiados links
032	EPIPE	Tubo quebrado
033	EDOM	Argumento de matemática fora de domínio do func
034	ERANGE	Resultado matemático não representável
035	EDEADLK	O bloqueio de recursos ocorreria
036	ENAMETOOLONG	Nome do ficheiro demasiado longo
037	ENOLCK	Não existem bloqueios de registo disponíveis
038	ENOSYS	Função não implementada
039	ENOTEMPTY	O diretório não está vazio
040	ELOOP	Muitos links simbólicos encontrados
041		
042	ENOMSG	Nenhuma mensagem do tipo desejado
043	EIDRM	Identificador removido

Número de erro	Código de erro	Significado
044	ECHRNG	Número do canal fora do intervalo
045	EL2NSYNC	Nível 2 não sincronizado
046	EL3HLT	Nível 3 interrompido
047	EL3RST	Reposição do nível 3
048	ELNRNG	Número da ligação fora do intervalo
049	EUNATCH	Controlador de protocolo não anexado
050	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

Número de erro	Código de erro	Significado
066	EREMOTE	O objeto é remoto
067	ENOLINK	O link foi cortado
068	EADV	Erro de anúncio
069	ESRMNT	Erro Srmount
070	ECOMM	Erro de comunicação no envio
071	EPROTO	Erro de protocolo
072	EMULTIHOP	Tentativa de Multihop
073	EDOTDOT	Erro específico do RFS
074	EBADMSG	Não é uma mensagem de dados
075	EOVERFLOW	Valor demasiado grande para o tipo de dados definido
076	ENOTUNIQ	Nome não exclusivo na rede
077	EBADFD	Descritor de arquivo em mau estado
078	EREMCHG	Endereço remoto alterado
079	ELIBACC	Não é possível acessar uma biblioteca compartilhada necessária
080	ELIBBAD	Acessando uma biblioteca compartilhada corrompida
081	ELIBSCN	
082	ELIBMAX	Tentando vincular em muitas bibliotecas compartilhadas
083	ELIBEXEC	Não é possível executar uma biblioteca compartilhada diretamente
084	EILSEQ	Sequência de bytes ilegal
085	ERESTART	A chamada do sistema interrompida deve ser reiniciada

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

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

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

Configurar destinos de mensagens de auditoria e de log

Considerações para usar um servidor syslog externo

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

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

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

Quando usar um servidor syslog externo

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

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

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

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

Como configurar um servidor syslog externo

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

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

- **Certificados de CA do servidor**: Um ou mais certificados de CA confiáveis para verificar o servidor syslog externo na codificação PEM. Se omitido, o certificado padrão da CA de grade será usado.
- **Certificado de cliente**: O certificado de cliente para autenticação para o servidor syslog externo na codificação PEM.
- **Chave privada do cliente**: Chave privada para o certificado do cliente na codificação PEM.

> Se você usar um certificado de cliente, você também deve usar uma chave privada de cliente. Se você fornecer uma chave privada criptografada, você também deve fornecer a senha. Não há benefício significativo de segurança ao usar uma chave privada criptografada porque a chave e a senha devem ser armazenadas; usar uma chave privada não criptografada, se disponível, é recomendado para simplificar.

Como estimar o tamanho do servidor syslog externo

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

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

Use S3 operações por segundo em fórmulas de estimativa

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

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

Fórmulas de estimativa para logs de auditoria

Se você não tiver informações sobre sua carga de trabalho S3 além do número de S3 operações por segundo que sua grade deve suportar, você pode estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, partindo do pressuposto de que você deixa os níveis de auditoria definidos para os valores padrão (todas as categorias definidas como normal, exceto armazenamento, que está definido como erro):

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

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

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

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

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

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

Se você puder determinar valores para P e K, poderá estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, partindo do pressuposto de que você deixa os níveis de auditoria definidos para os padrões (todas as categorias definidas como normal, exceto armazenamento, que está definido como erro):

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

Por exemplo, se sua grade for dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts, e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 1.500 mensagens syslog por segundo e

deve ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de aproximadamente 1 MB por segundo.

Fórmulas de estimativa para níveis de auditoria não padrão

As fórmulas fornecidas para logs de auditoria assumem o uso de configurações de nível de auditoria padrão (todas as categorias definidas como normal, exceto armazenamento, que é definido como erro). Fórmulas detalhadas para estimar a taxa e o tamanho médio das mensagens de auditoria para configurações de nível de auditoria não padrão não estão disponíveis. No entanto, a tabela a seguir pode ser usada para fazer uma estimativa aproximada da taxa; você pode usar a fórmula de tamanho médio fornecida para logs de auditoria, mas esteja ciente de que é provável que isso resulte em uma estimativa excessiva porque as mensagens de auditoria "extra" são, em média, menores do que as mensagens de auditoria padrão.

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

Fórmulas de estimativa para eventos de segurança

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

Fórmulas de estimativa para logs de aplicativos

Se você não tiver informações sobre sua carga de trabalho S3 além do número de S3 operações por segundo que sua grade deve suportar, você pode estimar o volume de Registros de aplicativos que seu servidor syslog externo precisará lidar com as seguintes fórmulas:

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

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

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

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

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

Exemplo de estimativas de dimensionamento

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

- Replicação
- Codificação de apagamento

Se você usar a replicação para proteção de dados

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

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

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

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

Assim, por exemplo, se sua grade é dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 1800 Registros de aplicativos por segundo e receberá (e normalmente armazenará) dados de aplicativos a uma taxa de 0,5 MB por segundo.

Se você usar codificação de apagamento para proteção de dados

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

Deixe K representar o tamanho médio da soma dos S3 nomes de conta, S3 bucket e S3 key. Suponha que o

nome da conta S3 seja sempre my-S3-account (13 bytes), buckets têm nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes), e objetos têm chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então K tem um valor de 90 (13-13-28-36).

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

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

Assim, por exemplo, se sua grade é dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 2.250 Registros de aplicativos por segundo e deve ser capaz de receber (e normalmente armazenar) dados de aplicativos a uma taxa de 0,6 MB por segundo.

Configurar mensagens de auditoria e servidor syslog externo

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

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

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

Antes de começar

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

Alterar os níveis de mensagens de auditoria

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

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

Esses padrões se aplicam se você instalou inicialmente o StorageGRID usando a versão 10,3 ou posterior. Se você usou inicialmente uma versão anterior do StorageGRID, o padrão para todas as categorias é definido como normal.

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

Passos

1. Selecione **CONFIGURATION** > **Monitoring** > **Audit and syslog Server**.
2. Para cada categoria de mensagem de auditoria, selecione um nível de auditoria na lista suspensa:

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

As mensagens incluídas para qualquer nível particular incluem aquelas que seriam registradas nos níveis

mais altos. Por exemplo, o nível normal inclui todas as mensagens de erro.

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

3. Selecione **Guardar**.

   Um banner verde indica que sua configuração foi salva.

Definir cabeçalhos de solicitação HTTP

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

Passos

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

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

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

   Quando cabeçalhos HTTP são encontrados em uma solicitação, eles são incluídos na mensagem de auditoria sob o campo HTRH.

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

3. Selecione **Guardar**

   Um banner verde indica que sua configuração foi salva.

Use um servidor syslog externo

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

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

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

Insira as informações do syslog

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

Passos

1. Na página servidor de auditoria e syslog, selecione **Configurar servidor syslog externo**. Ou, se tiver configurado anteriormente um servidor syslog externo, selecione **Editar servidor syslog externo**.

   O assistente Configurar servidor syslog externo é exibido.

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

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

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

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

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

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

7. Selecione **continuar**.

Gerenciar o conteúdo do syslog

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

Passos

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

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

◦ * Enviar logs de acesso*: Envia logs de acesso HTTP para solicitações externas ao Gerenciador de Grade, Gerenciamento do locatário, pontos de extremidade do balanceador de carga configurados e solicitações de federação de grade de sistemas remotos.

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

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

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

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

Gravidade	Descrição
Passagem	Cada mensagem enviada para o syslog externo para ter o mesmo valor de gravidade que quando foi registrada localmente no nó: • Para logs de auditoria, a gravidade é "info". • Para eventos de segurança, os valores de gravidade são gerados pela distribuição Linux nos nós. • Para logs de aplicativos, as severidades variam entre "info" e "notice", dependendo do problema. Por exemplo, adicionar um servidor NTP e configurar um grupo HA dá um valor de "info", enquanto parar intencionalmente o serviço SSM ou RSM dá um valor de "notice". • Para os logs de acesso, a gravidade é "INFO".
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

Gravidade	Descrição
6	Informativo: Mensagens informativas
7	Debug: Mensagens no nível de depuração

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

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

Instalação	Descrição
Passagem	Cada mensagem enviada para o syslog externo para ter o mesmo valor de instalação que quando foi registrada localmente no nó: • Para logs de auditoria, a instalação enviada para o servidor syslog externo é "local7". • Para eventos de segurança, os valores das instalações são gerados pela distribuição linux nos nós. • Para logs de aplicativos, os logs de aplicativos enviados para o servidor syslog externo têm os seguintes valores de instalação: ◦ `bycast.log`: usuário ou daemon ◦ `bycast-err.log`: usuário, daemon, local3 ou local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • Para logs de acesso, a instalação enviada para o servidor syslog externo é "local0".
0	kern (mensagens do kernel)
1	utilizador (mensagens no nível do utilizador)
2	e-mail
3	daemon (daemons do sistema)
4	auth (mensagens de segurança/autorização)
5	syslog (mensagens geradas internamente pelo syslogd)

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

3. Selecione **continuar**.

Enviar mensagens de teste

Antes de começar a usar um servidor syslog externo, você deve solicitar que todos os nós da grade enviem mensagens de teste para o servidor syslog externo. Você deve usar essas mensagens de teste para ajudá-lo a validar toda a infraestrutura de coleta de logs antes de se comprometer a enviar dados para o servidor syslog externo.

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

Passos

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

   Um banner verde indica que a configuração foi salva.

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

   Os resultados do teste aparecem continuamente na página até que você pare o teste. Enquanto o teste estiver em andamento, suas mensagens de auditoria continuam sendo enviadas para os destinos configurados anteriormente.

3. Se você receber algum erro, corrija-o e selecione **Enviar mensagens de teste** novamente.

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

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

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

6. Selecione **Parar e terminar**.

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

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

Selecione destinos de informações de auditoria

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

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

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

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

Passos

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

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

Opção	Descrição
Somente nós locais (padrão)	As mensagens de auditoria, os logs de eventos de segurança e os logs de aplicativos não são enviados para os nós de administração. Em vez disso, eles são salvos apenas nos nós que os geraram ("o nó local"). As informações de auditoria geradas em cada nó local são armazenadas no `/var/local/log/localaudit.log`. **Nota**: O StorageGRID remove periodicamente logs locais em uma rotação para liberar espaço. Quando o arquivo de log de um nó atinge 1 GB, o arquivo existente é salvo e um novo arquivo de log é iniciado. O limite de rotação para o log é de 21 arquivos. Quando a versão 22nd do arquivo de log é criada, o arquivo de log mais antigo é excluído. Em média, cerca de 20 GB de dados de log são armazenados em cada nó.
Nós de administração/nós locais	As mensagens de auditoria são enviadas para o log de auditoria nos nós de administração, e os logs de eventos de segurança e de aplicativos são armazenados nos nós que as geraram. As informações de auditoria são armazenadas nos seguintes arquivos: • Nós de administração (primários e não primários): `/var/local/audit/export/audit.log` • Todos os nós: O `/var/local/log/localaudit.log` arquivo está normalmente vazio ou ausente. Ele pode conter informações secundárias, como uma cópia adicional de algumas mensagens.
Servidor syslog externo	As informações de auditoria são enviadas para um servidor syslog externo e salvas nos nós locais (`/var/local/log/localaudit.log`). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é ativada depois de ter configurado um servidor syslog externo.
Nó de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria (`/var/local/audit/export/audit.log`) em nós de administração e as informações de auditoria são enviadas para o servidor syslog externo e salvas no nó local (`/var/local/log/localaudit.log`). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é ativada depois de ter configurado um servidor syslog externo.

2. Selecione **Guardar**.

É apresentada uma mensagem de aviso.

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

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

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

Utilize a monitorização SNMP

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

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

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

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

Armadilhas

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

Traps são suportados em todas as três versões do SNMP.

Informa

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

As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de intercetação e informação são enviadas nos seguintes casos:

- Um alerta padrão ou personalizado é acionado em qualquer nível de gravidade. Para suprimir notificações SNMP para um alerta, tem de "configure um silêncio"o alertar. As notificações de alerta são enviadas pelo

"Nó Admin. Remetente preferido".

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

Suporte à versão SNMP

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

	SNMPv1	SNMPv2c	SNMPv3
Consultas (OBTER e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	Cadeia de carateres da comunidade	Cadeia de carateres da comunidade	Utilizador do modelo de segurança baseado no utilizador (USM)
Notificações (ARMADILHA e INFORMAÇÃO)	Apenas armadilhas	Armadilhas e informações	Armadilhas e informações
Autenticação de notificação	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Utilizador USM para cada destino de armadilha

Limitações

- O StorageGRID suporta acesso MIB somente leitura. O acesso de leitura e gravação não é suportado.
- Todos os nós na grade recebem a mesma configuração.
- SNMPv3: O StorageGRID não suporta o modo de suporte de transporte (TSM).
- SNMPv3: O único protocolo de autenticação suportado é SHA (HMAC-SHA-96).
- SNMPv3: O único protocolo de privacidade suportado é AES.

Configure o agente SNMP

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

Antes de começar

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

Sobre esta tarefa

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

Todos os nós na grade usam a mesma configuração SNMP.

Especifique a configuração básica

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

Passos

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

   A página do agente SNMP é exibida.

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

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

Introduza cadeias de carateres da comunidade

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

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

Passos

1. Para **comunidade somente leitura**, opcionalmente, insira uma cadeia de carateres comunitária para permitir acesso MIB somente leitura em endereços de agentes IPv4 e IPv6.

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

   Cada string de comunidade pode ter no máximo 32 carateres e não pode conter carateres de espaço em branco.

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

   Até cinco cordas são permitidas.

Crie destinos de armadilha

Use a guia Trap Destinations (destinos de intercetação) na seção Other configurations (outras configurações) para definir um ou mais destinos para o StorageGRID trap (trap de intercetação) ou para informar notificações. Quando você ativa o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

Passos

1. Para o campo **Default trap Community** (comunidade de trap padrão), insira opcionalmente a string de comunidade padrão que você deseja usar para destinos de trap SNMPv1 ou SNMPv2.

   Conforme necessário, você pode fornecer uma string de comunidade ("personalizada") diferente quando você define um destino de armadilha específico.

   A comunidade de trap padrão pode ter no máximo 32 carateres e não pode conter carateres de espaço em branco.

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

SNMPv1

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

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

SNMPv2c

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

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

SNMPv3

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

Campo	Descrição
Tipo	Se o destino será usado para armadilhas ou informações.
Host	Um endereço IPv4 ou IPv6 ou FQDN para receber a armadilha.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo padrão de intercetação SNMP, a menos que você precise usar TCP.
Utilizador USM	O utilizador USM que será utilizado para autenticação. • Se selecionou **Trap**, apenas são apresentados utilizadores USM sem IDs de motor autoritativas. • Se selecionou **inform**, apenas são apresentados utilizadores USM com IDs de motor autoritativas. • Se não forem apresentados utilizadores: i. Crie e salve o destino da armadilha. ii. Vá para Crie utilizadores USM e crie o usuário. iii. Regresse ao separador Trap Destinations (destinos da armadilha), selecione o destino guardado na tabela e selecione **Edit** (Editar). iv. Selecione o utilizador.

5. Selecione **criar**.

   O destino da armadilha é criado e adicionado à tabela.

Criar endereços de agente

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

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

Passos

1. Selecione **criar**.
2. Introduza as seguintes informações.

Campo	Descrição
Protocolo da Internet	Se esse endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se esse endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Qual rede StorageGRID o agente ouvirá. • Redes Grid, Admin e Client: O agente SNMP escutará consultas em todas as três redes. • Rede de rede • Rede de administração • Rede de clientes **Nota**: Se você usar a rede do cliente para dados inseguros e criar um endereço de agente para a rede do cliente, esteja ciente de que o tráfego SNMP também será inseguro.
Porta	Opcionalmente, o número da porta que o agente SNMP deve ouvir. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. **Nota**: Quando você salva o agente SNMP, o StorageGRID abre automaticamente as portas de endereço do agente no firewall interno. Você deve garantir que todos os firewalls externos permitam acesso a essas portas.

3. Selecione **criar**.

   O endereço do agente é criado e adicionado à tabela.

Crie utilizadores USM

Se estiver a utilizar o SNMPv3, utilize o separador utilizadores USM na secção outras configurações para definir os utilizadores USM que estão autorizados a consultar o MIB ou a receber traps e informações.

SNMPv3 *inform* destinos devem ter usuários com IDs de motor. SNMPv3 *trap* destino não pode ter usuários com IDs de motor.

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

Passos

1. Selecione **criar**.
2. Introduza as seguintes informações.

Campo	Descrição
Nome de utilizador	Um nome exclusivo para este utilizador USM. Os nomes de usuário podem ter um máximo de 32 carateres e não podem conter carateres de espaço em branco. O nome de usuário não pode ser alterado depois que o usuário é criado.
Acesso MIB somente leitura	Se selecionado, este utilizador deverá ter acesso apenas de leitura à MIB.
ID do motor autoritário	Se este utilizador for utilizado num destino de informação, o ID de mecanismo autorizado para este utilizador. Insira 10 a 64 carateres hexadecimais (5 a 32 bytes) sem espaços. Este valor é necessário para utilizadores USM que serão selecionados em destinos de armadilha para informação. Este valor não é permitido para utilizadores USM que serão selecionados em destinos de armadilha para armadilhas. **Nota**: Este campo não é mostrado se você selecionou **Acesso MIB somente leitura** porque os usuários USM que têm acesso MIB somente leitura não podem ter IDs de mecanismo.
Nível de segurança	O nível de segurança para o utilizador USM: • **AuthPriv**: Este usuário se comunica com autenticação e privacidade (criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe, um protocolo de privacidade e uma palavra-passe. • **AuthNoPriv**: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe.
Protocolo de autenticação	Sempre definido como SHA, que é o único protocolo suportado (HMAC-SHA-96).
Palavra-passe	A senha que este usuário usará para autenticação.
Protocolo de privacidade	Mostrado apenas se você selecionou **authPriv** e sempre definido como AES, que é o único protocolo de privacidade suportado.
Palavra-passe	Mostrado apenas se você selecionou **authPriv**. A senha que este usuário usará para privacidade.

3. Selecione **criar**.

   O utilizador USM é criado e adicionado à tabela.

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

A nova configuração do agente SNMP fica ativa.

Atualize o agente SNMP

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

Antes de começar

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

Sobre esta tarefa

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

Passos

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

   A página do agente SNMP é exibida.

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

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

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

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

   c. Opcionalmente, marque ou desmarque a caixa de seleção **Ativar traps de autenticação** para controlar se o agente SNMP do StorageGRID envia traps de autenticação quando recebe mensagens de protocolo autenticadas incorretamente.
4. Se você usar SNMPv1 ou SNMPv2c, opcionalmente, atualize ou adicione uma comunidade **somente leitura** na seção cadeias de Comunidade.
5. Para atualizar destinos de intercetação, selecione a guia destinos de intercetação na seção outras configurações.

   Utilize este separador para definir um ou mais destinos para o StorageGRID trap ou para informar notificações. Quando você ativa o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

   Para obter detalhes sobre o que introduzir, "Criar destinos de armadilha"consulte .

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

     Se você remover a comunidade de trap padrão, primeiro deve garantir que todos os destinos de trap

existentes usem uma cadeia de carateres de comunidade personalizada.

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

6. Para atualizar endereços de agentes, selecione a guia endereços de agentes na seção outras configurações.

   Use esta guia para especificar um ou mais "endereços de escuta". Estes são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

   Para obter detalhes sobre o que introduzir, "Criar endereços de agente"consulte .

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

7. Para atualizar os utilizadores USM, selecione o separador utilizadores USM na secção outras configurações.

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

   Para obter detalhes sobre o que introduzir, "Crie utilizadores USM"consulte .

   - Para adicionar um utilizador USM, selecione **criar**.
   - Para editar um utilizador USM, selecione o botão de opção e selecione **Edit**.

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

     > Se você adicionar ou remover um ID de mecanismo autoritário de um usuário e esse usuário estiver selecionado atualmente para um destino, você deverá editar ou remover o destino. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

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

     > Se o usuário removido estiver selecionado atualmente para um destino de armadilha, você deve editar ou remover o destino. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

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

8. Quando tiver atualizado a configuração do agente SNMP, selecione **Save**.

Acesse arquivos MIB

Os arquivos MIB contêm definições e informações sobre as propriedades dos recursos e

serviços gerenciados para os nós em sua grade. Você pode acessar arquivos MIB que definem os objetos e notificações do StorageGRID. Esses arquivos podem ser úteis para monitorar sua grade.

Consulte "Utilize a monitorização SNMP" para obter mais informações sobre ficheiros SNMP e MIB.

Acesse arquivos MIB

Siga estes passos para aceder aos ficheiros MIB.

Passos

1. Selecione **CONFIGURATION** > **Monitoring** > **SNMP Agent**.
2. Na página do agente SNMP, selecione o arquivo que deseja baixar:
   - **NetApp-StorageGRID-MIB.txt**: Define a tabela de alertas e notificações (traps) acessíveis em todos os nós de administração.
   - * ES-NetApp-06-MIB.mib*: Define objetos e notificações para dispositivos baseados em série e.
   - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com interface BMC.

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

3. Para extrair os OIDs StorageGRID do arquivo MIB:

   a. Obtenha o OID da raiz do MIB do StorageGRID:

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

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

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

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

O `snmptranslate` comando tem muitas opções que são úteis para explorar o MIB. Este comando está disponível em qualquer nó StorageGRID.

Conteúdo do arquivo MIB

Todos os objetos estão sob o OID StorageGRID.

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

Objetos MIB

Nome do objeto	Código Objeto (OID)	Descrição
ActiveAlertCount		O número de alertas ativos na activeAlertTable.
ActiveAlertTable		Uma tabela de alertas ativos no StorageGRID.
ActiveAlertId		O ID do alerta. Apenas exclusivo no conjunto atual de alertas ativos.
ActiveAlertName		O nome do alerta.
ActiveAlertInstance		O nome da entidade que gerou o alerta, normalmente o nome do nó.
ActiveAlertSeverity		A gravidade do alerta.
ActiveAlertStartTime		A data e a hora em que o alerta foi acionado.

Tipos de notificação (armadilhas)

Todas as notificações incluem as seguintes variáveis como varbinds:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Tipo de notificação	Código Objeto (OID)	Descrição
ActiveMinorAlert		Um alerta com gravidade menor
ActiveMajorAlert		Um alerta com grande gravidade
ActiveCriticalAlert		Um alerta com gravidade crítica

Colete dados adicionais do StorageGRID

Use gráficos e gráficos

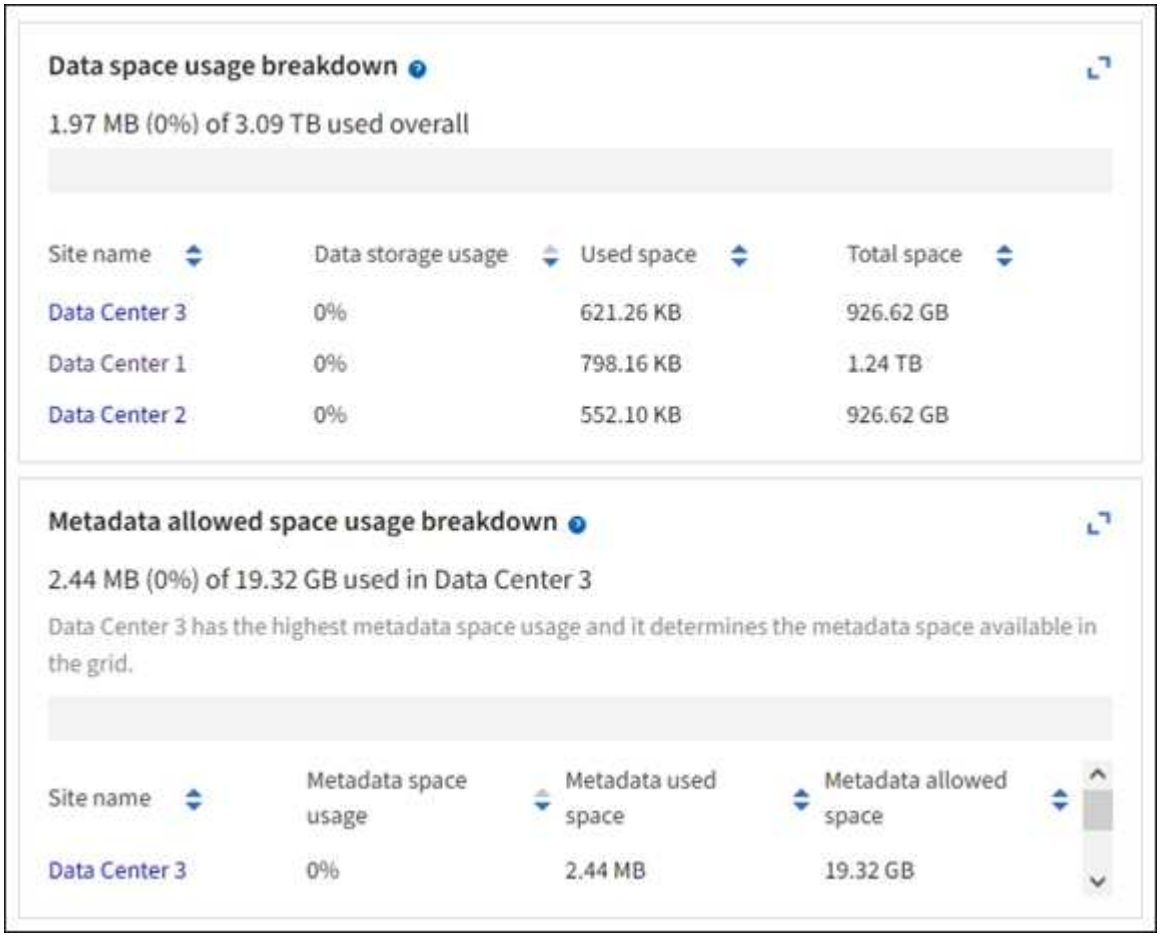
Você pode usar gráficos e relatórios para monitorar o estado do sistema StorageGRID e solucionar problemas.

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

Tipos de gráficos

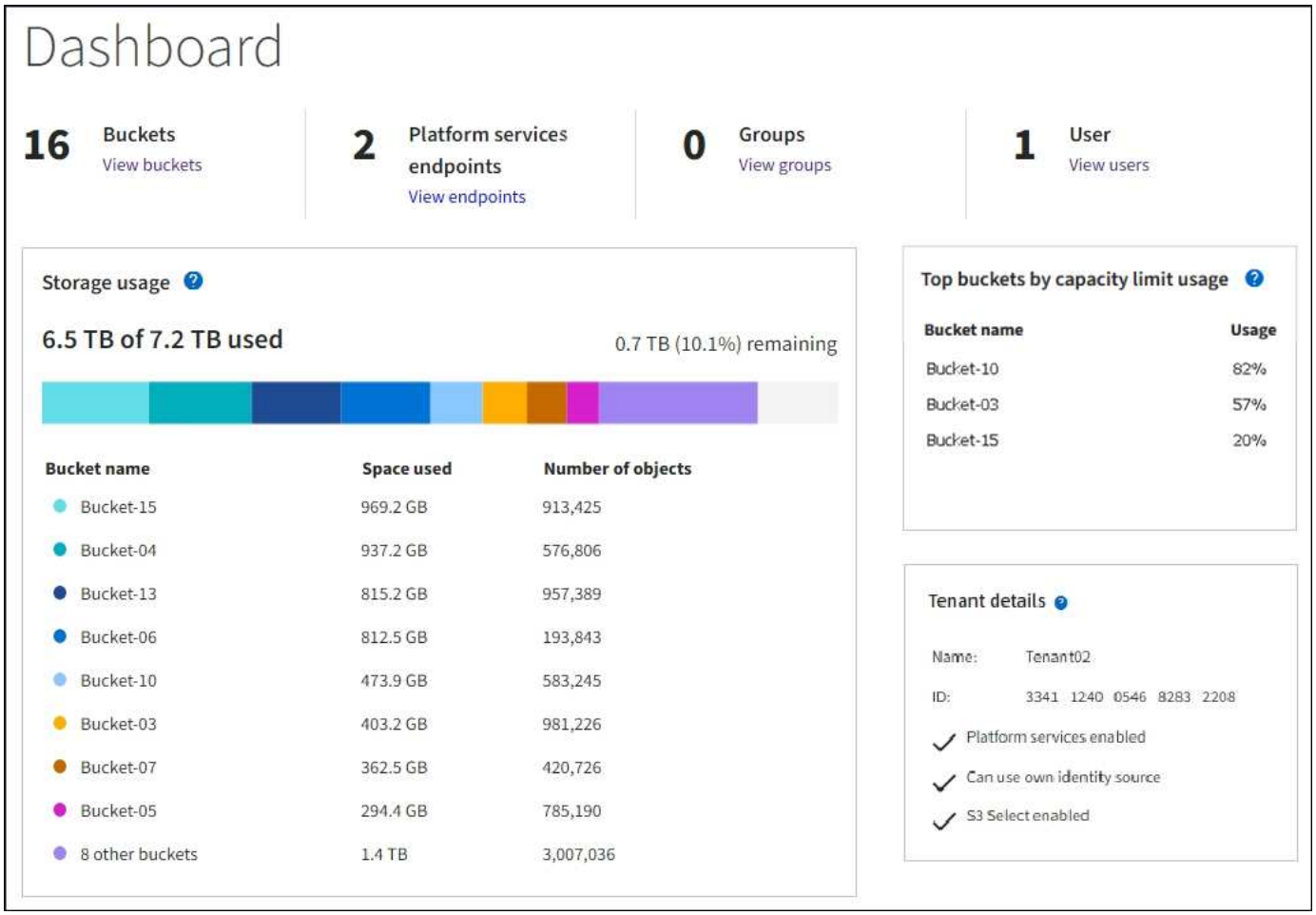
Gráficos e gráficos resumem os valores de métricas e atributos específicos do StorageGRID.

O painel do Gerenciador de Grade inclui cartões que resumem o armazenamento disponível para a grade e cada local.



O painel uso do armazenamento no painel do Gerenciador do locatário exibe o seguinte:

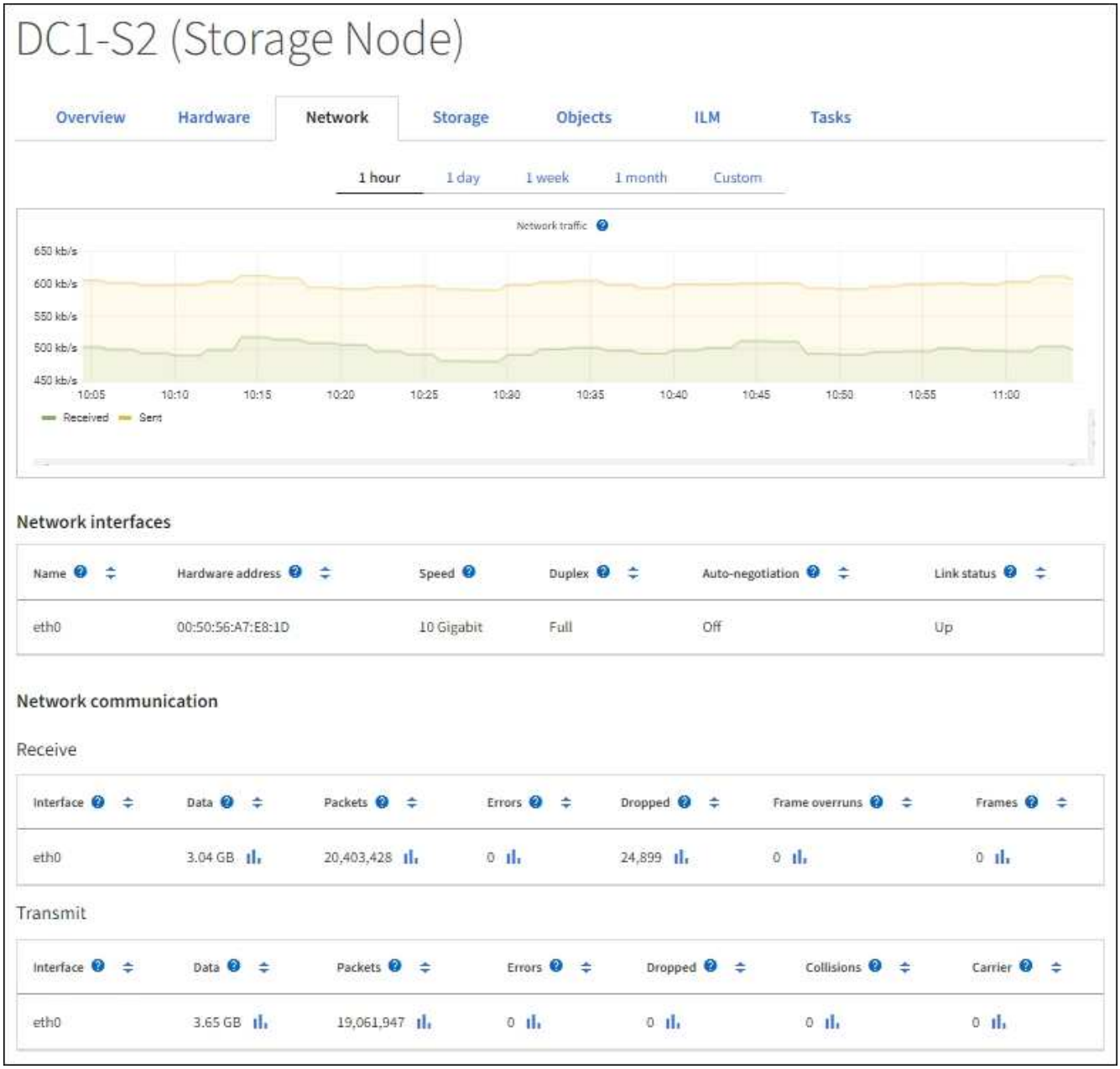
- Uma lista dos maiores baldes (S3) ou contentores (Swift) para o inquilino
- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou contentores
- A quantidade total de espaço utilizado e, se for definida uma quota, a quantidade e a percentagem de espaço restante



Além disso, gráficos que mostram como as métricas e atributos do StorageGRID mudam ao longo do tempo estão disponíveis na página de nós e na página **SUPPORT** > **Tools** > **Grid topology**.

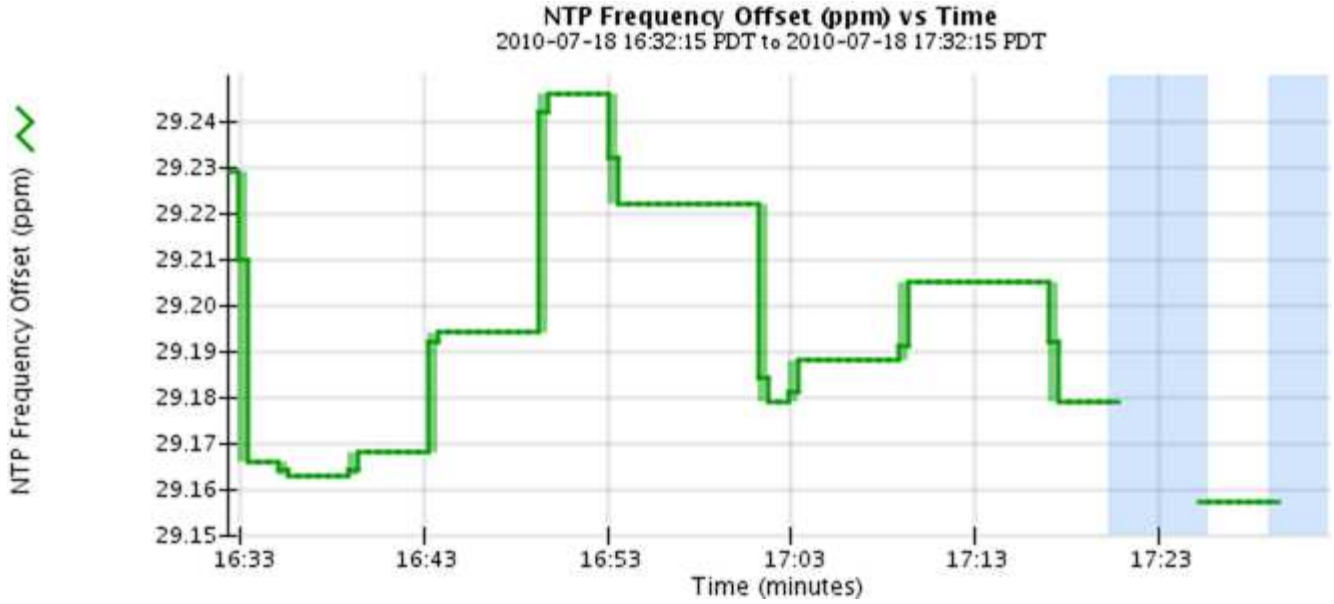
Existem quatro tipos de gráficos:

- **Gráficos Grafana**: Mostrados na página de nós, gráficos Grafana são usados para plotar os valores das métricas Prometheus ao longo do tempo. Por exemplo, a guia **NÓS** > **rede** para um nó de armazenamento inclui um gráfico Grafana para tráfego de rede.

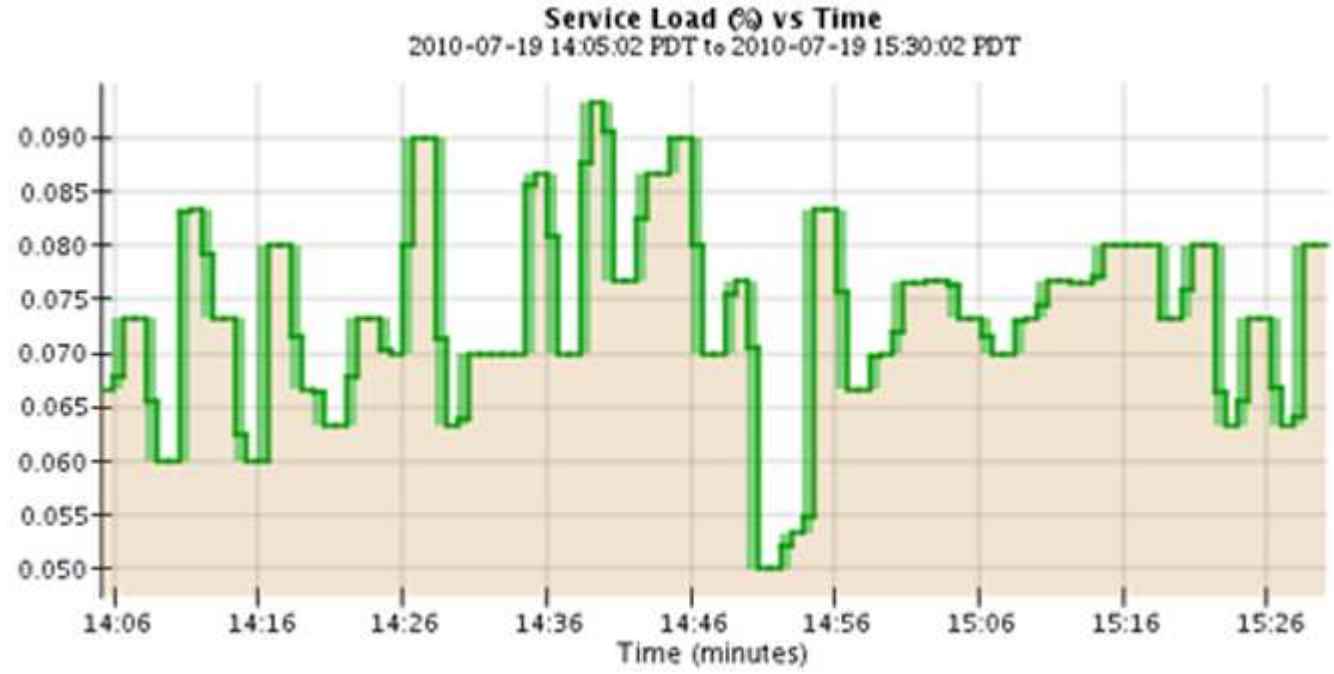


Gráficos Grafana também estão incluídos nos painéis pré-construídos disponíveis na página **SUPPORT** > **Tools** > **Metrics**.

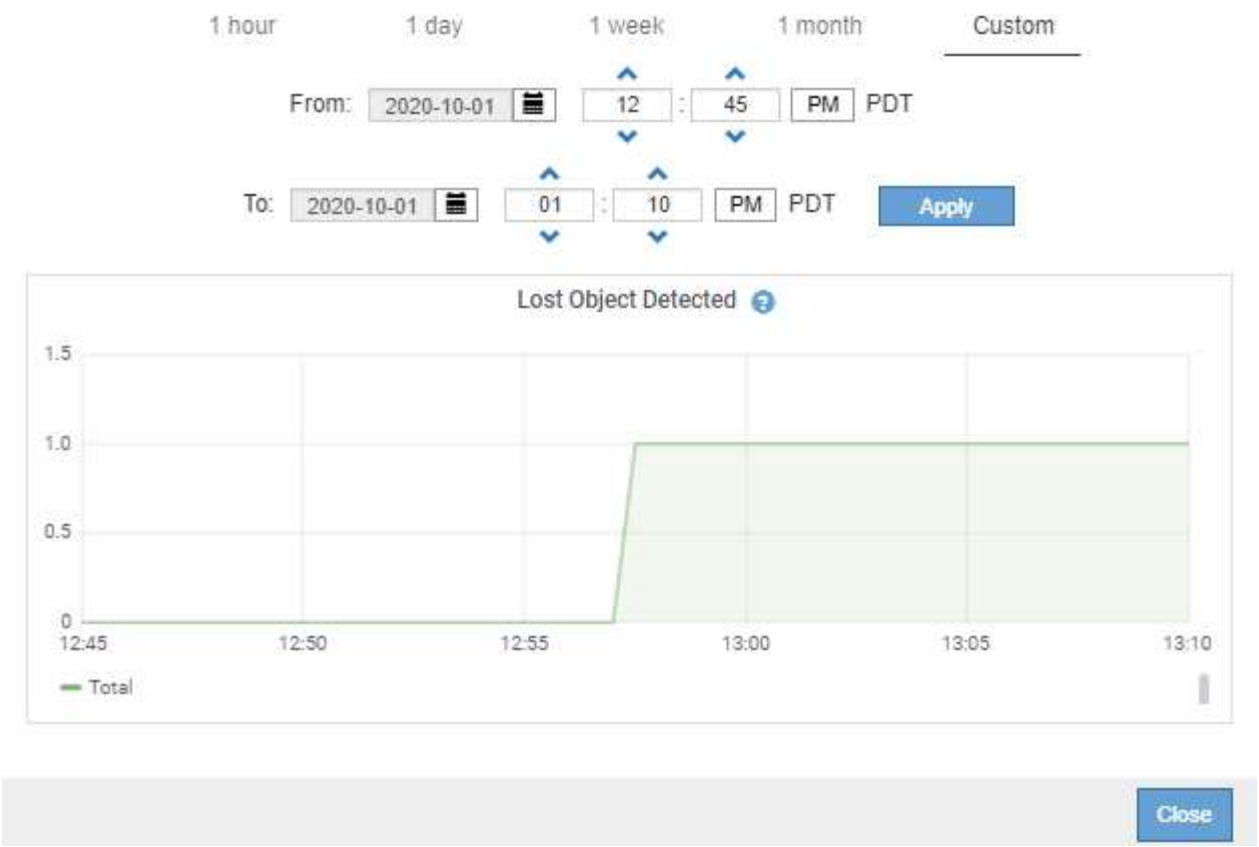
- **Gráficos de linha**: Disponíveis na página de nós e na página **SUPPORT** > **Tools** > **Grid topoly** (selecione o ícone do gráfico após um valor de dados), os gráficos de linha são usados para plotar os valores dos atributos StorageGRID que têm um valor unitário (como deslocamento de frequência NTP, em ppm). As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



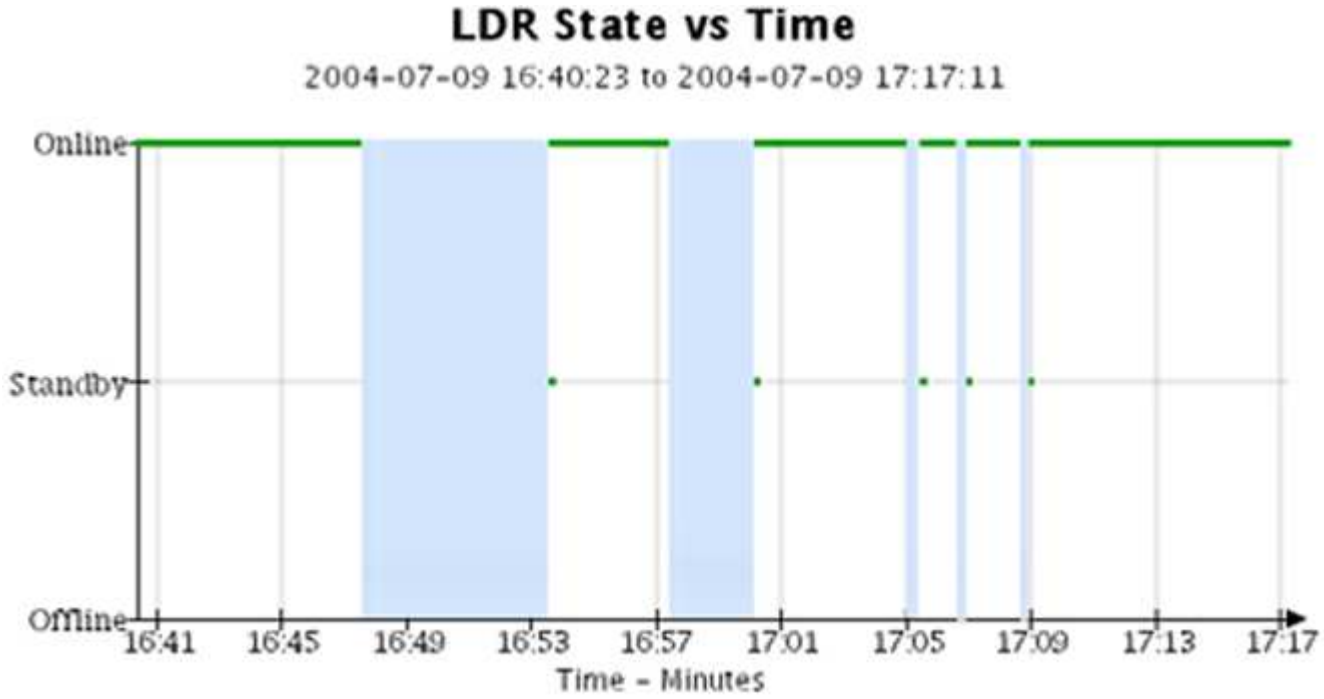
- **Gráficos de área**: Disponíveis na página de nós e na página **SUPPORT** > **Tools** > **Grid topology** (selecione o ícone do gráfico após um valor de dados), os gráficos de área são usados para plotar quantidades de atributos volumétricos, como contagens de objetos ou valores de carga de serviço. Os gráficos de área são semelhantes aos gráficos de linha, mas incluem um sombreamento marrom claro abaixo da linha. As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



- Alguns gráficos são denotados com um tipo diferente de ícone de gráfico e têm um formato diferente:



- **State graph**: Disponível na página **SUPPORT** > **Tools** > **Grid topoly** (selecione o ícone do gráfico após um valor de dados), os gráficos de estado são usados para plotar valores de atributo que representam estados distintos, como um estado de serviço que pode ser on-line, standby ou offline. Os gráficos de estado são semelhantes aos gráficos de linha, mas a transição é descontínua, ou seja, o valor salta de um valor de estado para outro.

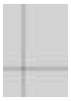


Informações relacionadas

- "Exibir a página nós"
- "Veja a árvore de topologia de Grade"
- "Analise as métricas de suporte"

Legenda da carta

As linhas e cores usadas para desenhar gráficos têm significado específico.

Exemplo	Significado
	Os valores de atributo relatados são plotados usando linhas verdes escuras.
	O sombreamento verde claro em torno de linhas verdes escuras indica que os valores reais nesse intervalo de tempo variam e foram "encadernados" para plotagem mais rápida. A linha escura representa a média ponderada. O intervalo em verde claro indica os valores máximo e mínimo dentro do compartimento. O sombreamento castanho claro é usado para gráficos de área para indicar dados volumétricos.
	Áreas em branco (sem dados plotados) indicam que os valores do atributo não estavam disponíveis. O fundo pode ser azul, cinza ou uma mistura de cinza e azul, dependendo do estado do serviço que relata o atributo.
	O sombreamento azul claro indica que alguns ou todos os valores do atributo naquele momento eram indeterminados; o atributo não estava relatando valores porque o serviço estava em um estado desconhecido.
	O sombreamento cinza indica que alguns ou todos os valores de atributo naquele momento não eram conhecidos porque o serviço que relata os atributos estava administrativamente inativo.
	Uma mistura de sombreamento cinza e azul indica que alguns dos valores de atributo na época eram indeterminados (porque o serviço estava em um estado desconhecido), enquanto outros não eram conhecidos porque o serviço relatando os atributos estava administrativamente para baixo.

Apresentar gráficos e gráficos

A página nós contém os gráficos e gráficos que você deve acessar regularmente para monitorar atributos como capacidade de storage e taxa de transferência. Em alguns casos, especialmente ao trabalhar com suporte técnico, você pode usar a página **SUPPORT** > **Tools** > **Grid topology** para acessar gráficos adicionais.

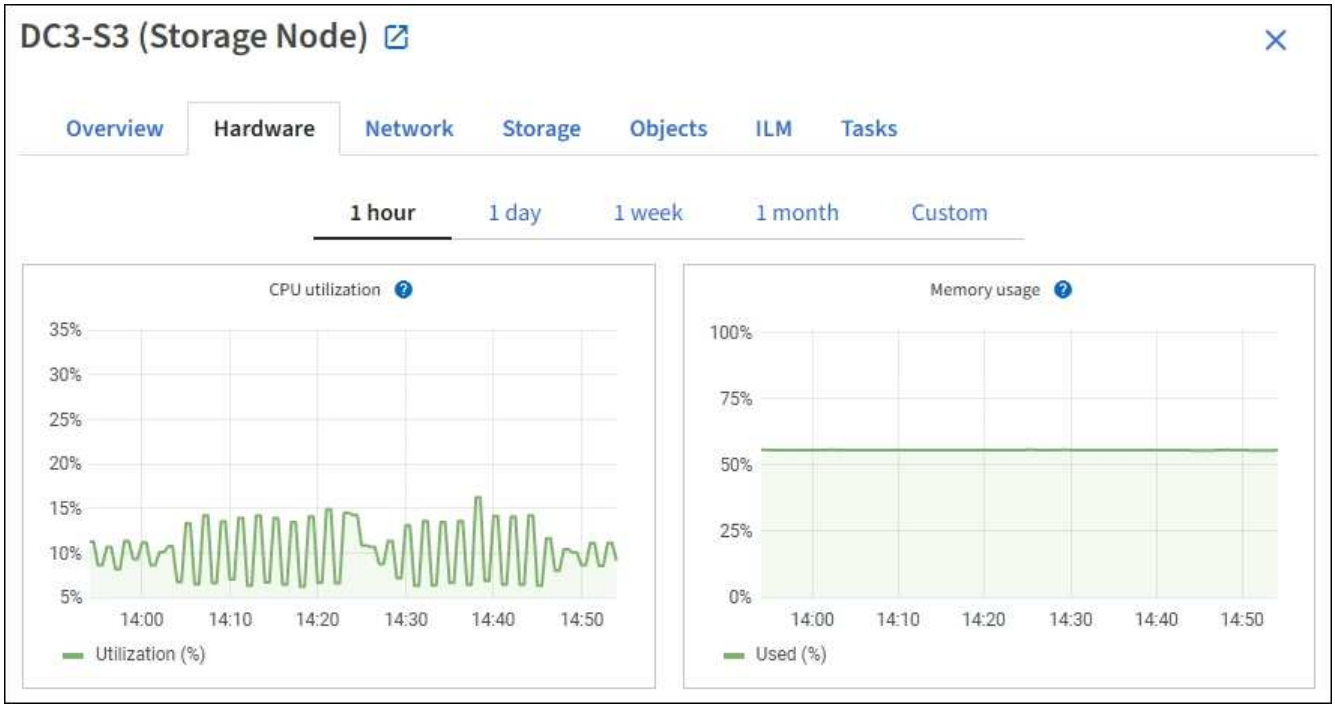
Antes de começar

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

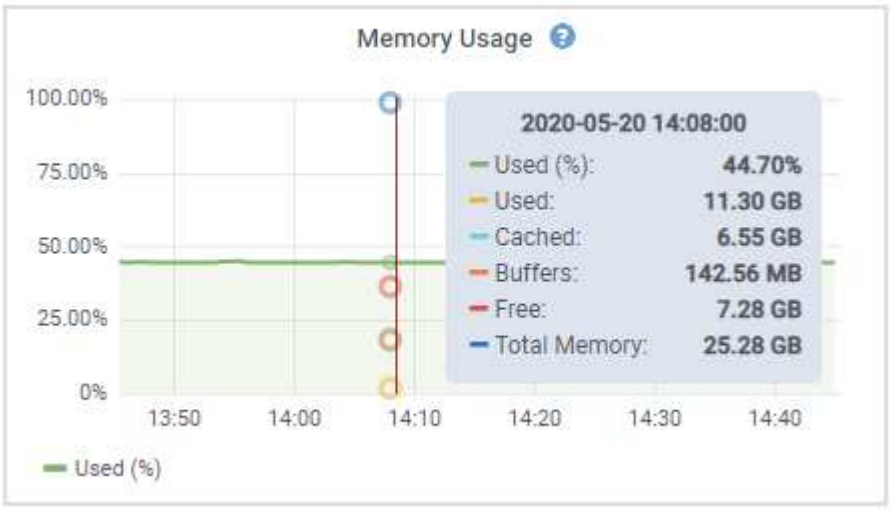
Passos

1. Selecione **NODES**. Em seguida, selecione um nó, um site ou toda a grade.
2. Selecione o separador para o qual pretende ver as informações.

Algumas guias incluem um ou mais gráficos Grafana, que são usados para plotar os valores das métricas de Prometheus ao longo do tempo. Por exemplo, a guia **NÓS** > **hardware** de um nó inclui dois gráficos Grafana.



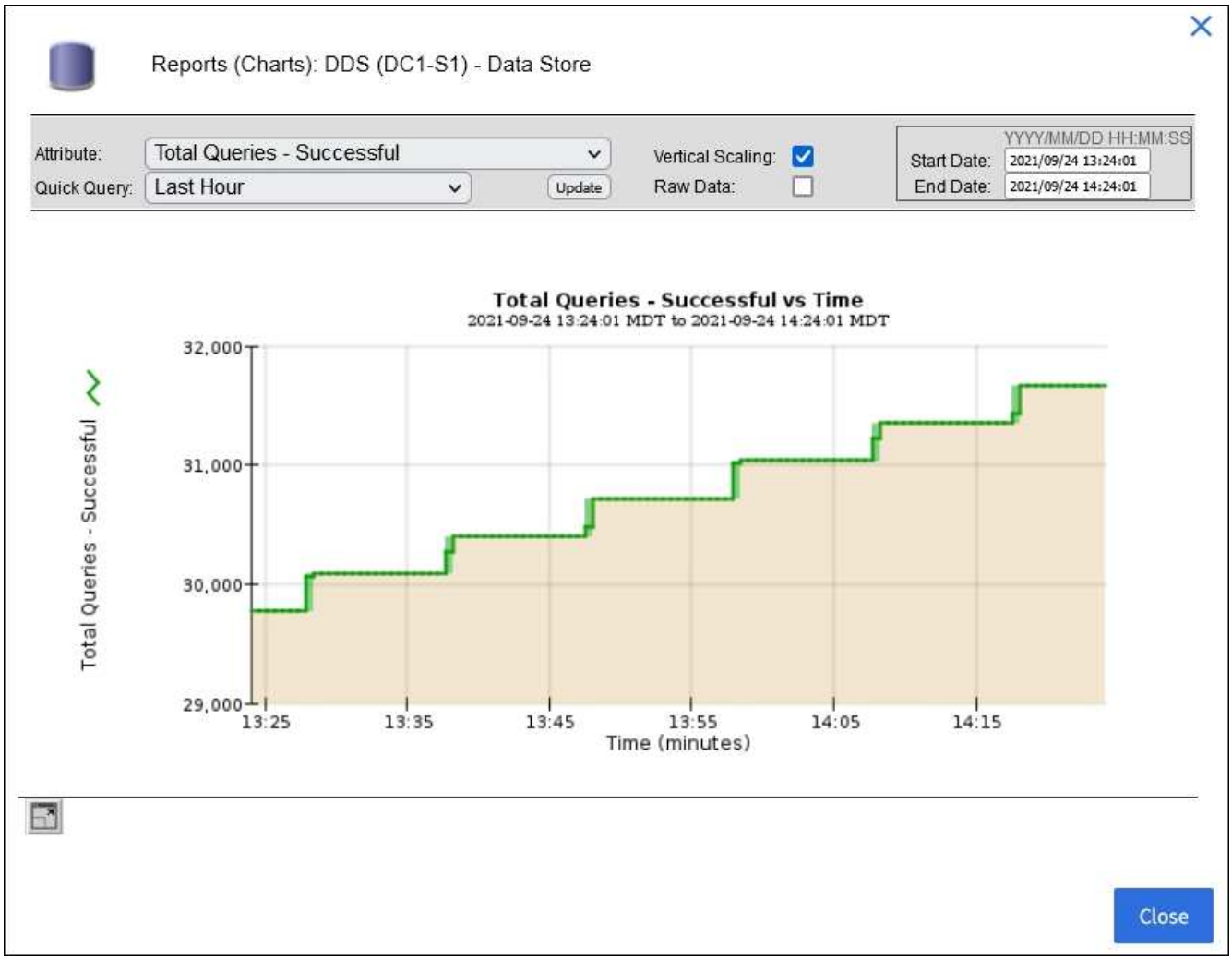
3. Opcionalmente, posicione o cursor sobre o gráfico para ver valores mais detalhados para um determinado ponto no tempo.

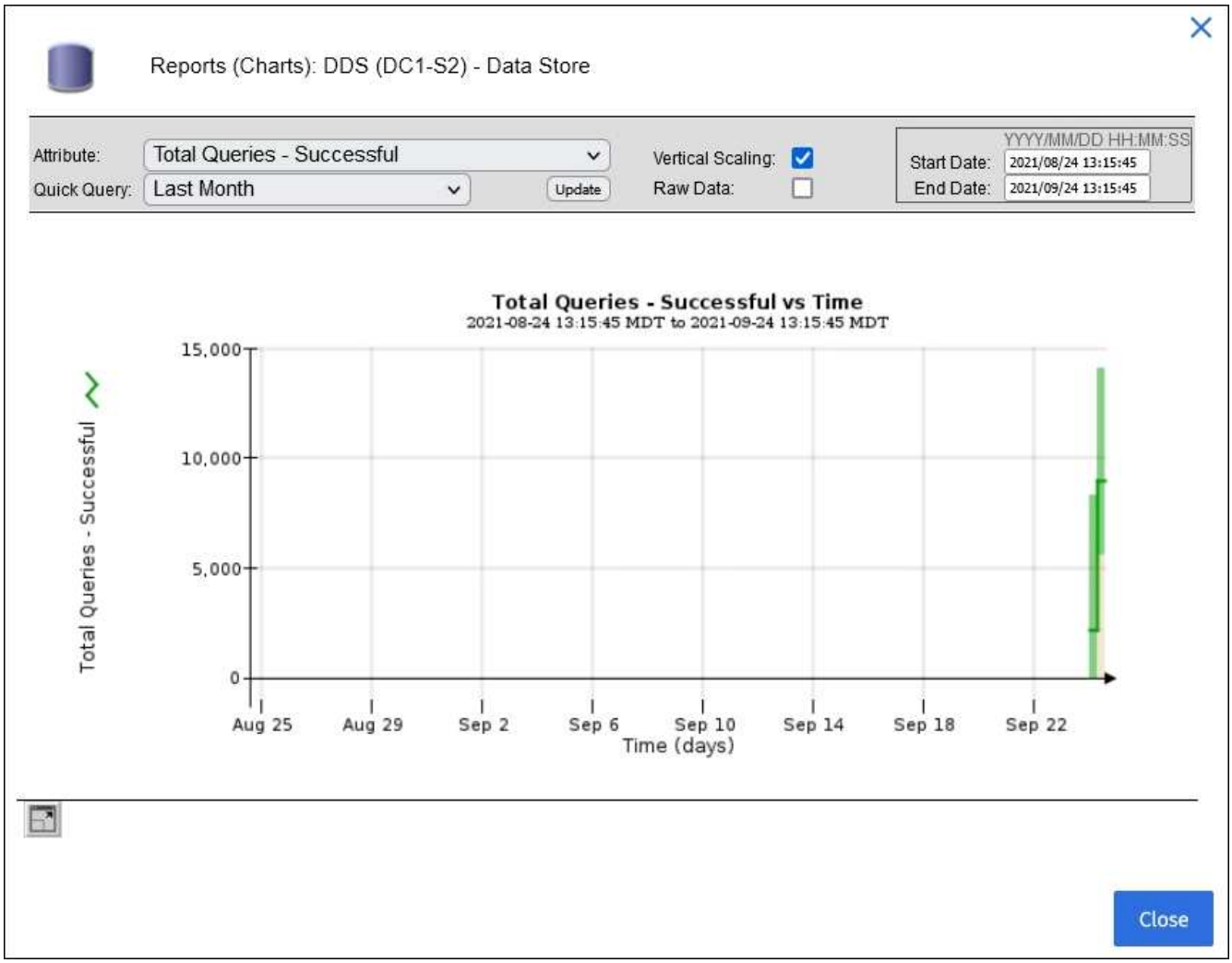


4. Conforme necessário, muitas vezes é possível exibir um gráfico para um atributo ou métrica específico. Na tabela na página nós, selecione o ícone do gráfico à direita do nome do atributo.

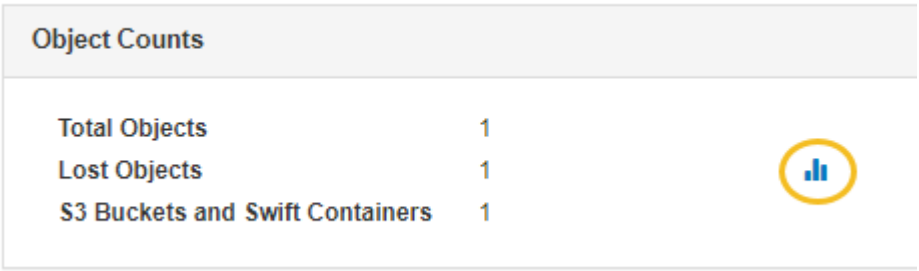
> Os gráficos não estão disponíveis para todas as métricas e atributos.

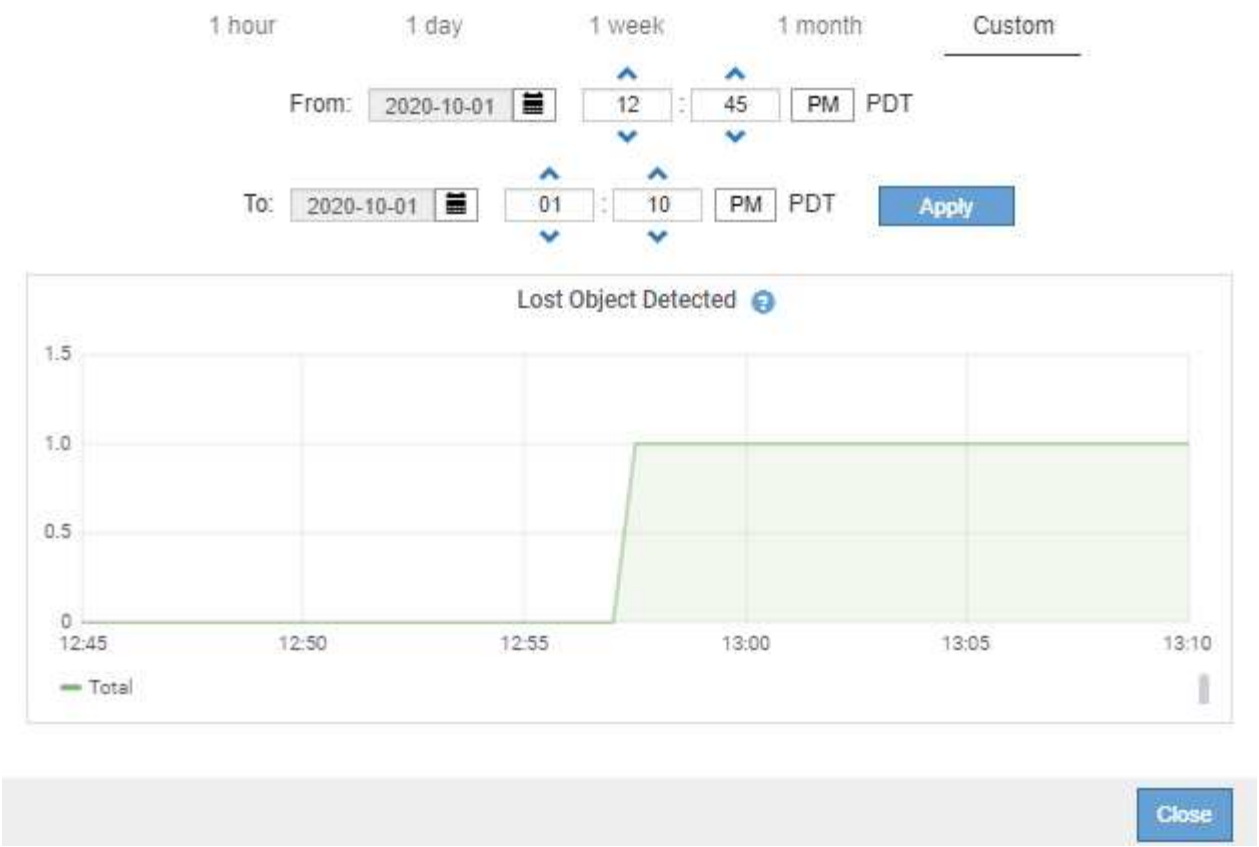
Exemplo 1: Na guia objetos de um nó de armazenamento, você pode selecionar o ícone do gráfico para ver o número total de consultas de armazenamento de metadados bem-sucedidas para o nó de armazenamento.


Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

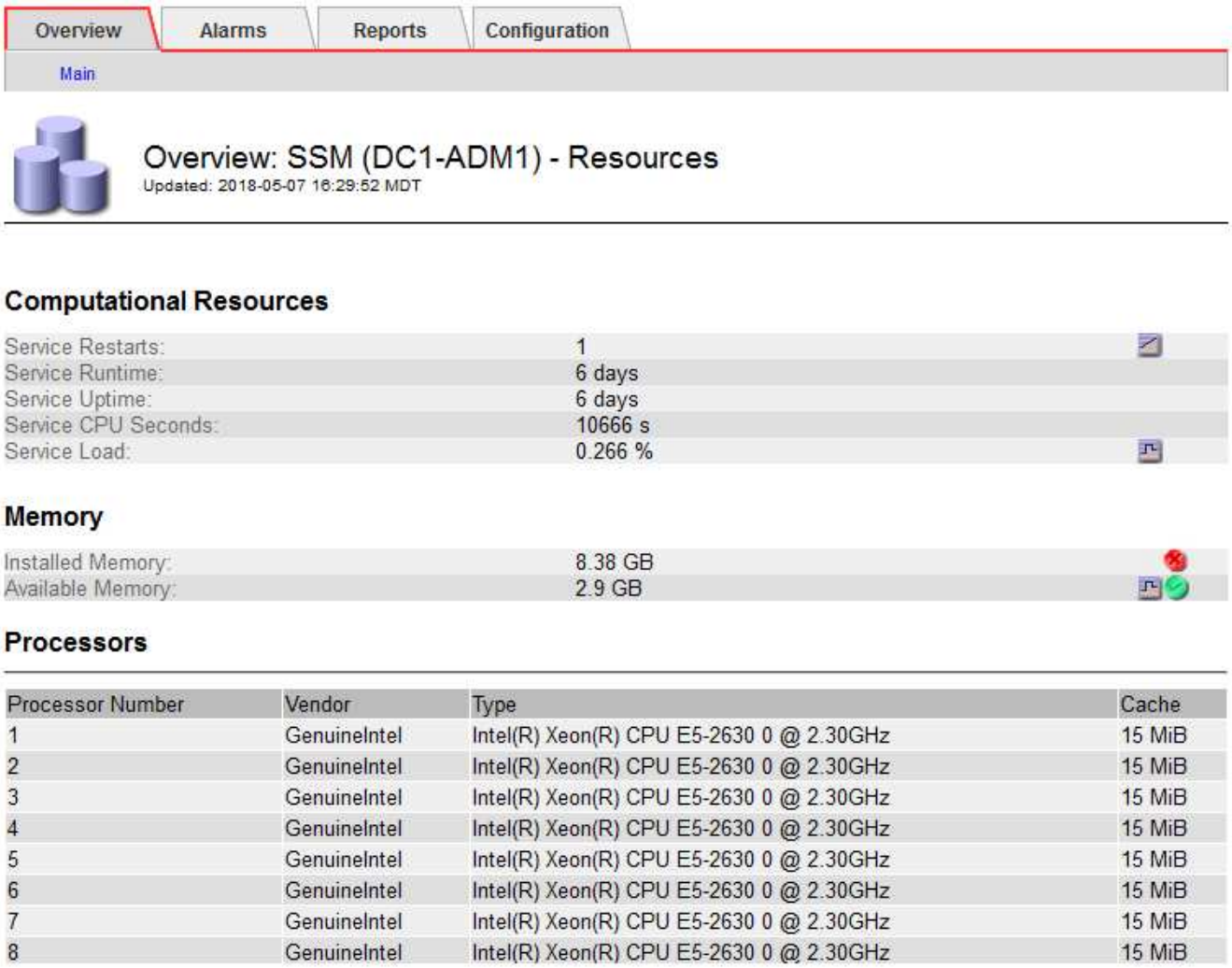


Exemplo 2: Na guia objetos de um nó de armazenamento, você pode selecionar o ícone do gráfico para ver o gráfico Grafana da contagem de objetos perdidos detetados ao longo do tempo.





5. Para exibir gráficos para atributos que não são exibidos na página nó, selecione **support** > **Tools** > **Grid topoly**.
6. Selecione ***grid node*** > ***component ou Service*** > **Overview** > **Main**.



7. Selecione o ícone do gráfico ao lado do atributo.

   O visor muda automaticamente para a página **relatórios** > **gráficos**. O gráfico exibe os dados do atributo no último dia.

Gerar gráficos

Os gráficos exibem uma representação gráfica dos valores de dados de atributos. Você pode gerar relatórios em um local de data center, nó de grade, componente ou serviço.

Antes de começar

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

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***grid node*** > ***component ou Service*** > **Reports** > **Charts**.
3. Selecione o atributo para relatar na lista suspensa **Atributo**.
4. Para forçar o eixo Y a iniciar em zero, desmarque a caixa de seleção **vertical Scaling**.
5. Para mostrar valores com precisão total, marque a caixa de seleção **dados brutos** ou arredondar valores

para um máximo de três casas decimais (por exemplo, para atributos reportados como porcentagens), desmarque a caixa de seleção **dados brutos**.

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

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

   O gráfico aparece após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo.

7. Se você selecionou consulta personalizada, personalize o período de tempo para o gráfico inserindo **Data de início** e **Data de término**.

   Utilize o formato *YYYY/MM/DDHH:MM:SS* na hora local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

8. Selecione **Atualizar**.

   Um gráfico é gerado após alguns segundos. Aguarde vários minutos para a tabulação de longos intervalos de tempo. Dependendo do período de tempo definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado são exibidos.

Use relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Existem dois tipos de relatórios gerados dependendo do período de tempo em que você está relatando: Relatórios de texto bruto para períodos inferiores a uma semana e relatórios de texto agregados para períodos de tempo superiores a uma semana.

Relatórios de texto bruto

Um relatório de texto bruto exibe detalhes sobre o atributo selecionado:

- Hora recebida: Data e hora local em que um valor de amostra dos dados de um atributo foi processado pelo serviço NMS.
- Hora da amostra: Data e hora locais em que um valor de atributo foi amostrado ou alterado na origem.
- Valor: Valor do atributo no tempo da amostra.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Agregar relatórios de texto

Um relatório de texto agregado exibe dados durante um período de tempo mais longo (geralmente uma semana) do que um relatório de texto bruto. Cada entrada é o resultado de resumir vários valores de atributo (um agregado de valores de atributo) pelo serviço NMS ao longo do tempo em uma única entrada com valores médios, máximos e mínimos que são derivados da agregação.

Cada entrada exibe as seguintes informações:

- Hora agregada: Data e hora locais da última vez que o serviço NMS agregou (coletou) um conjunto de valores de atributo alterados.
- Valor médio: A média do valor do atributo durante o período de tempo agregado.
- Valor mínimo: O valor mínimo durante o período de tempo agregado.
- Valor máximo: O valor máximo durante o período de tempo agregado.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Gerar relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Você pode gerar relatórios em um local de data center, nó de grade, componente ou serviço.

Antes de começar

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

Sobre esta tarefa

Para dados de atributos que se espera que estejam mudando continuamente, esses dados de atributo são amostrados pelo serviço NMS (na origem) em intervalos regulares. Para dados de atributos que mudam com pouca frequência (por exemplo, dados baseados em eventos como alterações de estado ou status), um valor de atributo é enviado ao serviço NMS quando o valor muda.

O tipo de relatório apresentado depende do período de tempo configurado. Por padrão, relatórios de texto agregados são gerados para períodos de tempo superiores a uma semana.

Texto cinza indica que o serviço foi desativado administrativamente durante o período de amostragem. Texto azul indica que o serviço estava em um estado desconhecido.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***grid node*** > ***component ou Service*** > **Reports** > **Text**.
3. Selecione o atributo para relatar na lista suspensa **Atributo**.
4. Selecione o número de resultados por página na lista suspensa **resultados por página**.
5. Para arredondar valores para um máximo de três casas decimais (por exemplo, para atributos reportados como porcentagens), desmarque a caixa de seleção **dados brutos**.
6. Selecione o período de tempo para relatar na lista suspensa **consulta rápida**.

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

O relatório aparece após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo.

7. Se você selecionou consulta personalizada, você precisa personalizar o período de tempo para relatar inserindo **Data de início** e **Data de término**.

   Utilize o formato `YYYY/MM/DDHH:MM:SS` na hora local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

8. Clique em **Atualizar**.

   Um relatório de texto é gerado após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo. Dependendo do período de tempo definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado são exibidos.

Exportar relatórios de texto

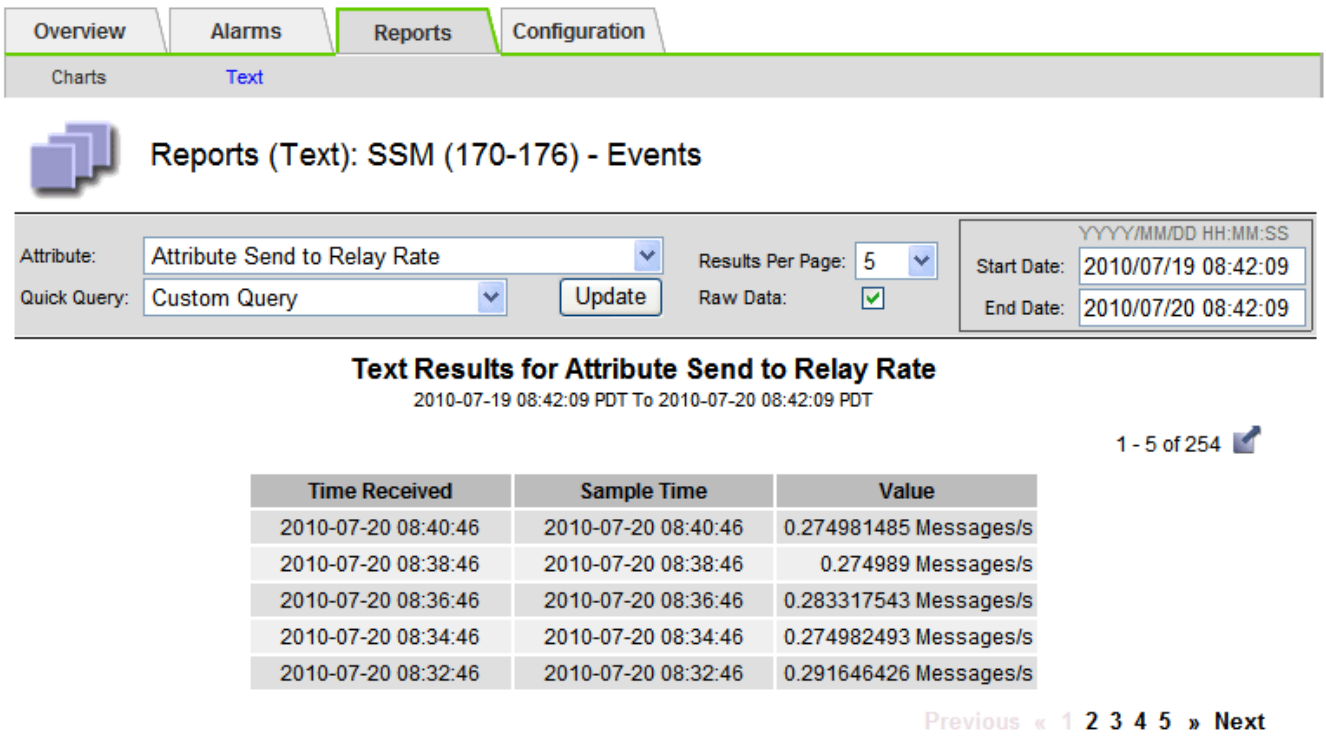
Os relatórios de texto exportados abrem uma nova guia do navegador, que permite selecionar e copiar os dados.

Sobre esta tarefa

Os dados copiados podem então ser salvos em um novo documento (por exemplo, uma Planilha) e usados para analisar o desempenho do sistema StorageGRID.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Crie um relatório de texto.
3. Clique em *Exportar*.



A janela Exportar relatório de texto abre-se exibindo o relatório.

Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. Selecione e copie o conteúdo da janela Exportar Relatório de texto.

   Esses dados podem agora ser colados em um documento de terceiros, como uma Planilha.

Monitore O PUT e obtenha desempenho

Você pode monitorar o desempenho de certas operações, como armazenamento e recuperação de objetos, para ajudar a identificar alterações que podem exigir mais investigação.

Sobre esta tarefa

Para monitorar O desempenho, você pode executar comandos S3 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 das seguintes S3 operações: DELETE, GET, HEAD, Metadata updated, POST, PUT

Ao analisar os resultados, observe o tempo médio necessário para atender a uma solicitação, bem como o throughput geral que você pode alcançar. Repita os mesmos testes regularmente e registe os resultados, para que possa identificar tendências que possam necessitar de investigação.

- Você pode "Baixe S3tester a partir de github".

Monitorar operações de verificação de objetos

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

Antes de começar

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

Sobre esta tarefa

Dois "processos de verificação" trabalham juntos para garantir a integridade dos dados:

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

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

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

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

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

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

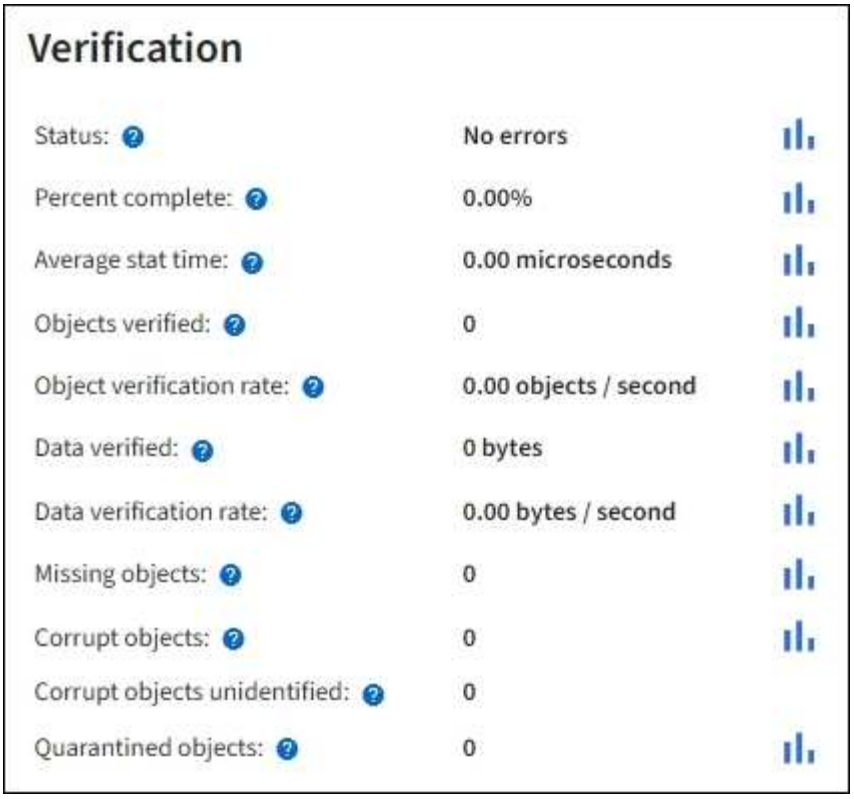
Passos

1. Reveja os resultados das verificações de antecedentes:

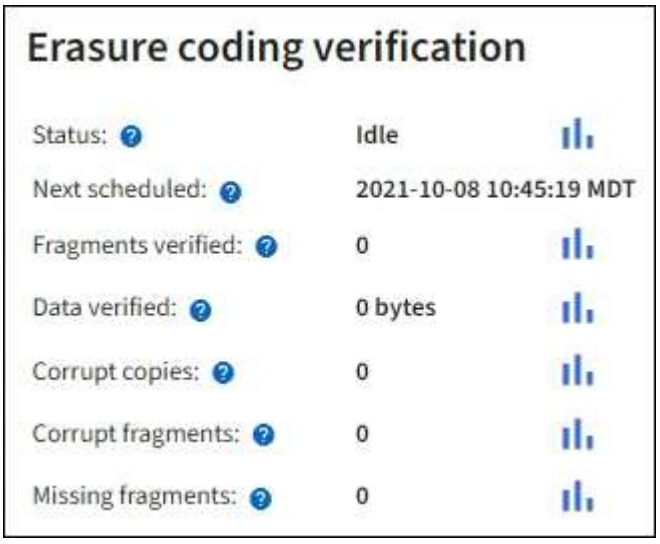
   a. Selecione **NODES** > ***Storage Node*** > **Objects**.

   b. Verifique os resultados da verificação:

      - Para verificar a verificação de dados de objetos replicados, observe os atributos na seção Verificação.

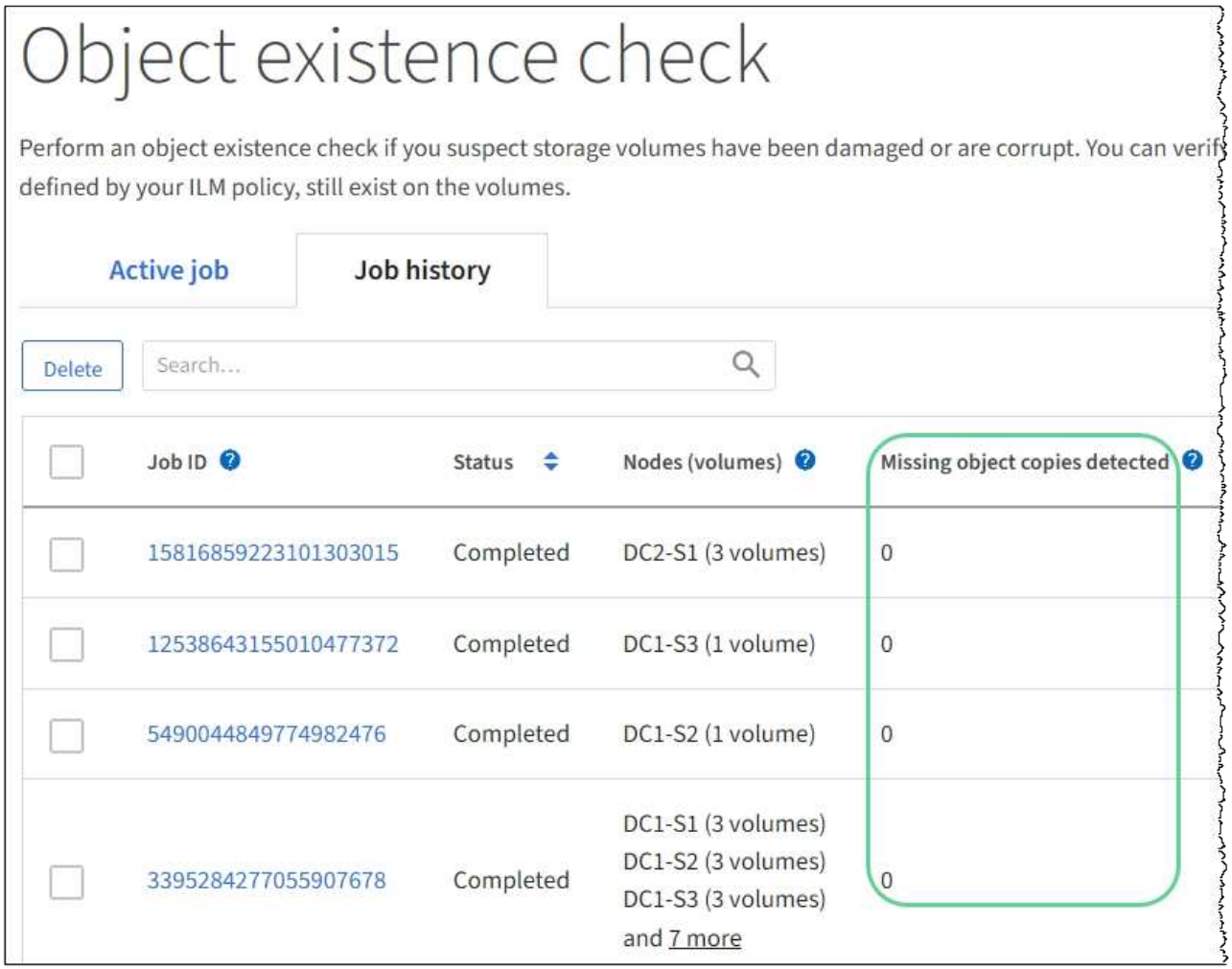


- Para verificar a verificação de fragmentos codificados por apagamento, selecione ***Storage Node*** > **ILM** e veja os atributos na seção de verificação de codificação de apagamento.



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

2. Reveja os resultados dos trabalhos de verificação de existência de objeto:
   a. Selecione **MAINTENANCE** > **Object existence check** > **Job history**.
   b. Digitalizar a coluna cópias de objeto em falta detetadas. Se algum trabalho resultar em 100 ou mais cópias de objetos ausentes e o alerta **objetos perdidos** tiver sido acionado, entre em Contato com o suporte técnico.



Monitorar eventos

Você pode monitorar eventos que são detetados por um nó de grade, incluindo eventos personalizados que você criou para rastrear eventos registrados no servidor syslog. A mensagem último evento mostrada no Gerenciador de Grade fornece mais informações sobre o evento mais recente.

As mensagens de evento também são listadas no `/var/local/log/bycast-err.log` arquivo de log. Consulte "Referência de ficheiros de registo".

O alarme SMTT (Total de eventos) pode ser repetidamente acionado por problemas como problemas de rede, interrupções de energia ou atualizações. Esta seção tem informações sobre a investigação de eventos para que você possa entender melhor por que esses alarmes ocorreram. Se um evento ocorreu devido a um problema conhecido, é seguro redefinir os contadores de eventos.

Passos

1. Revise os eventos do sistema para cada nó de grade:
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***site*** > ***grid node*** > **SSM** > **Eventos** > **Visão geral** > **Principal**.
2. Gere uma lista de mensagens de eventos anteriores para ajudar a isolar problemas que ocorreram no passado:

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

b. Selecione ***site*** > ***grid node*** > **SSM** > **Eventos** > **relatórios**.

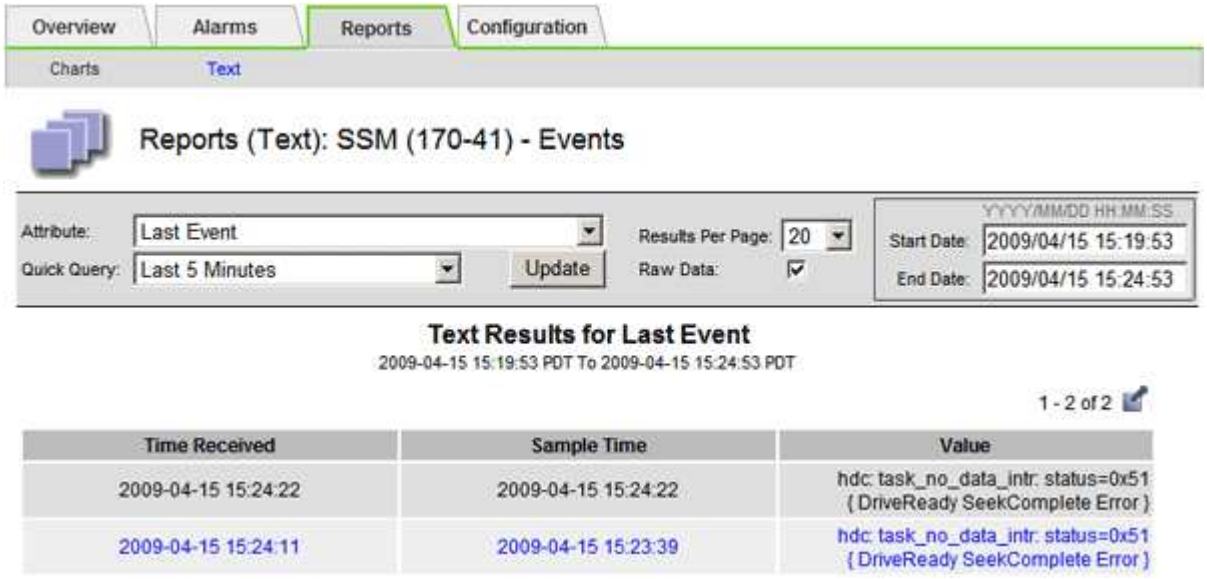
c. Selecione **texto**.

O atributo **último evento** não é mostrado no "vista de gráficos". Para visualizá-lo:

d. Altere **Atributo** para **último evento**.

e. Opcionalmente, selecione um período de tempo para **consulta rápida**.

f. Selecione **Atualizar**.



Crie eventos syslog personalizados

Eventos personalizados permitem que você acompanhe todos os eventos de usuário do kernel, daemon, erro e nível crítico registrados no servidor syslog. Um evento personalizado pode ser útil para monitorar a ocorrência de mensagens de log do sistema (e, portanto, eventos de segurança de rede e falhas de hardware).

Sobre esta tarefa

Considere criar eventos personalizados para monitorar problemas recorrentes. As considerações a seguir se aplicam a eventos personalizados.

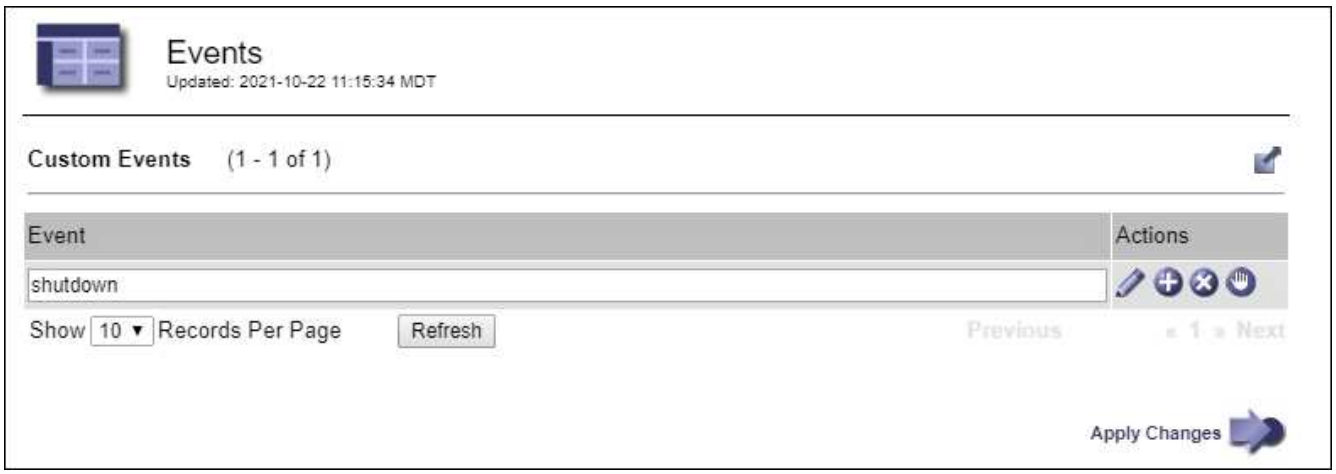
- Depois que um evento personalizado é criado, cada ocorrência dele é monitorada.
- Para criar um evento personalizado com base em palavras-chave nos `/var/local/log/messages` arquivos, os logs nesses arquivos devem ser:
  - Gerado pelo kernel
  - Gerado pelo daemon ou programa do usuário no nível de erro ou crítico

Nota: nem todas as entradas nos `/var/local/log/messages` arquivos serão correspondidas a menos que satisfaçam os requisitos acima indicados.

Passos

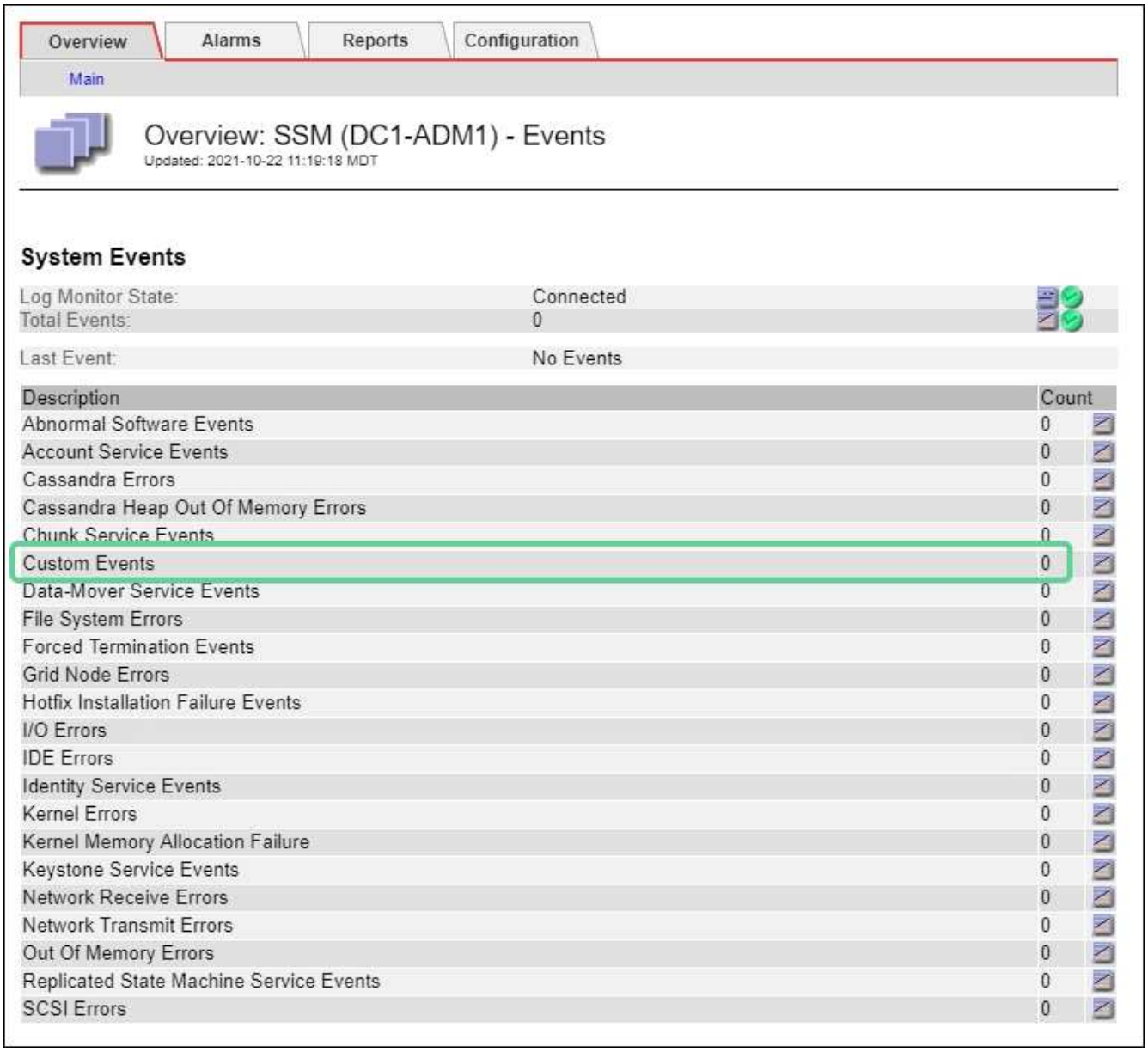
1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Custom events**.

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



4. Selecione **aplicar alterações**.
5. Selecione **SUPPORT** > **Tools** > **Grid topology**.
6. Selecione ***grid node*** > **SSM** > **Eventos**.
7. Localize a entrada de Eventos personalizados na tabela Eventos e monitore o valor de **Count**.

   Se a contagem aumentar, um evento personalizado que você está monitorando está sendo acionado nesse nó de grade.



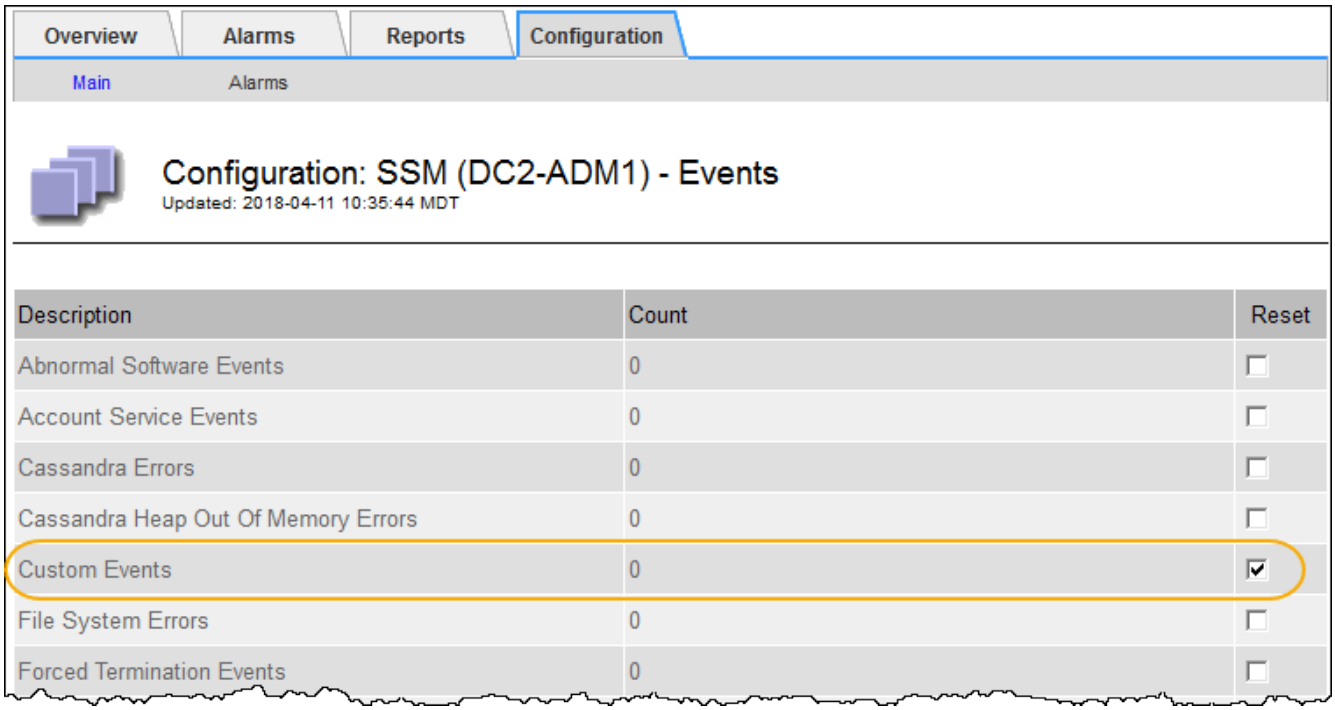
Redefina a contagem de eventos personalizados para zero

Se você quiser redefinir o contador apenas para eventos personalizados, use a página topologia de grade no menu suporte.

A reposição de um contador faz com que o alarme seja acionado pelo próximo evento. Em contraste, quando você reconhece um alarme, esse alarme só é reacionado se o próximo nível de limiar for atingido.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***grid node*** > **SSM** > **Eventos** > **Configuração** > **Principal**.
3. Marque a caixa de seleção **Reset** para Eventos personalizados.



4. Selecione **aplicar alterações**.

Rever mensagens de auditoria

As mensagens de auditoria podem ajudá-lo a entender melhor as operações detalhadas do seu sistema StorageGRID. Você pode usar logs de auditoria para solucionar problemas e avaliar o desempenho.

Durante a operação normal do sistema, todos os serviços StorageGRID geram mensagens de auditoria, como segue:

- As mensagens de auditoria do sistema estão relacionadas ao próprio sistema de auditoria, aos estados dos nós da grade, à atividade de tarefas em todo o sistema e às operações de backup de serviço.
- As mensagens de auditoria de storage de objetos estão relacionadas ao armazenamento e gerenciamento de objetos no StorageGRID, incluindo armazenamento de objetos e recuperações, transferências de nó de grade para nó de grade e verificações.
- As mensagens de auditoria de leitura e gravação do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para criar, modificar ou recuperar um objeto.
- As mensagens de auditoria de gerenciamento Registram solicitações de usuários para a API de gerenciamento.

Cada nó Admin armazena mensagens de auditoria em arquivos de texto. O compartilhamento de auditoria contém o arquivo ativo (audit.log), bem como logs de auditoria compatados de dias anteriores. Cada nó na grade também armazena uma cópia das informações de auditoria geradas no nó.

Você pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

O StorageGRID pode enviar informações de auditoria por padrão, ou você pode alterar o destino:

- O padrão do StorageGRID é destinos de auditoria de nó local.
- As entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de

storage.

- Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos Registros de auditoria continuam a ser gerados e armazenados quando um servidor syslog externo é configurado.
- "Saiba mais sobre como configurar mensagens de auditoria e destinos de log".

Para obter detalhes sobre o arquivo de log de auditoria, o formato das mensagens de auditoria, os tipos de mensagens de auditoria e as ferramentas disponíveis para analisar mensagens de auditoria, "Rever registos de auditoria"consulte .

Colete arquivos de log e dados do sistema

Você pode usar o Gerenciador de Grade para recuperar arquivos de log e dados do sistema (incluindo dados de configuração) para seu sistema StorageGRID.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade no nó Admin principal usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você deve ter a senha de provisionamento.

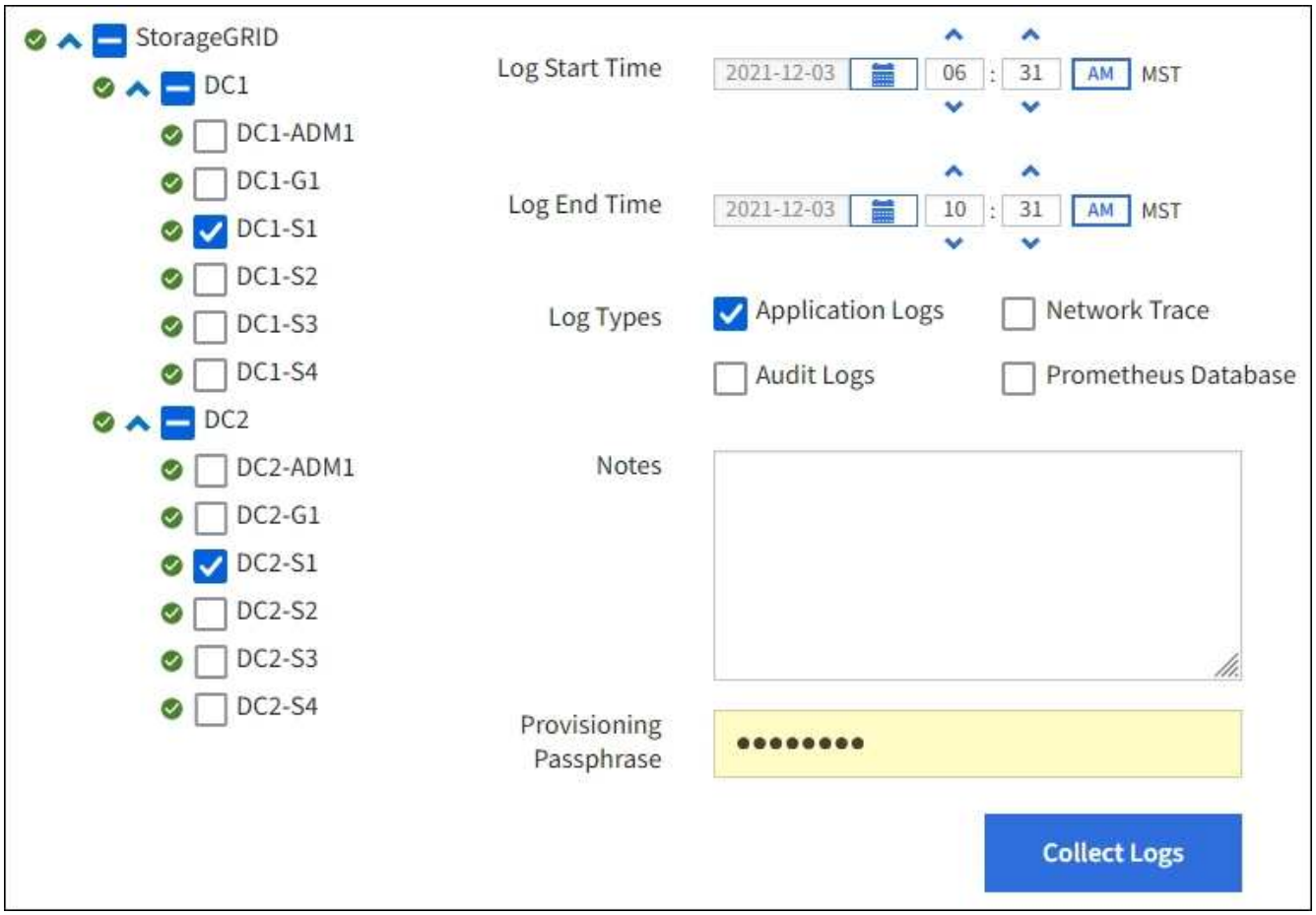
Sobre esta tarefa

Você pode usar o Gerenciador de Grade para coletar "ficheiros de registo", dados do sistema e dados de configuração de qualquer nó de grade para o período de tempo selecionado. Os dados são coletados e arquivados em um arquivo .tar.gz que você pode baixar para seu computador local.

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

Passos

1. Selecione **SUPPORT** > **Tools** > **Logs**.



2. Selecione os nós de grade para os quais você deseja coletar arquivos de log.

   Conforme necessário, você pode coletar arquivos de log para toda a grade ou para todo o site do data center.

3. Selecione **hora de início** e **hora de término** para definir o intervalo de tempo dos dados a serem incluídos nos arquivos de log.

   Se você selecionar um período de tempo muito longo ou coletar logs de todos os nós em uma grade grande, o arquivo de log pode se tornar muito grande para ser armazenado em um nó ou muito grande para ser coletado para o nó de administração principal para download. Se isso ocorrer, você deve reiniciar a coleta de logs com um conjunto menor de dados.

4. Selecione os tipos de registos que pretende recolher.
   - **Logs de aplicativos**: Logs específicos de aplicativos que o suporte técnico utiliza com mais frequência para solução de problemas. Os registos recolhidos são um subconjunto dos registos de aplicações disponíveis.
   - **Logs de auditoria**: Logs contendo as mensagens de auditoria geradas durante a operação normal do sistema.
   - **Rastreamento de rede**: Logs usados para depuração de rede.
   - **Prometheus Database**: Métricas de séries temporais dos serviços em todos os nós.
5. Opcionalmente, insira notas sobre os arquivos de log que você está reunindo na caixa de texto * Notas*.

   Você pode usar essas notas para fornecer informações de suporte técnico sobre o problema que o levou a coletar os arquivos de log. Suas anotações são adicionadas a um arquivo `info.txt` chamado ,

juntamente com outras informações sobre a coleção de arquivos de log. O `info.txt` ficheiro é guardado no pacote de arquivo de registo.

6. Introduza a frase-passe de aprovisionamento do seu sistema StorageGRID na caixa de texto **frase-passe de aprovisionamento**.
7. Selecione **Collect Logs**.

   Quando você envia uma nova solicitação, a coleção anterior de arquivos de log é excluída.

   Você pode usar a página Logs para monitorar o progresso da coleção de arquivos de log para cada nó de grade.

   Se você receber uma mensagem de erro sobre o tamanho do log, tente coletar logs por um período de tempo menor ou por menos nós.

8. Selecione **Download** quando a coleção de arquivos de log estiver concluída.

   O arquivo *.tar.gz* contém todos os arquivos de log de todos os nós de grade onde a coleta de log foi bem-sucedida. Dentro do arquivo combinado *.tar.gz*, há um arquivo de log para cada nó de grade.

Depois de terminar

Você pode baixar novamente o pacote de arquivo de log mais tarde, se precisar.

Opcionalmente, você pode selecionar **Excluir** para remover o pacote de arquivo de log e liberar espaço em disco. O pacote de arquivo de log atual é removido automaticamente da próxima vez que você coletar arquivos de log.

Acione manualmente um pacote AutoSupport

Para ajudar o suporte técnico na solução de problemas com o sistema StorageGRID, você pode acionar manualmente um pacote AutoSupport a ser enviado.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você deve ter a permissão de acesso root ou outra configuração de grade.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Na guia **ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

   O StorageGRID tenta enviar um pacote AutoSupport para o site de suporte da NetApp. Se a tentativa for bem-sucedida, os valores **resultado mais recente** e **último tempo bem-sucedido** na guia **resultados** serão atualizados. Se houver um problema, o valor **resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar o pacote AutoSupport novamente.

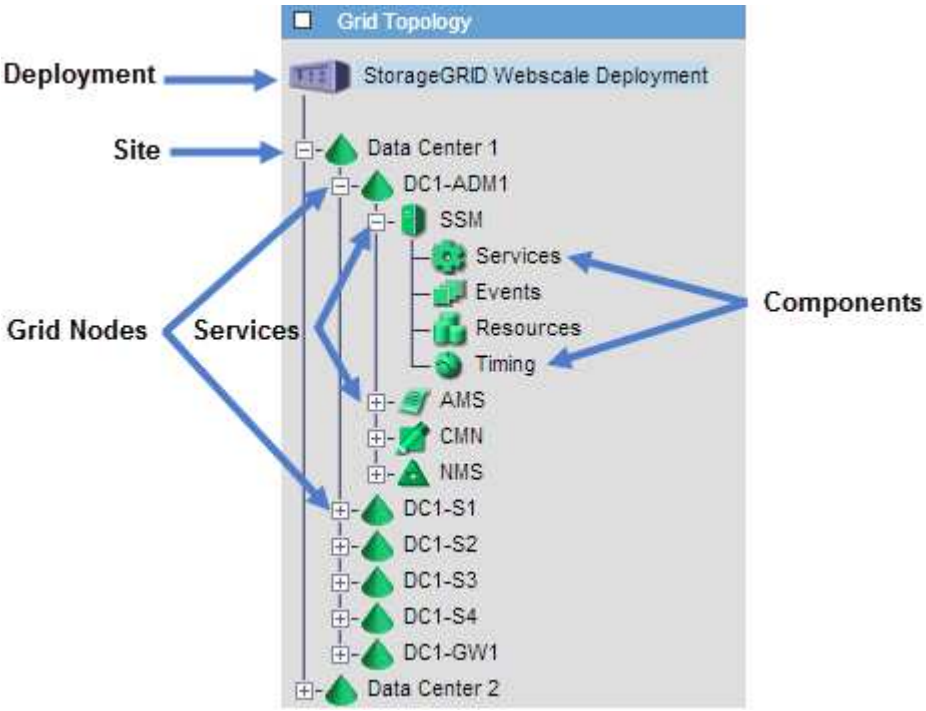
   Depois de enviar um pacote AutoSupport acionado pelo usuário, atualize a página AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Veja a árvore de topologia de Grade

A árvore de topologia de grade fornece acesso a informações detalhadas sobre

elementos do sistema StorageGRID, incluindo sites, nós de grade, serviços e componentes. Na maioria dos casos, você só precisa acessar a árvore de topologia de grade quando instruído na documentação ou quando estiver trabalhando com suporte técnico.

Para acessar a árvore de topologia de grade, selecione **SUPPORT** > **Tools** > **Grid topology**.



Para expandir ou recolher a árvore de topologia de Grade, clique ⊞ ou no local, nó ou ⊟ nível de serviço. Para expandir ou recolher todos os itens em todo o site ou em cada nó, mantenha pressionada a tecla **<Ctrl>** e clique em.

Atributos do StorageGRID

Atributos reportam valores e status para muitas das funções do sistema StorageGRID. Os valores de atributo estão disponíveis para cada nó de grade, cada local e toda a grade.

Os atributos do StorageGRID são usados em vários lugares no Gerenciador de Grade:

- **Página de nós**: Muitos dos valores mostrados na página de nós são atributos StorageGRID. (As métricas Prometheus também são mostradas nas páginas de nós.)
- **Grid Topology tree**: Os valores de atributo são mostrados na árvore Grid Topology (**SUPPORT** > **Tools** > **Grid topology**).
- **Eventos**: Os eventos do sistema ocorrem quando certos atributos Registram uma condição de erro ou falha para um nó, incluindo erros como erros de rede.

Valores de atributo

Os atributos são reportados com o melhor esforço e estão aproximadamente corretos. As atualizações de atributos podem ser perdidas em algumas circunstâncias, como a falha de um serviço ou a falha e reconstrução de um nó de grade.

Além disso, os atrasos de propagação podem retardar o relatório de atributos. Os valores atualizados para a

maioria dos atributos são enviados para o sistema StorageGRID em intervalos fixos. Pode demorar vários minutos até que uma atualização seja visível no sistema, e dois atributos que mudam mais ou menos simultaneamente podem ser reportados em momentos ligeiramente diferentes.

Analise as métricas de suporte

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

Antes de começar

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

Sobre esta tarefa

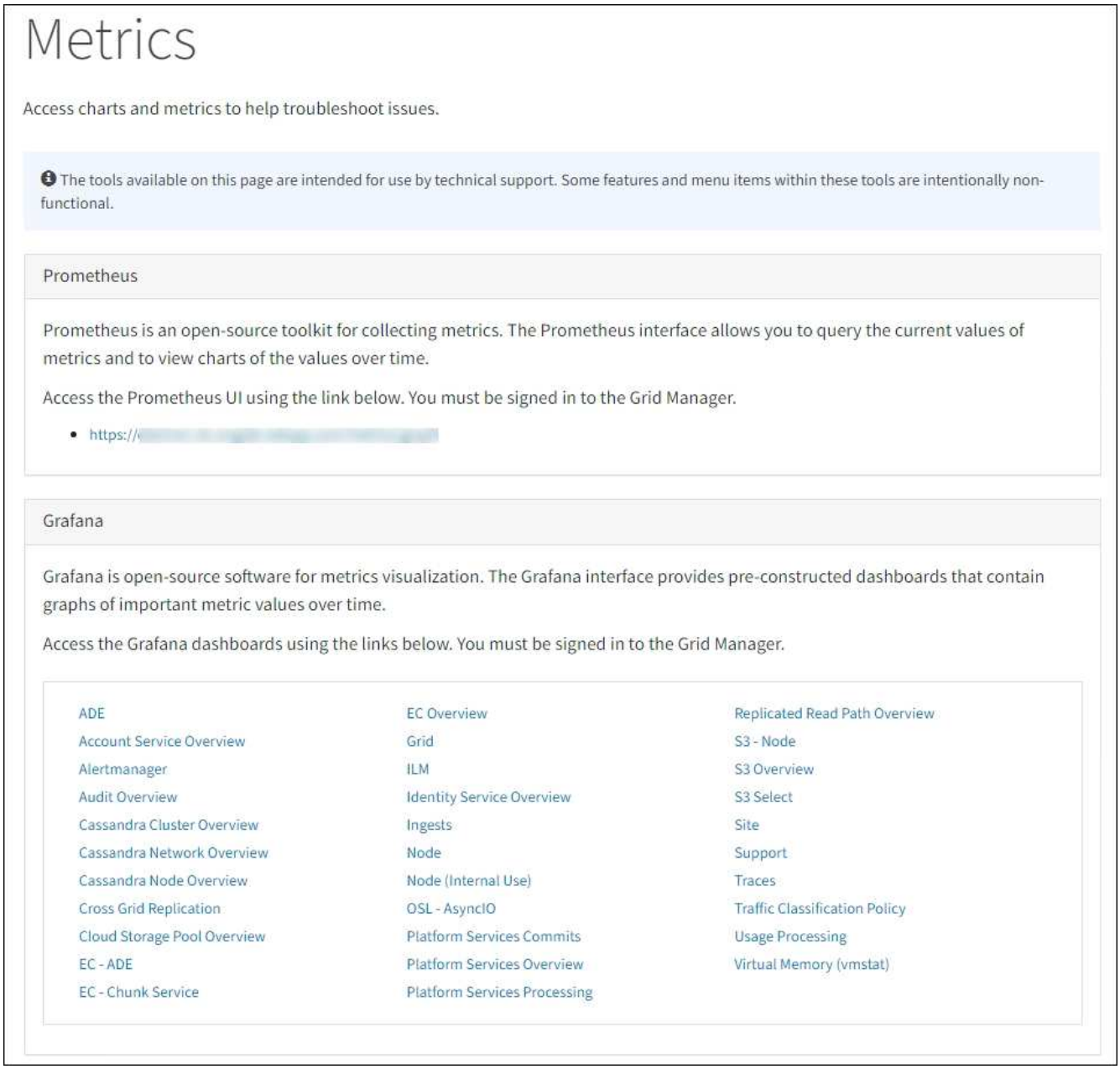
A página Metrics permite que você acesse as interfaces de usuário Prometheus e Grafana. Prometheus é um software de código aberto para coletar métricas. Grafana é um software de código aberto para visualização de métricas.

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

Passos

1. Conforme indicado pelo suporte técnico, selecione **SUPPORT** > **Tools** > **Metrics**.

   Um exemplo da página Metrics é mostrado aqui:



2. Para consultar os valores atuais das métricas do StorageGRID e visualizar gráficos dos valores ao longo do tempo, clique no link na seção Prometheus.

   A interface Prometheus é exibida. Você pode usar essa interface para executar consultas sobre as métricas disponíveis do StorageGRID e para traçar métricas do StorageGRID ao longo do tempo.

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

3. Para acessar painéis pré-construídos contendo gráficos de métricas do StorageGRID ao longo do tempo, clique nos links na seção Grafana.

   A interface Grafana para o link selecionado é exibida.

Execute o diagnóstico

Ao solucionar um problema, você pode trabalhar com o suporte técnico para executar diagnósticos no sistema StorageGRID e analisar os resultados.

- "Analise as métricas de suporte"
- "Métricas de Prometheus comumente usadas"

Antes de começar

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

Sobre esta tarefa

A página Diagnósticos executa um conjunto de verificações de diagnóstico no estado atual da grade. Cada verificação de diagnóstico pode ter um de três Estados:

-

- **Normal**: Todos os valores estão dentro do intervalo normal.
- **Atenção**: Um ou mais valores estão fora do intervalo normal.
- **Atenção**: Um ou mais dos valores estão significativamente fora do intervalo normal.

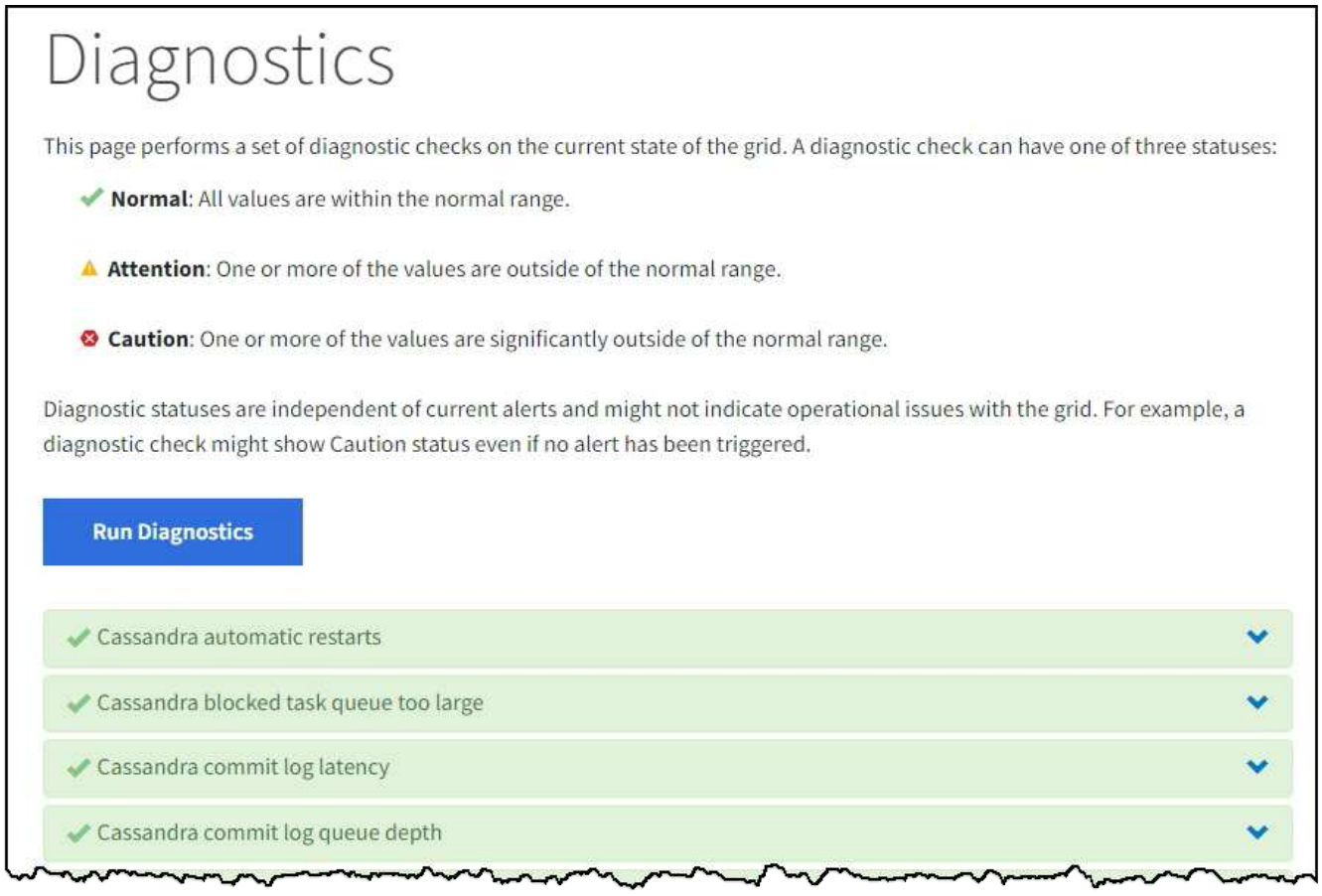
Os Estados de diagnóstico são independentes dos alertas atuais e podem não indicar problemas operacionais com a grade. Por exemplo, uma verificação de diagnóstico pode mostrar o estado de precaução mesmo que nenhum alerta tenha sido acionado.

Passos

1. Selecione **SUPPORT** > **Tools** > **Diagnostics**.

   A página Diagnósticos é exibida e lista os resultados de cada verificação de diagnóstico. Os resultados são classificados por gravidade (cuidado, atenção e, em seguida, normal). Dentro de cada gravidade, os resultados são ordenados alfabeticamente.

   Neste exemplo, todos os diagnósticos têm um estado normal.



2. Para saber mais sobre um diagnóstico específico, clique em qualquer lugar da linha.

   São apresentados detalhes sobre o diagnóstico e os seus resultados atuais. Os seguintes detalhes são listados:

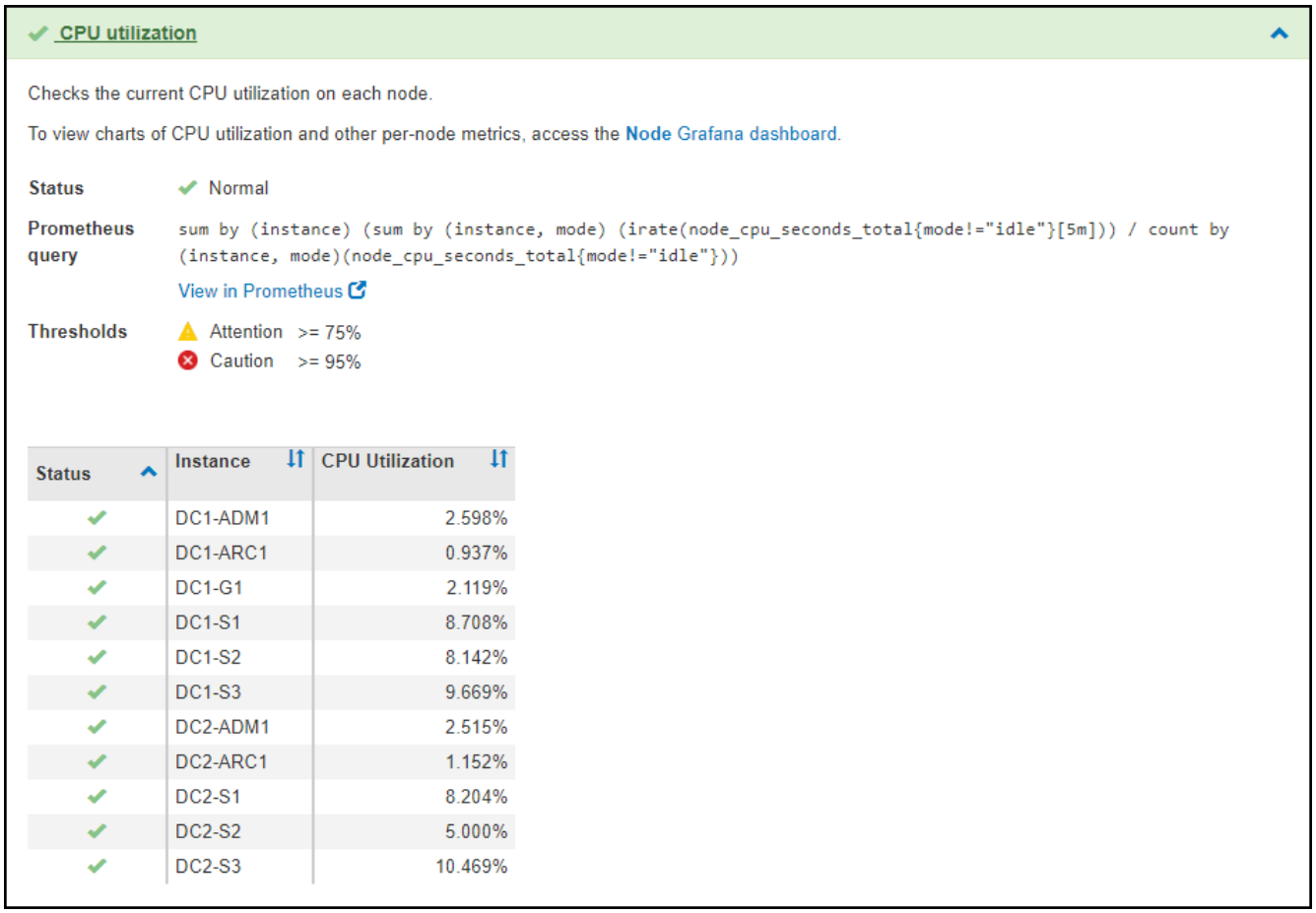
   - **Status**: O estado atual deste diagnóstico: Normal, atenção ou cuidado.
   - **Consulta Prometheus**: Se usada para o diagnóstico, a expressão Prometheus que foi usada para

gerar os valores de status. (Uma expressão Prometheus não é usada para todos os diagnósticos.)

- **Limiares**: Se disponíveis para o diagnóstico, os limiares definidos pelo sistema para cada estado de diagnóstico anormal. (Os valores de limite não são usados para todos os diagnósticos.)

  Não é possível alterar esses limites.

- **Valores de estado**: Uma tabela que mostra o estado e o valor do diagnóstico em todo o sistema StorageGRID. Neste exemplo, a utilização atual da CPU para cada nó em um sistema StorageGRID é mostrada. Todos os valores de nós estão abaixo dos limites de atenção e cuidado, portanto, o status geral do diagnóstico é normal.



3. **Opcional**: Para ver gráficos do Grafana relacionados a este diagnóstico, clique no link **painel do Grafana**.

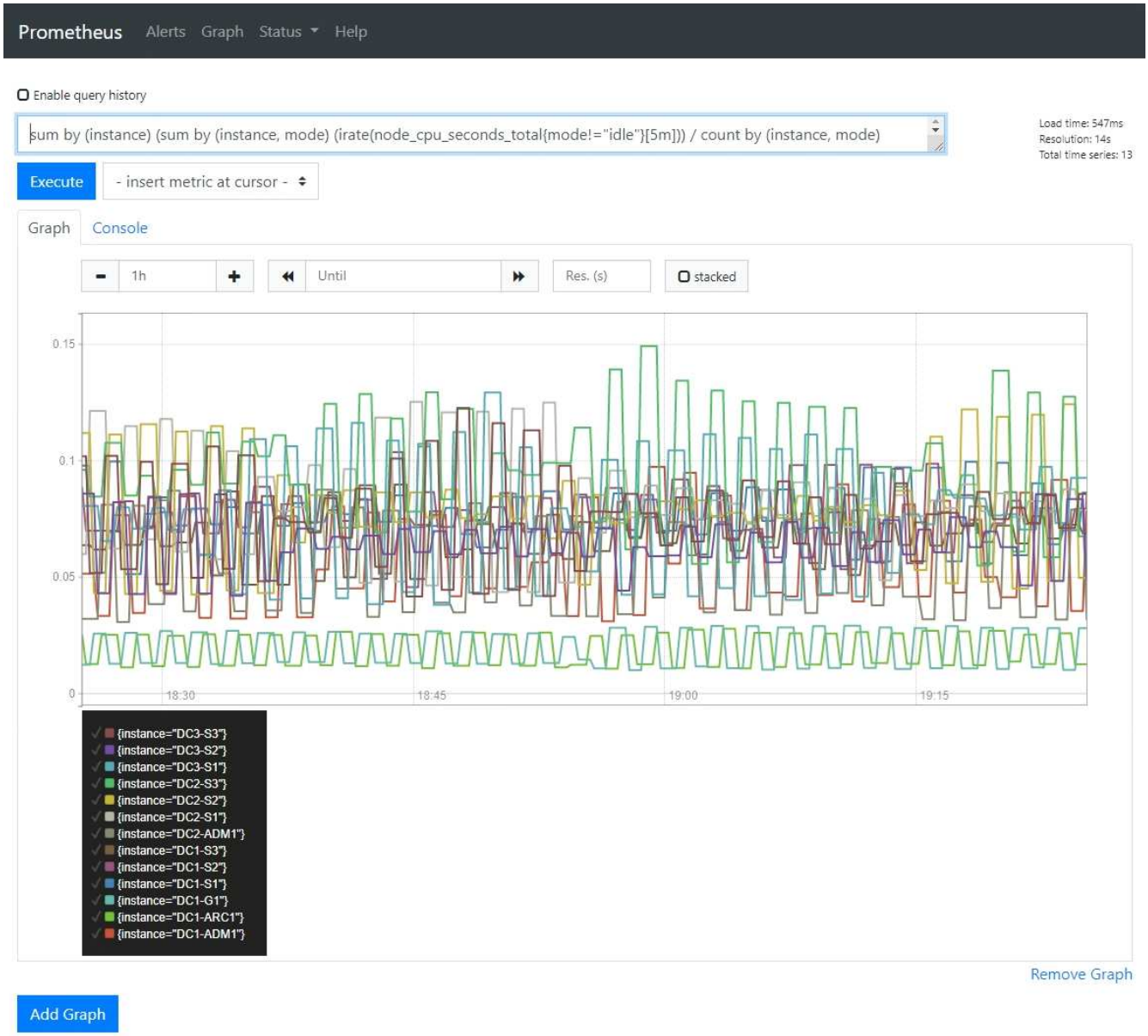
   Este link não é exibido para todos os diagnósticos.

   O painel do Grafana relacionado é exibido. Neste exemplo, o painel Node aparece mostrando a utilização da CPU ao longo do tempo para este nó, bem como outros gráficos Grafana para o nó.

   Você também pode acessar os painéis Grafana pré-construídos na seção Grafana da página **SUPPORT** > **Tools** > **Metrics**.

4. **Opcional**: Para ver um gráfico da expressão Prometheus ao longo do tempo, clique em **Exibir em Prometheus**.

   Aparece um gráfico Prometheus da expressão usada no diagnóstico.



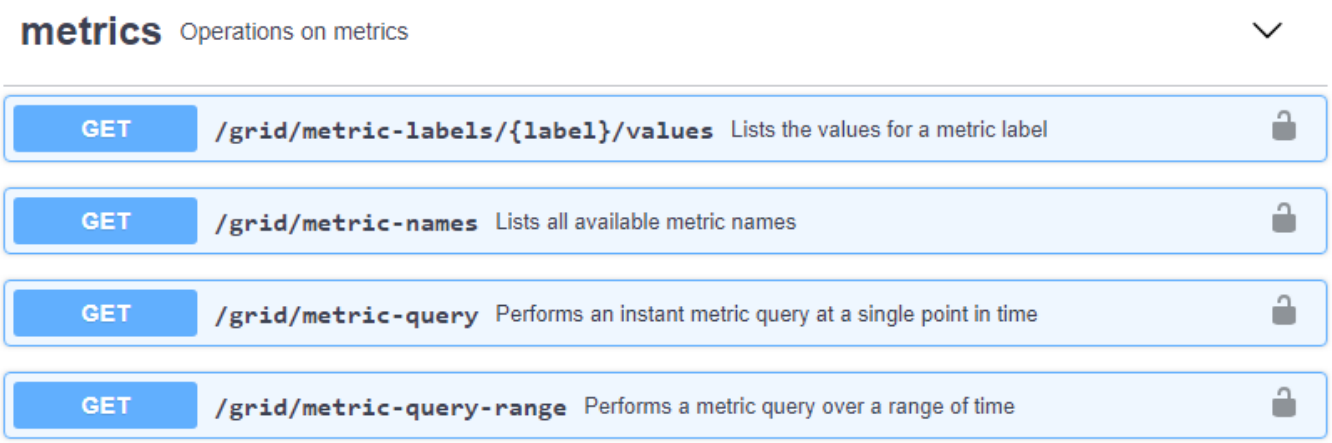
Crie aplicativos de monitoramento personalizados

Você pode criar aplicativos e painéis de monitoramento personalizados usando as métricas do StorageGRID disponíveis na API de gerenciamento de grade.

Se você quiser monitorar métricas que não são exibidas em uma página existente do Gerenciador de Grade ou se quiser criar painéis personalizados para o StorageGRID, use a API de Gerenciamento de Grade para consultar métricas do StorageGRID.

Você também pode acessar métricas do Prometheus diretamente com uma ferramenta de monitoramento externa, como Grafana. O uso de uma ferramenta externa requer que você carregue ou gere um certificado de cliente administrativo para permitir que o StorageGRID autentique a ferramenta para segurança. Consulte "Instruções para administrar o StorageGRID".

Para exibir as operações da API de métricas, incluindo a lista completa das métricas disponíveis, acesse o Gerenciador de Grade. Na parte superior da página, selecione o ícone de ajuda e selecione **Documentação da API** > **métricas**.



Os detalhes de como implementar um aplicativo de monitoramento personalizado estão além do escopo desta documentação.

Solucionar problemas do sistema StorageGRID

Solucionar problemas de um sistema StorageGRID

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

Normalmente, você pode resolver problemas sozinho. No entanto, talvez seja necessário encaminhar alguns problemas para o suporte técnico.

defina o problema

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

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

Pergunta	Exemplo de resposta
O que o sistema StorageGRID está fazendo ou não está fazendo? Quais são seus sintomas?	Os aplicativos clientes estão relatando que os objetos não podem ser ingeridos no StorageGRID.
Quando o problema começou?	A ingestão de objetos foi negada pela primeira vez em cerca de 14:50 em 8 de janeiro de 2020.
Como você notou o problema pela primeira vez?	Notificado pela aplicação do cliente. Também recebeu notificações por e-mail de alerta.
O problema acontece de forma consistente, ou apenas às vezes?	O problema está em curso.
Se o problema ocorrer regularmente, quais as etapas que o causam	O problema acontece toda vez que um cliente tenta ingerir um objeto.

Pergunta	Exemplo de resposta
Se o problema ocorrer intermitentemente, quando ocorre? Registre os horários de cada incidente que você está ciente.	O problema não é intermitente.
Você já viu esse problema antes? Com que frequência você teve esse problema no passado?	Esta é a primeira vez que vi esta questão.

Avaliar o risco e o impactos no sistema

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

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

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

Coletar dados

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

Tipo de dados a recolher	Por que coletar esses dados	Instruções
Crie a linha do tempo das mudanças recentes	As alterações ao seu sistema StorageGRID, à sua configuração ou ao seu ambiente podem causar um novo comportamento.	• Crie uma linha do tempo das mudanças recentes

Tipo de dados a recolher	Por que coletar esses dados	Instruções
Reveja alertas	Os alertas podem ajudá-lo a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre os problemas subjacentes que podem estar causando o problema. Revise a lista de alertas atuais para ver se o StorageGRID identificou a causa raiz de um problema para você. Reveja alertas acionados no passado para obter informações adicionais.	• "Ver alertas atuais e resolvidos"
Monitorar eventos	Os eventos incluem qualquer erro de sistema ou eventos de falha para um nó, incluindo erros como erros de rede. Monitore eventos para saber mais sobre problemas ou para ajudar na solução de problemas.	• "Monitorar eventos"
Identifique tendências usando gráficos e relatórios de texto	As tendências podem fornecer pistas valiosas sobre quando os problemas apareceram pela primeira vez e podem ajudá-lo a entender a rapidez com que as coisas estão mudando.	• "Use gráficos e gráficos" • "Use relatórios de texto"
Estabeleça linhas de base	Recolher informações sobre os níveis normais de vários valores operacionais. Esses valores de linha de base, e desvios dessas linhas de base, podem fornecer pistas valiosas.	• Estabeleça linhas de base
Execute testes de ingestão e recuperação	Para solucionar problemas de desempenho com ingestão e recuperação, use uma estação de trabalho para armazenar e recuperar objetos. Compare os resultados com os vistos ao usar o aplicativo cliente.	• "Monitore O PUT e obtenha desempenho"
Rever mensagens de auditoria	Revise as mensagens de auditoria para seguir as operações do StorageGRID em detalhes. Os detalhes nas mensagens de auditoria podem ser úteis para solucionar muitos tipos de problemas, incluindo problemas de desempenho.	• "Rever mensagens de auditoria"
Verifique os locais dos objetos e a integridade do armazenamento	Se você estiver tendo problemas de armazenamento, verifique se os objetos estão sendo colocados onde você espera. Verifique a integridade dos dados do objeto em um nó de storage.	• "Monitorar operações de verificação de objetos" • "Confirmar localizações de dados do objeto" • "Verifique a integridade do objeto"

Tipo de dados a recolher	Por que coletar esses dados	Instruções
Coletar dados para suporte técnico	O suporte técnico pode solicitar que você colete dados ou revise informações específicas para ajudar a solucionar problemas.	• "Colete arquivos de log e dados do sistema" • "Acione manualmente um pacote AutoSupport" • "Analise as métricas de suporte"

Crie uma linha do tempo de mudanças recentes

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

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

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

Hora da mudança	Tipo de alteração	Detalhes
Por exemplo: • Quando você iniciou a recuperação do nó? • Quando a atualização de software foi concluída? • Interrompeu o processo?	O que aconteceu? O que fez?	Documente todos os detalhes relevantes sobre a alteração. Por exemplo: • Detalhes das alterações de rede. • Qual hotfix foi instalado. • Como as cargas de trabalho do cliente mudaram. Certifique-se de observar se mais de uma mudança estava acontecendo ao mesmo tempo. Por exemplo, essa alteração foi feita enquanto uma atualização estava em andamento?

Exemplos de mudanças recentes significativas

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi recentemente instalado, expandido ou recuperado?
- O sistema foi atualizado recentemente? Foi aplicado um hotfix?
- Algum hardware foi reparado ou alterado recentemente?
- A política ILM foi atualizada?

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

Estabeleça linhas de base

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

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

Propriedade	Valor	Como obter
Consumo médio de metadados	GB consumido/dia Percentagem consumida/dia	Vá para o Gerenciador de Grade. Na página nós, selecione toda a grade ou um site e vá para a guia armazenamento. No gráfico armazenamento usado - metadados de objetos, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar quanto armazenamento de metadados é consumido diariamente Você pode coletar essas informações para todo o sistema ou para um data center específico.
Taxa de operações S3/Swift	Operações/segundo	No painel do Grid Manager, selecione **Performance** > **S3 operations** ou **Performance** > **Swift operations**. Para ver as taxas de ingestão e recuperação e contagens de um site ou nó específico, selecione **NÓS** > ***site ou nó de armazenamento*** > **objetos**. Posicione o cursor sobre o gráfico de ingestão e recuperação para S3.
Falha nas operações S3/Swift	Operações	Selecione **SUPPORT** > **Tools** > **Grid topology**. Na guia Visão geral na seção operações da API, veja o valor de operações S3 - Falha ou operações rápidas - Falha.
Taxa de avaliação ILM	Objetos/segundo	Na página nós, selecione ***grid*** > **ILM**. No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de linha de base para **taxa de avaliação** para o seu sistema.
Taxa de digitalização ILM	Objetos/segundo	Selecione **NODES** > ***grid*** > **ILM**. No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de linha de base para **taxa de digitalização** para o seu sistema.
Objetos enfileirados de operações do cliente	Objetos/segundo	Selecione **NODES** > ***grid*** > **ILM**. No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de linha de base para **objetos enfileirados (de operações do cliente)** para o seu sistema.

Propriedade	Valor	Como obter
Latência média da consulta	Milissegundos	Selecione **NODES** > ***Storage Node*** > **Objects**. Na tabela consultas, exiba o valor da latência média.

Analisar dados

Use as informações coletadas para determinar a causa do problema e possíveis soluções.

A análise é dependente de problemas, mas em geral:

- Localize pontos de falha e gargalos usando os alertas.
- Reconstrua o histórico do problema usando o histórico de alertas e os gráficos.
- Use gráficos para encontrar anomalias e comparar a situação do problema com a operação normal.

Lista de verificação de informações de encaminhamento

Se você não conseguir resolver o problema sozinho, entre em Contato com o suporte técnico. Antes de entrar em Contato com o suporte técnico, reúna as informações listadas na tabela a seguir para facilitar a resolução de problemas.

✔	Item	Notas
	Declaração do problema	Quais são os sintomas do problema? Quando o problema começou? Isso acontece de forma consistente ou intermitente? Se intermitentemente, que horas ocorreu? Defina o problema
	Avaliação de impactos	Qual é a gravidade do problema? Qual é o impactos na aplicação cliente? • O cliente foi conetado com sucesso antes? • O cliente pode obter, recuperar e excluir dados?
	ID do sistema StorageGRID	Selecione **MAINTENANCE** > **System** > **License**. A ID do sistema StorageGRID é apresentada como parte da licença atual.
	Versão do software	Na parte superior do Gerenciador de Grade, selecione o ícone de ajuda e selecione **sobre** para ver a versão do StorageGRID.

✔	Item	Notas
	Personalização	Resumir como o seu sistema StorageGRID está configurado. Por exemplo, liste o seguinte: • A grade usa compactação de storage, criptografia de storage ou conformidade? • O ILM faz objetos replicados ou codificados por apagamento? O ILM garante a redundância do site? As regras do ILM usam os comportamentos de ingestão equilibrada, rigorosa ou dupla confirmação?
	Ficheiros de registo e dados do sistema	Recolha ficheiros de registo e dados do sistema para o seu sistema. Selecione **SUPPORT** > **Tools** > **Logs**. Você pode coletar logs para toda a grade ou para nós selecionados. Se você estiver coletando logs somente para nós selecionados, certifique-se de incluir pelo menos um nó de armazenamento que tenha o serviço ADC. (Os três primeiros nós de storage em um local incluem o serviço ADC.) "Colete arquivos de log e dados do sistema"
	Informações da linha de base	Colete informações básicas sobre operações de ingestão, operações de recuperação e consumo de armazenamento. Estabeleça linhas de base
	Cronograma das mudanças recentes	Crie uma linha do tempo que resume quaisquer alterações recentes ao sistema ou ao seu ambiente. Crie uma linha do tempo das mudanças recentes
	Histórico de esforços para diagnosticar o problema	Se você tomou medidas para diagnosticar ou solucionar o problema sozinho, certifique-se de Registrar as etapas que você tomou e o resultado.

Solucionar problemas de objetos e storage

Confirmar localizações de dados do objeto

Dependendo do problema, você pode querer "confirme onde os dados do objeto estão sendo armazenados". Por exemplo, você pode querer verificar se a política ILM está funcionando como esperado e os dados do objeto estão sendo armazenados onde se pretende.

Antes de começar

- Você deve ter um identificador de objeto, que pode ser um dos seguintes:

- **UUID**: O Identificador universalmente exclusivo do objeto. Introduza o UUID em todas as maiúsculas.
- **CBID**: O identificador exclusivo do objeto dentro do StorageGRID . Você pode obter o CBID de um objeto a partir do log de auditoria. Introduza o CBID em todas as maiúsculas.
- **S3 bucket e chave de objeto**: Quando um objeto é ingerido através do "Interface S3", o aplicativo cliente usa uma combinação de bucket e chave de objeto para armazenar e identificar o objeto.

Passos

1. Selecione **ILM** > **Object metadata lookup**.
2. Digite o identificador do objeto no campo **Identificador**.

   Você pode inserir um UUID, CBID, S3 bucket/object-key ou Swift container/object-name.

3. Se você quiser procurar uma versão específica do objeto, digite o ID da versão (opcional).

4. Selecione **Procurar**.

   O "resultados de pesquisa de metadados de objetos" aparece. Esta página lista os seguintes tipos de informações:

   - Metadados do sistema, incluindo o ID do objeto (UUID), o ID da versão (opcional), o nome do objeto, o nome do contentor, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e hora em que o objeto foi criado pela primeira vez e a data e hora em que o objeto foi modificado pela última vez.
   - Quaisquer pares de valor-chave de metadados de usuário personalizados associados ao objeto.
   - Para objetos S3D, qualquer par de chave-valor de marca de objeto associado ao objeto.
   - Para cópias de objetos replicadas, o local de storage atual de cada cópia.
   - Para cópias de objetos com codificação de apagamento, o local de storage atual de cada fragmento.
   - Para cópias de objetos em um Cloud Storage Pool, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
   - Para objetos segmentados e objetos de várias partes, uma lista de segmentos, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, apenas os primeiros 100 segmentos são mostrados.
   - Todos os metadados de objetos no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não são garantidos para persistir de liberação para liberação.

     O exemplo a seguir mostra os resultados da pesquisa de metadados de objeto para um objeto de teste

S3 que é armazenado como duas cópias replicadas.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Falhas no armazenamento de objetos (volume de storage)

O storage subjacente em um nó de storage é dividido em armazenamentos de objetos. Os armazenamentos de objetos também são conhecidos como volumes de armazenamento.

Você pode exibir informações de armazenamento de objetos para cada nó de armazenamento. Os armazenamentos de objetos são mostrados na parte inferior da página **NÓS** > ***Storage Node*** > **Storage**.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

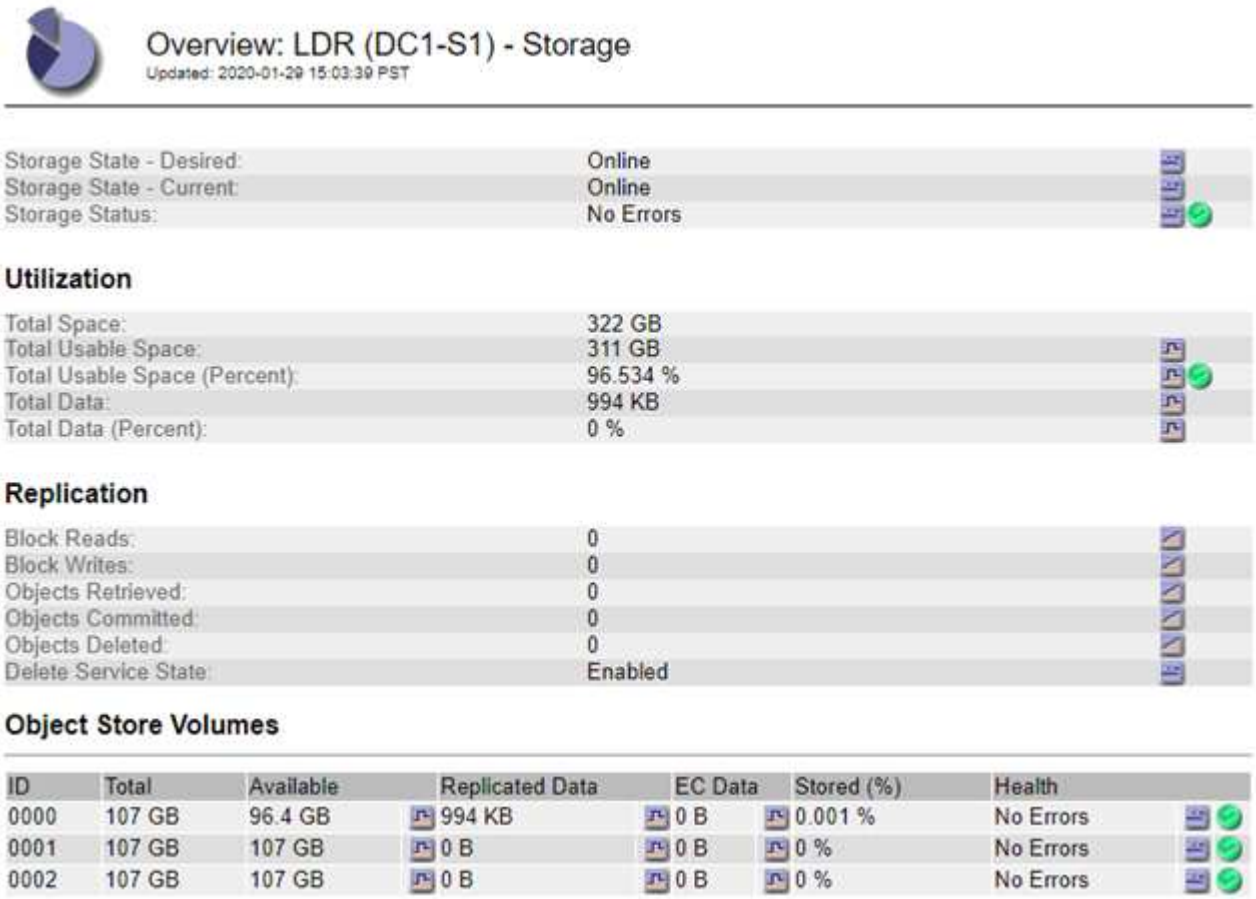
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Para ver mais "Detalhes sobre cada nó de storage", siga estas etapas:

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***site*** > ***Storage Node*** > **LDR** > **Storage** > **Overview** > **Main**.



Dependendo da natureza da falha, as falhas com um volume de armazenamento podem ser refletidas no "alertas de volume de storage". Se um volume de armazenamento falhar, você deve reparar o volume de armazenamento com falha para restaurar o nó de armazenamento para a funcionalidade completa o mais rápido possível. Se necessário, você pode ir para a guia **Configuração** e "Coloque o nó de storage em um estado somente leitura" para que o sistema StorageGRID possa usá-lo para recuperação de dados enquanto você se prepara para uma recuperação completa do servidor.

Verifique a integridade do objeto

O sistema StorageGRID verifica a integridade dos dados de objetos nos nós de storage, verificando se há objetos corrompidos ou ausentes.

Existem dois processos de verificação: Verificação de fundo e verificação de existência de objeto (anteriormente chamada de verificação de primeiro plano). Eles trabalham juntos para garantir a integridade dos dados. A verificação em segundo plano é executada automaticamente e verifica continuamente a correção dos dados do objeto. Verificação de existência de objeto pode ser acionada por um usuário para verificar mais rapidamente a existência (embora não a correção) de objetos.

O que é a verificação em segundo plano?

O processo de verificação em segundo plano verifica automaticamente e continuamente os nós de storage em

busca de cópias corrompidas de dados de objetos e tenta reparar automaticamente quaisquer problemas encontrados.

A verificação em segundo plano verifica a integridade dos objetos replicados e dos objetos codificados por apagamento, da seguinte forma:

- **Objetos replicados**: Se o processo de verificação em segundo plano encontrar um objeto replicado que está corrompido, a cópia corrompida será removida de seu local e colocada em quarentena em outro lugar no nó de armazenamento. Em seguida, uma nova cópia não corrompida é gerada e colocada para satisfazer as políticas ILM ativas. A nova cópia pode não ser colocada no nó de armazenamento que foi usado para a cópia original.

> Os dados de objetos corrompidos são colocados em quarentena em vez de excluídos do sistema, para que ainda possam ser acessados. Para obter mais informações sobre como acessar dados de objetos em quarentena, entre em Contato com o suporte técnico.

- **Objetos codificados por apagamento**: Se o processo de verificação em segundo plano detetar que um fragmento de um objeto codificado por apagamento está corrompido, o StorageGRID tentará automaticamente reconstruir o fragmento ausente no mesmo nó de storage, usando os dados restantes e fragmentos de paridade. Se o fragmento corrompido não puder ser reconstruído, uma tentativa é feita para recuperar outra cópia do objeto. Se a recuperação for bem-sucedida, uma avaliação ILM será executada para criar uma cópia de substituição do objeto codificado de apagamento.

  O processo de verificação em segundo plano verifica objetos apenas nos nós de storage. Ele não verifica objetos em um pool de armazenamento em 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 relacionados à verificação em segundo plano

Se o sistema detetar um objeto corrompido que ele não pode corrigir automaticamente (porque a corrupção impede que o objeto seja identificado), o alerta **Objeto corrompido não identificado detetado** é acionado.

Se a verificação em segundo plano não puder substituir um objeto corrompido porque ele não consegue localizar outra cópia, o alerta **objetos perdidos** é acionado.

Altere a taxa de verificação em segundo plano

Você pode alterar a taxa na qual a verificação em segundo plano verifica os dados de objetos replicados em um nó de storage se tiver preocupações com a integridade dos dados.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

Você pode alterar a taxa de verificação para verificação em segundo plano em um nó de storage:

- Adaptive (adaptável): Predefinição. A tarefa foi projetada para verificar no máximo 4 MB/s ou 10 objetos/s

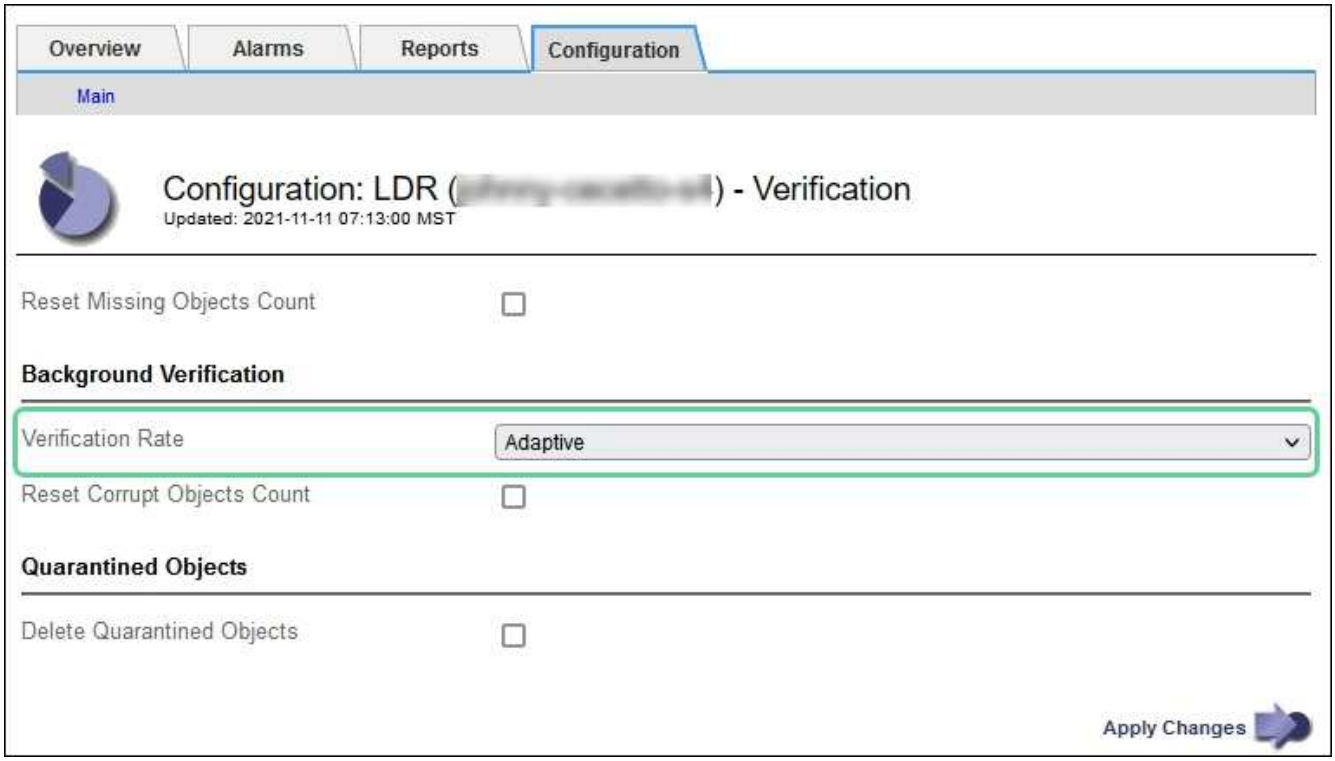
(o que for excedido primeiro).

- Alta: A verificação do armazenamento prossegue rapidamente, a uma taxa que pode retardar as atividades normais do sistema.

Use a taxa de verificação alta somente quando suspeitar que uma falha de hardware ou software pode ter dados de objeto corrompidos. Após a conclusão da verificação de fundo de alta prioridade, a taxa de verificação é automaticamente redefinida para Adaptive (adaptável).

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Storage Node*** > **LDR** > **Verificação**.
3. Selecione **Configuração** > **Principal**.
4. Aceda a **LDR** > **Verificação** > **Configuração** > **Principal**.
5. Em Verificação em segundo plano, selecione **taxa de verificação** > **alta** ou **taxa de verificação** > **adaptável**.



6. Clique em **aplicar alterações**.
7. Monitore os resultados da verificação em segundo plano para objetos replicados.
   a. Vá para **NODES** > ***Storage Node*** > **Objects**.
   b. Na seção Verificação, monitore os valores para **objetos corrompidos** e **objetos corrompidos não identificados**.

      Se a verificação em segundo plano encontrar dados de objeto replicados corrompidos, a métrica **objetos corrompidos** será incrementada e o StorageGRID tentará extrair o identificador de objeto dos dados, da seguinte forma:

      - Se o identificador do objeto puder ser extraído, o StorageGRID criará automaticamente uma nova cópia dos dados do objeto. A nova cópia pode ser feita em qualquer lugar do sistema

StorageGRID que satisfaça as políticas ativas de ILM.

- Se o identificador de objeto não puder ser extraído (porque foi corrompido), a métrica **objetos corrompidos não identificados** é incrementada e o alerta **Objeto corrompido não identificado detetado** é acionado.

c. Se forem encontrados dados de objeto replicados corrompidos, entre em Contato com o suporte técnico para determinar a causa raiz da corrupção.

8. Monitore os resultados da verificação em segundo plano para objetos codificados por apagamento.

   Se a verificação em segundo plano encontrar fragmentos corrompidos de dados de objetos codificados por apagamento, o atributo fragmentos corrompidos detetados é incrementado. O StorageGRID se recupera reconstruindo o fragmento corrompido no mesmo nó de storage.

   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***Storage Node*** > **LDR** > **Erasure Coding**.
   c. Na tabela resultados da verificação, monitore o atributo fragmentos corrompidos detetados (ECCD).

9. Depois que os objetos corrompidos forem restaurados automaticamente pelo sistema StorageGRID, redefina a contagem de objetos corrompidos.
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***Storage Node*** > **LDR** > **Verificação** > **Configuração**.
   c. Selecione **Redefinir contagem de objetos corrompidos**.
   d. Clique em **aplicar alterações**.

10. Se você estiver confiante de que objetos em quarentena não são necessários, você pode excluí-los.

    Se o alerta **Objects Lost** foi acionado, o suporte técnico pode querer acessar objetos em quarentena para ajudar a depurar o problema subjacente ou tentar a recuperação de dados.

    a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
    b. Selecione ***Storage Node*** > **LDR** > **Verificação** > **Configuração**.
    c. Selecione **Excluir objetos em quarentena**.
    d. Selecione **aplicar alterações**.

O que é verificação de existência de objeto?

A verificação de existência de objeto verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados por apagamento existem em um nó de storage. A verificação de existência do objeto não verifica os dados do objeto em si (a verificação em segundo plano faz isso); em vez disso, fornece uma maneira de verificar a integridade dos dispositivos de armazenamento, especialmente se um problema de hardware recente poderia ter afetado a integridade dos dados.

Ao contrário da verificação em segundo plano, que ocorre automaticamente, você deve iniciar manualmente uma tarefa de verificação de existência de objeto.

A verificação de existência de objeto lê os metadados de cada objeto armazenado no StorageGRID e verifica a existência de cópias de objeto replicadas e fragmentos de objeto codificados por apagamento. Quaisquer dados em falta são tratados da seguinte forma:

- **Cópias replicadas**: Se uma cópia de dados de objetos replicados estiver ausente, o StorageGRID tentará substituir automaticamente a cópia de uma cópia armazenada em outro lugar do sistema. O nó de

armazenamento executa uma cópia existente através de uma avaliação ILM, que determinará que a política ILM atual não está mais sendo atendida para este objeto porque outra cópia está faltando. Uma nova cópia é gerada e colocada para satisfazer as políticas de ILM ativas do sistema. Esta nova cópia pode não ser colocada no mesmo local onde a cópia em falta foi armazenada.

- **Fragmentos codificados por apagamento**: Se um fragmento de um objeto codificado por apagamento estiver ausente, o StorageGRID tentará reconstruir automaticamente o fragmento ausente no mesmo nó de storage usando os fragmentos restantes. Se o fragmento ausente não puder ser reconstruído (porque muitos fragmentos foram perdidos), o ILM tenta encontrar outra cópia do objeto, que ele pode usar para gerar um novo fragmento codificado de apagamento.

Executar verificação de existência de objeto

Você cria e executa um trabalho de verificação de existência de objeto de cada vez. Ao criar uma tarefa, você seleciona os nós de storage e os volumes que deseja verificar. Você também seleciona a consistência do trabalho.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você garantiu que os nós de storage que deseja verificar estão online. Selecione **NÓS** para exibir a tabela de nós. Certifique-se de que nenhum ícone de alerta aparece ao lado do nome do nó para os nós que você deseja verificar.
- Você garantiu que os seguintes procedimentos estão **não** sendo executados nos nós que deseja verificar:
  - Expansão de grade para adicionar um nó de storage
  - Desativação do nó de storage
  - Recuperação de um volume de armazenamento com falha
  - Recuperação de um nó de armazenamento com uma unidade de sistema com falha
  - Rebalancear a EC
  - Clone de nó do dispositivo

A verificação existência de objeto não fornece informações úteis enquanto estes procedimentos estão em curso.

Sobre esta tarefa

Uma tarefa de verificação de existência de objeto pode levar dias ou semanas para ser concluída, dependendo do número de objetos na grade, dos nós e volumes de storage selecionados e da consistência selecionada. Você pode executar apenas uma tarefa de cada vez, mas pode selecionar vários nós e volumes de storage ao mesmo tempo.

Passos

1. Selecione **MAINTENANCE** > **Tasks** > **Object existence check**.
2. Selecione **criar trabalho**. O assistente criar uma tarefa de verificação de existência de objeto é exibido.
3. Selecione os nós que contêm os volumes que você deseja verificar. Para selecionar todos os nós on-line, marque a caixa de seleção **Nome do nó** no cabeçalho da coluna.

   Você pode pesquisar por nome do nó ou site.

   Não é possível selecionar nós que não estão conetados à grade.

4. Selecione **continuar**.
5. Selecione um ou mais volumes para cada nó na lista. Você pode pesquisar volumes usando o número do volume de armazenamento ou o nome do nó.

   Para selecionar todos os volumes para cada nó selecionado, marque a caixa de seleção **volume de armazenamento** no cabeçalho da coluna.

6. Selecione **continuar**.
7. Selecione a consistência do trabalho.

   A consistência determina quantas cópias dos metadados de objetos são usadas para a verificação de existência do objeto.

   - * Strong-site*: Duas cópias de metadados em um único site.
   - **Strong-global**: Duas cópias de metadados em cada local.
   - **Todos** (padrão): Todas as três cópias de metadados em cada site.

     Para obter mais informações sobre consistência, consulte as descrições no assistente.

8. Selecione **continuar**.
9. Reveja e verifique as suas seleções. Você pode selecionar **Previous** para ir para uma etapa anterior no assistente para atualizar suas seleções.

   Uma tarefa de verificação de existência de objeto é gerada e é executada até que uma das seguintes situações ocorra:

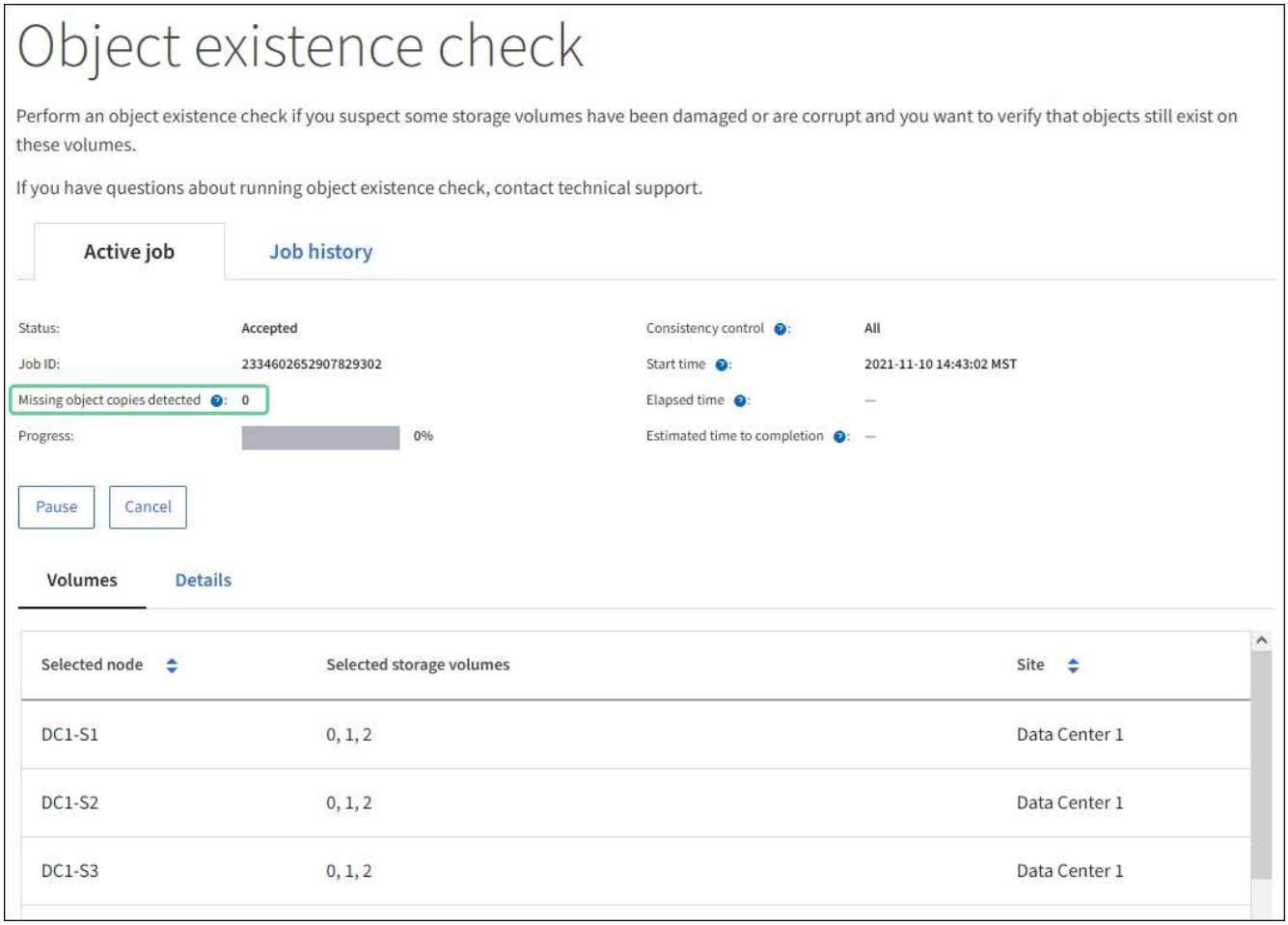
   - O trabalho é concluído.
   - Pausa ou cancelar o trabalho. Você pode retomar um trabalho em pausa, mas não pode retomar um trabalho cancelado.
   - O trabalho vai abaixo. O alerta **Object existence check has stalled** é acionado. Siga as ações corretivas especificadas para o alerta.
   - O trabalho falha. O alerta **Verificação de existência de objeto falhou** é acionado. Siga as ações corretivas especificadas para o alerta.
   - É apresentada uma mensagem "Service unavailable" (Serviço indisponível) ou "Internal Server error" (erro interno do servidor). Após um minuto, atualize a página para continuar a monitorizar o trabalho.

     Conforme necessário, você pode navegar para longe da página de verificação existência de Objeto e retornar para continuar monitorando o trabalho.

10. À medida que a tarefa é executada, exiba a guia **trabalho ativo** e observe o valor de cópias de objetos ausentes detetadas.

    Esse valor representa o número total de cópias ausentes de objetos replicados e objetos codificados por apagamento com um ou mais fragmentos ausentes.

    Se o número de cópias de objetos ausentes detetadas for maior que 100, pode haver um problema com o armazenamento do nó de armazenamento.



11. Após a conclusão do trabalho, execute quaisquer ações adicionais necessárias:
    - Se as cópias de objeto em falta detetadas forem zero, não foram encontrados problemas. Nenhuma ação é necessária.
    - Se as cópias de objetos em falta detetadas forem maiores que zero e o alerta **objetos perdidos** não tiver sido acionado, todas as cópias em falta foram reparadas pelo sistema. Verifique se quaisquer problemas de hardware foram corrigidos para evitar danos futuros às cópias de objetos.
    - Se as cópias de objetos em falta detetadas forem maiores que zero e o alerta **objetos perdidos** tiver sido acionado, a integridade dos dados poderá ser afetada. Entre em Contato com o suporte técnico.
    - Você pode investigar cópias de objetos perdidos usando grep para extrair as mensagens de auditoria LLST: `grep LLST audit_file_name`.

      Este procedimento é semelhante ao de "investigando objetos perdidos", embora para cópias de objetos que você pesquise em `LLST` vez `OLST` de .

12. Se você selecionou a consistência forte ou forte-global para a tarefa, aguarde aproximadamente três semanas pela consistência dos metadados e execute novamente a tarefa nos mesmos volumes novamente.

    Quando o StorageGRID tiver tido tempo para alcançar a consistência de metadados para os nós e volumes incluídos na tarefa, a execução novamente da tarefa pode limpar cópias de objetos ausentes relatadas erroneamente ou fazer com que cópias de objetos adicionais sejam verificadas se elas foram perdidas.

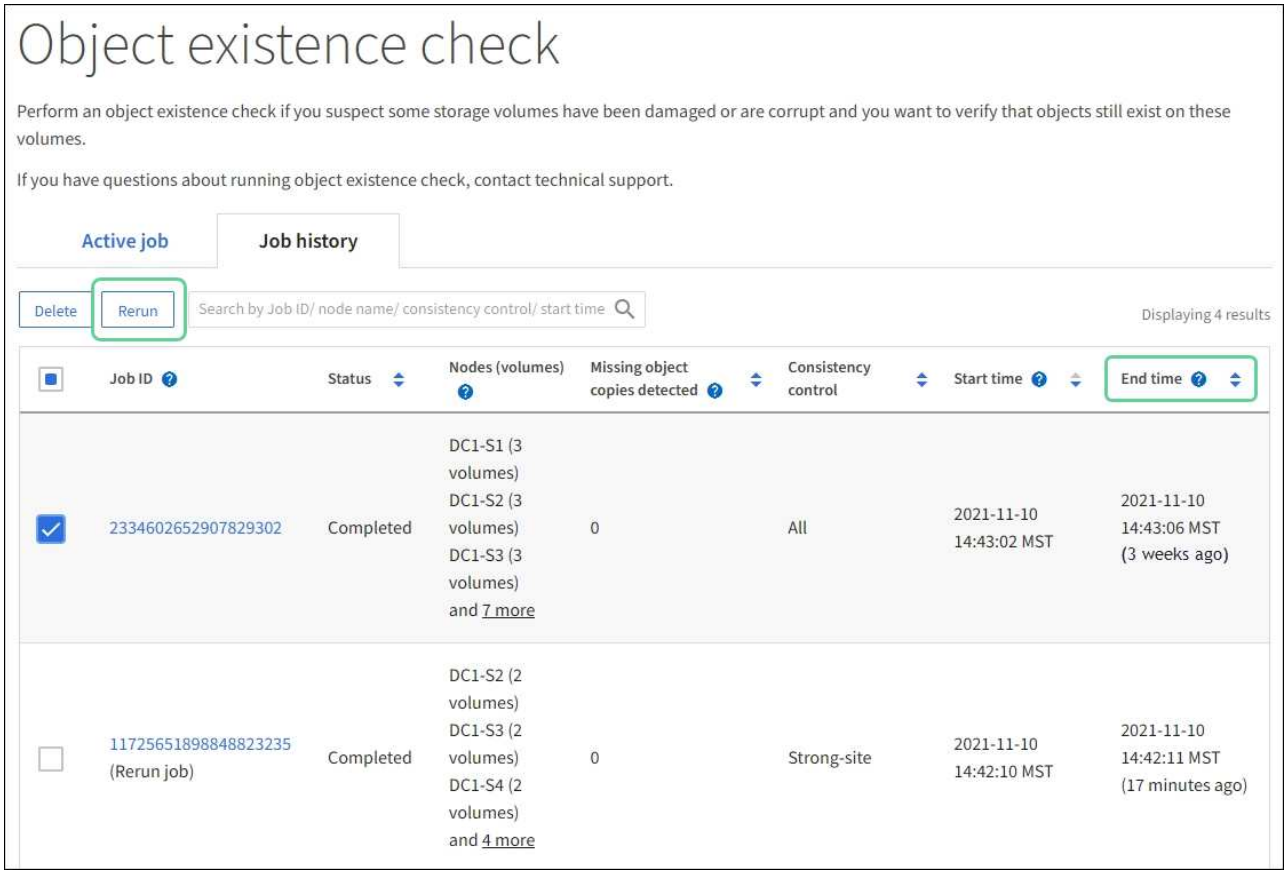
    a. Selecione **MAINTENANCE** > **Object existence check** > **Job history**.

b. Determine quais trabalhos estão prontos para serem executados novamente:

   i. Olhe para a coluna **hora de fim** para determinar quais trabalhos foram executados há mais de três semanas.

   ii. Para esses trabalhos, examine a coluna de controle de consistência para sites fortes ou globais.

c. Selecione a caixa de verificação para cada trabalho que pretende executar novamente e, em seguida, selecione **Reexecutar**.



d. No assistente de reexecução de trabalhos, reveja os nós e volumes selecionados e a consistência.

e. Quando estiver pronto para executar novamente os trabalhos, selecione **Reexecutar**.

É apresentado o separador trabalho ativo. Todos os trabalhos selecionados são reexecutados como um trabalho com consistência de um local forte. Um campo **trabalhos relacionados** na seção Detalhes lista os IDs dos trabalhos originais.

Depois de terminar

Se ainda tiver preocupações sobre a integridade dos dados, aceda a **SUPPORT** > **Tools** > **Grid topoly** > ***site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration** > **Main** e aumente a taxa de verificação em segundo plano. A verificação em segundo plano verifica a exatidão de todos os dados de objetos armazenados e repara quaisquer problemas que encontrar. Encontrar e reparar possíveis problemas o mais rápido possível reduz o risco de perda de dados.

Resolução de problemas S3 COLOQUE o alerta tamanho do objeto demasiado grande

O alerta S3 PUT Object Size too large (tamanho do objeto de COLOCAÇÃO muito grande) é acionado se um locatário tentar uma operação PutObject não multiparte que exceda o limite de tamanho S3 de 5 GiB.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Determine quais locatários usam objetos maiores que 5 GiB, para que você possa notificá-los.

Passos

1. Aceda a **CONFIGURATION** > **Monitoring** > **Audit and syslog Server**.
2. Se as gravações do cliente forem normais, acesse o log de auditoria:

   a. Introduza `ssh admin@primary_Admin_Node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

   e. Introduza `cd /var/local/log`

   "Saiba mais sobre os destinos para informações de auditoria".

   f. Identifique quais locatários estão usando objetos maiores que 5 GiB.

      i. Introduza `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

      ii. Para cada mensagem de auditoria nos resultados, observe `S3AI` o campo para determinar o ID da conta do locatário. Use os outros campos da mensagem para determinar qual endereço IP foi usado pelo cliente, pelo bucket e pelo objeto:

Código	Descrição
SAIP	IP de origem
S3AI	ID do inquilino
S3BK	Balde
S3KY	Objeto
CSIZ	Tamanho (bytes)

Exemplo de resultados de log de auditoria

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Se as gravações do cliente não forem normais, use o ID do locatário do alerta para identificar o locatário:

   a. Aceda a **SUPPORT** > **Tools** > **Logs**. Colete logs de aplicativos para o nó de armazenamento no alerta. Especifique 15 minutos antes e depois do alerta.

   b. Extraia o arquivo e vá `bycast.log` para :

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. PESQUISE o log `method=PUT` e identifique o cliente no `clientIP` campo.

      Exemplo bycast.log

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Informe aos locatários que o tamanho máximo do PutObject é de 5 GiB e para usar uploads de várias partes para objetos maiores que 5 GiB.
5. Ignore o alerta por uma semana se o aplicativo tiver sido alterado.

Solucionar problemas de dados de objetos perdidos e ausentes

Solucionar problemas de dados de objetos perdidos e ausentes

Os objetos podem ser recuperados por vários motivos, incluindo solicitações de leitura de um aplicativo cliente, verificações em segundo plano de dados de objeto replicados, reavaliações ILM e a restauração de dados de objeto durante a recuperação de um nó de armazenamento.

O sistema StorageGRID usa informações de localização nos metadados de um objeto para determinar a partir de qual local recuperar o objeto. Se uma cópia do objeto não for encontrada no local esperado, o sistema tentará recuperar outra cópia do objeto de outra parte do sistema, assumindo que a política ILM contém uma regra para fazer duas ou mais cópias do objeto.

Se esta recuperação for bem-sucedida, o sistema StorageGRID substitui a cópia em falta do objeto. Caso contrário, o alerta **objetos perdidos** é acionado, da seguinte forma:

- Para cópias replicadas, se outra cópia não puder ser recuperada, o objeto será considerado perdido e o alerta será acionado.
- Para cópias codificadas por apagamento, se uma cópia não puder ser recuperada do local esperado, o atributo cópias corrompidas detetadas (ECOR) será incrementado por um antes de uma tentativa ser feita para recuperar uma cópia de outro local. Se nenhuma outra cópia for encontrada, o alerta é acionado.

Você deve investigar todos os alertas **objetos perdidos** imediatamente para determinar a causa raiz da perda e determinar se o objeto ainda pode existir em um nó de armazenamento offline ou de outra forma indisponível no momento. "Investigue objetos perdidos"Consulte .

No caso de perda de dados de objetos sem cópias, não há solução de recuperação. No entanto, você deve redefinir o contador de objetos perdidos para evitar que objetos perdidos conhecidos mascarem quaisquer novos objetos perdidos. "Repor contagens de objetos perdidas e em falta"Consulte .

Investigue objetos perdidos

Quando o alerta **Objects Lost** é acionado, você deve investigar imediatamente. Colete informações sobre os objetos afetados e entre em Contato com o suporte técnico.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

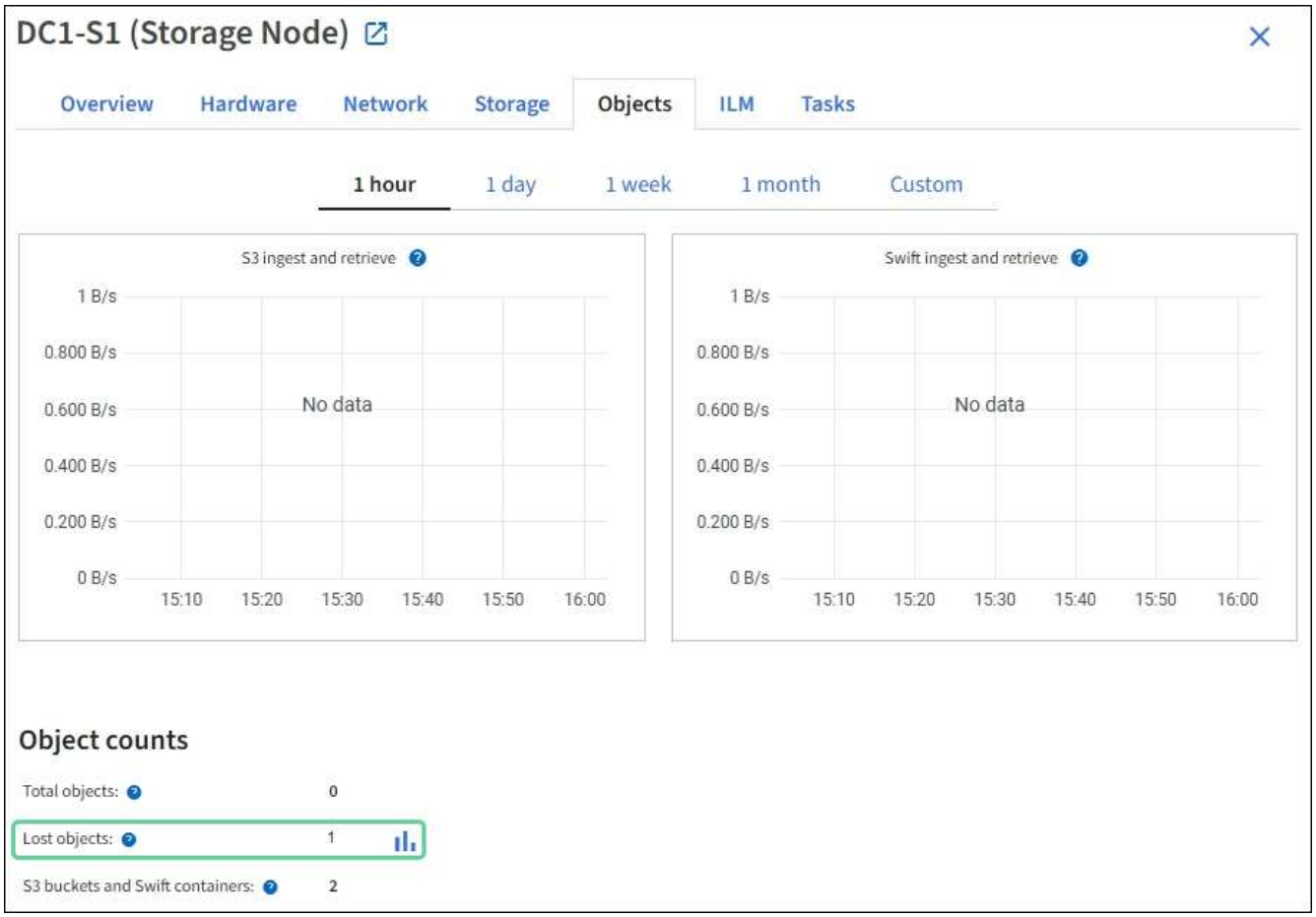
O alerta **objetos perdidos** indica que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

Investigue alertas de objetos perdidos imediatamente. Talvez seja necessário tomar medidas para evitar mais perda de dados. Em alguns casos, você pode restaurar um objeto perdido se você tomar uma ação imediata.

Passos

1. Selecione **NODES**.
2. Selecione ***Storage Node*** > **Objects**.
3. Revise o número de objetos perdidos mostrados na tabela contagens de objetos.

   Esse número indica o número total de objetos que esse nó de grade deteta como ausente de todo o sistema StorageGRID. O valor é a soma dos contadores de objetos perdidos do componente armazenamento de dados nos serviços LDR e DDS.



4. A partir de um nó Admin, "acesse o log de auditoria"para determinar o identificador exclusivo (UUID) do objeto que acionou o alerta **objetos perdidos**:
   a. Faça login no nó da grade:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
   b. Mude para o diretório onde os logs de auditoria estão localizados. Introduza: `cd /var/local/log/`

      "Saiba mais sobre os destinos para informações de auditoria".
   c. Use grep para extrair as mensagens de auditoria OLST (Object Lost). Introduza: `grep OLST audit_file_name`
   d. Observe o valor UUID incluído na mensagem.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Procure os metadados para o objeto perdido usando o UUID:
   a. Selecione **ILM** > **Object metadata lookup**.
   b. Introduza o UUID e selecione **Procurar**.
   c. Revise os locais nos metadados e tome a ação apropriada:

Metadados	Conclusão
<object_identifier> Objeto não encontrado	Se o objeto não for encontrado, a mensagem "ERROR":" é retornada. Se o objeto não for encontrado, você pode redefinir a contagem de **objetos perdidos** para limpar o alerta. A falta de um objeto indica que o objeto foi intencionalmente excluído.
Localizações > 0	Se houver locais listados na saída, o alerta **objetos perdidos** pode ser um falso positivo. Confirme se os objetos existem. Use o ID do nó e o filepath listados na saída para confirmar se o arquivo de objeto está no local listado. (O procedimento para "procurar objetos potencialmente perdidos" explica como usar o ID do nó para encontrar o nó de armazenamento correto.) Se os objetos existirem, você pode redefinir a contagem de **objetos perdidos** para limpar o alerta.
Localização: 0	Se não houver locais listados na saída, o objeto está potencialmente ausente. Você pode tentar "procure e restaure o objeto" para si mesmo, ou você pode entrar em Contato com o suporte técnico. O suporte técnico pode pedir-lhe para determinar se existe um procedimento de recuperação de armazenamento em curso. Consulte as informações sobre "Restaurando dados de objetos usando o Grid Manager" e "restaurar dados de objeto para um volume de armazenamento".

Pode ser possível encontrar e restaurar objetos que acionaram um alerta **Objeto perdido** e um alarme de objetos perdidos legado (PERDIDOS) e que você identificou como potencialmente perdido.

Antes de começar

- Você tem o UUID de qualquer objeto perdido, conforme identificado em "Investigue objetos perdidos".
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Você pode seguir este procedimento para procurar cópias replicadas do objeto perdido em outro lugar na grade. Na maioria dos casos, o objeto perdido não será encontrado. No entanto, em alguns casos, você pode encontrar e restaurar um objeto replicado perdido se você executar uma ação de prompt.

Contacte o suporte técnico para obter assistência com este procedimento.

Passos

1. A partir de um nó Admin, procure os logs de auditoria para possíveis localizações de objetos:

   a. Faça login no nó da grade:

      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      iii. Digite o seguinte comando para mudar para root: `su -`

      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

   b. Mude para o diretório onde os logs de auditoria estão localizados: `cd /var/local/log/`

      "Saiba mais sobre os destinos para informações de auditoria".

   c. Use grep para extrair o "auditar mensagens associadas ao objeto potencialmente perdido" e enviá-los para um arquivo de saída. Introduza: `grep uuid-value audit_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 esta mensagem de exemplo.

```
[AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
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.

a. Localize o nó de armazenamento associado a este ID de nó LDR. No Gerenciador de Grade, selecione **support** > **Tools** > **Grid topology**. Em seguida, selecione ***Data Center*** > ***Storage Node*** > **LDR**.

O ID do nó para o serviço LDR está na tabela informações do nó. Reveja as informações de cada nó de armazenamento até encontrar o que hospeda este LDR.

2. Determine se o objeto existe no nó de armazenamento indicado na mensagem de auditoria:

a. Faça login no nó da grade:

i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

iii. Digite o seguinte comando para mudar para root: `su -`

iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

b. Determine se o caminho do arquivo para o objeto existe.

Para o caminho do arquivo do objeto, use o valor de PCLD da mensagem de auditoria LLST.

Por exemplo, digite:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Sempre inclua o caminho do arquivo de objeto em aspas simples em comandos para escapar de quaisquer carateres especiais.

- Se o caminho do objeto não for encontrado, o objeto é perdido e não pode ser restaurado usando este procedimento. Entre em Contato com o suporte técnico.

- Se o caminho do objeto for encontrado, continue com a próxima etapa. Você pode tentar restaurar o objeto encontrado de volta para o StorageGRID.

3. Se o caminho do objeto foi encontrado, tente restaurar o objeto para StorageGRID:
   a. No mesmo nó de storage, altere a propriedade do arquivo de objeto para que ele possa ser gerenciado pelo StorageGRID. Introduza: `chown ldr-user:bycast 'file_path_of_object'`
   b. Telnet para localhost 1402 para acessar o console LDR. Introduza: `telnet 0 1402`
   c. Introduza: `cd /proc/STOR`
   d. Introduza: `Object_Found 'file_path_of_object'`

      Por exemplo, digite:

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      A emissão do `Object_Found` comando notifica a grade da localização do objeto. Ele também aciona as políticas ILM ativas, que fazem cópias adicionais conforme especificado em cada política.

      > Se o nó de armazenamento onde você encontrou o objeto estiver offline, você poderá copiar o objeto para qualquer nó de armazenamento que esteja online. Coloque o objeto em qualquer diretório /var/local/rangedb do nó de armazenamento online. Em seguida, emita o `Object_Found` comando usando esse caminho de arquivo para o objeto.

      - Se o objeto não puder ser restaurado, o `Object_Found` comando falhará. Entre em Contato com o suporte técnico.
      - Se o objeto foi restaurado com sucesso para o StorageGRID, uma mensagem de sucesso será exibida. Por exemplo:

        ```
        ade 12448208: /proc/STOR > Object_Found
        '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

        ade 12448208: /proc/STOR > Object found succeeded.
        First packet of file was valid. Extracted key: 38186FE53E3C49A5
        Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
        '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
        ```

        Avance para o passo seguinte.

4. Se o objeto foi restaurado com sucesso para o StorageGRID, verifique se os novos locais foram criados:
   a. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
   b. Selecione **ILM** > **Object metadata lookup**.
   c. Introduza o UUID e selecione **Procurar**.
   d. Revise os metadados e verifique os novos locais.
5. Em um nó Admin, pesquise os logs de auditoria para a mensagem de auditoria ORLM para este objeto para confirmar que o gerenciamento do ciclo de vida das informações (ILM) colocou cópias conforme

necessário.

a. Faça login no nó da grade:

   i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

   ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   iii. Digite o seguinte comando para mudar para root: `su -`

   iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

b. Mude para o diretório onde os logs de auditoria estão localizados: `cd /var/local/log/`

c. Use grep para extrair as mensagens de auditoria associadas ao objeto para um arquivo de saída. Introduza: `grep uuid-value audit_file_name > output_file_name`

   Por exemplo:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

d. Use o grep para extrair as mensagens de auditoria regras de objeto atendidas (ORLM) deste arquivo de saída. Introduza: `grep ORLM output_file_name`

   Por exemplo:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

   Uma mensagem de auditoria ORLM se parece com esta mensagem de exemplo.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Localize o campo LOCS na mensagem de auditoria.

   Se presente, o valor de CLDI em LOCS é o ID do nó e o ID do volume onde uma cópia de objeto foi criada. Esta mensagem mostra que o ILM foi aplicado e que duas cópias de objeto foram criadas em dois locais na grade.

6. "Redefina as contagens de objetos perdidas e ausentes" No Gerenciador de Grade.

Repor contagens de objetos perdidas e em falta

Depois de investigar o sistema StorageGRID e verificar se todos os objetos perdidos gravados são perdidos permanentemente ou se é um alarme falso, você pode redefinir o valor do atributo objetos perdidos para zero.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

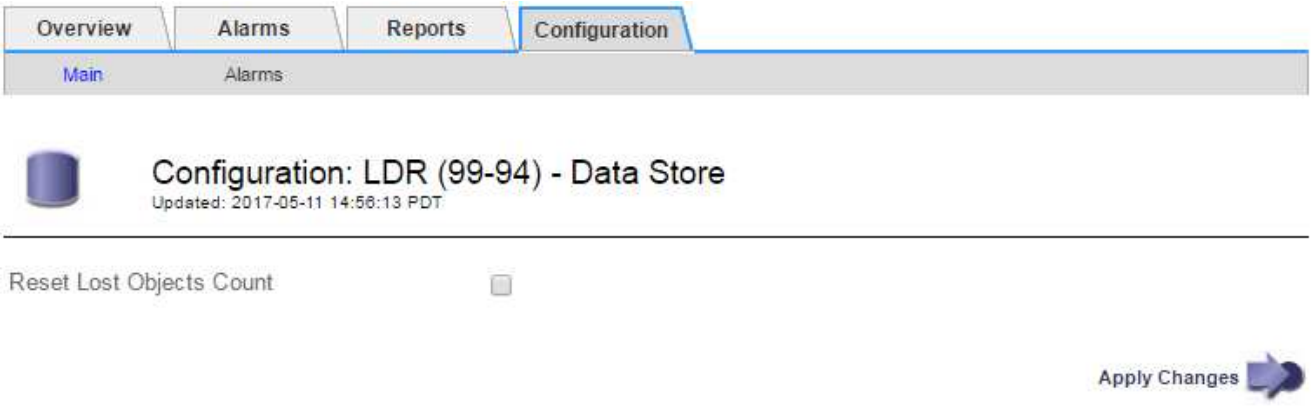
Você pode redefinir o contador de objetos perdidos a partir de uma das seguintes páginas:

- **SUPORTE** > **Ferramentas** > **topologia de grelha** > ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Overview** > **Main**
- **SUPORTE** > **Ferramentas** > **topologia de grelha** > ***Site*** > ***Storage Node*** > **DDS** > **Data Store** > **Visão geral** > **Main**

Estas instruções mostram a reposição do contador a partir da página **LDR** > **Data Store**.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Site*** > ***Storage Node*** > **LDR** > **armazenamento de dados** > **Configuração** para o nó de armazenamento que tem o alerta **objetos perdidos** ou o alarme PERDIDO.
3. Selecione **Redefinir contagem de objetos perdidos**.



4. Clique em **aplicar alterações**.

   O atributo objetos perdidos é redefinido para 0 e o alerta **objetos perdidos** e o alarme PERDIDO são apagados, o que pode levar alguns minutos.

5. Opcionalmente, redefina outros valores de atributo relacionados que podem ter sido incrementados no processo de identificação do objeto perdido.

   a. Selecione ***Site*** > ***Storage Node*** > **LDR** > **Codificação de apagamento** > **Configuração**.

   b. Selecione **Redefinir leituras de contagem de falhas** e **Redefinir cópias corrompidas detetadas contagem**.

   c. Clique em **aplicar alterações**.

d. Selecione ***Site*** > ***Storage Node*** > **LDR** > **Verificação** > **Configuração**.

e. Selecione **Redefinir contagem de objetos ausentes** e **Redefinir contagem de objetos corrompidos**.

f. Se você tiver certeza de que objetos em quarentena não são necessários, selecione **Excluir objetos em quarentena**.

Objetos em quarentena são criados quando a verificação em segundo plano identifica uma cópia de objeto replicado corrompido. Na maioria dos casos, o StorageGRID substitui automaticamente o objeto corrompido e é seguro excluir os objetos em quarentena. No entanto, se o alerta **objetos perdidos** ou o alarme PERDIDO for acionado, o suporte técnico pode querer acessar os objetos em quarentena.

g. Clique em **aplicar alterações**.

Pode demorar alguns momentos para que os atributos sejam redefinidos depois de clicar em **Apply Changes** (aplicar alterações).

Solucionar problemas do alerta de armazenamento de dados de objetos baixos

O alerta **armazenamento de dados de objeto baixo** monitora quanto espaço está disponível para armazenar dados de objeto em cada nó de armazenamento.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

O alerta **armazenamento de dados de objeto baixo** é acionado quando a quantidade total de dados de objeto replicados e codificados por apagamento em um nó de armazenamento atende a uma das condições configuradas na regra de alerta.

Por padrão, um alerta principal é acionado quando essa condição é avaliada como verdadeira:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Nesta condição:

- `storagegrid_storage_utilization_data_bytes` É uma estimativa do tamanho total de dados de objetos replicados e codificados por apagamento para um nó de storage.
- `storagegrid_storage_utilization_usable_space_bytes` É a quantidade total de espaço de storage de objetos restante para um nó de storage.

Se um alerta maior ou menor **armazenamento de dados de objeto baixo** for acionado, você deve executar um procedimento de expansão o mais rápido possível.

Passos

1. Selecione **ALERTAS** > **atual**.

A página Alertas é exibida.

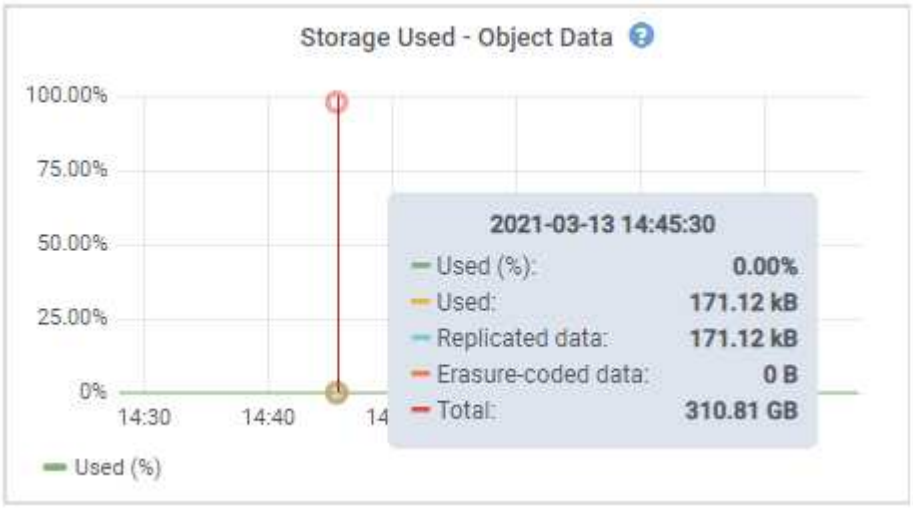
2. Na tabela de alertas, expanda o grupo de alertas **armazenamento de dados de objeto baixo**, se necessário, e selecione o alerta que deseja exibir.

   Selecione o alerta e não o cabeçalho de um grupo de alertas.

3. Revise os detalhes na caixa de diálogo e observe o seguinte:
   - Tempo acionado
   - O nome do site e do nó
   - Os valores atuais das métricas para este alerta
4. Selecione **NÓS** > ***Storage Node ou Site*** > **Storage**.
5. Posicione o cursor sobre o gráfico armazenamento usado - dados do objeto.

   São apresentados os seguintes valores:

   - **Usado (%)**: A porcentagem do espaço utilizável total que foi usado para dados do objeto.
   - **Usado**: A quantidade de espaço utilizável total que foi usado para dados de objeto.
   - **Dados replicados**: Uma estimativa da quantidade de dados de objetos replicados neste nó, site ou grade.
   - **Dados codificados por apagamento**: Uma estimativa da quantidade de dados de objetos codificados por apagamento neste nó, site ou grade.
   - **Total**: A quantidade total de espaço utilizável neste nó, site ou grade. O valor usado é a `storagegrid_storage_utilization_data_bytes` métrica.



6. Selecione os controles de tempo acima do gráfico para exibir o uso do armazenamento em diferentes períodos de tempo.

   Analisar o uso do armazenamento ao longo do tempo pode ajudá-lo a entender quanto armazenamento foi usado antes e depois do alerta ser acionado e pode ajudá-lo a estimar quanto tempo pode levar para que o espaço restante do nó fique cheio.

7. Assim que possível, "adicionar capacidade de armazenamento" para a sua grade.

   Você pode adicionar volumes de storage (LUNs) aos nós de storage existentes ou adicionar novos nós de storage.

Para obter mais informações, "Gerencie nós de storage completos"consulte .

Solucionar problemas de alertas de substituição de marca d'água somente leitura baixa

Se você usar valores personalizados para marcas d'água de volume de armazenamento, talvez seja necessário resolver o alerta **baixa substituição de marca d'água somente leitura**. Se possível, você deve atualizar seu sistema para começar a usar os valores otimizados.

Nas versões anteriores, as três "marcas de água do volume de armazenamento" eram configurações globais e número 8212; os mesmos valores aplicados a cada volume de armazenamento em cada nó de armazenamento. A partir do StorageGRID 11,6, o software pode otimizar essas marcas d'água para cada volume de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

Quando você atualiza para o StorageGRID 11,6 ou superior, marcas de água otimizadas somente leitura e leitura-gravação são aplicadas automaticamente a todos os volumes de armazenamento, a menos que uma das seguintes opções seja verdadeira:

- Seu sistema está próximo da capacidade e não poderá aceitar novos dados se forem aplicadas marcas de água otimizadas. Neste caso, o StorageGRID não alterará as configurações de marca d'água.
- Você definiu anteriormente qualquer uma das marcas d'água do volume de armazenamento para um valor personalizado. O StorageGRID não substituirá as configurações personalizadas de marca d'água com valores otimizados. No entanto, o StorageGRID pode acionar o alerta de substituição de marca d'água **baixa somente de leitura** se o valor personalizado para a marca d'água somente leitura suave do volume de armazenamento for muito pequeno.

Entenda o alerta

Se você usar valores personalizados para marcas d'água de volume de armazenamento, o alerta **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 da marca d'água somente leitura suave do volume de armazenamento é menor do que o valor otimizado mínimo para esse nó de armazenamento. 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 a marca d'água somente leitura suave do volume de armazenamento para 5 GB. Agora suponha que o StorageGRID calculou os seguintes valores otimizados para os quatro volumes de armazenamento no nó de armazenamento A:

Volume 0	12 GB
Volume 1	12 GB
Volume 2	11 GB

Volume 3	15 GB

O alerta **Low read-only watermark override** é acionado para o nó de armazenamento A porque sua marca d'água personalizada (5 GB) é menor do que o valor otimizado mínimo para todos os volumes nesse nó (11 GB). Se você continuar usando a configuração personalizada, o nó pode ser executado criticamente baixo no espaço antes que ele possa fazer a transição com segurança para o estado somente leitura.

Resolva o alerta

Siga estes passos se um ou mais alertas de substituição de marca d'água somente leitura baixa* tiverem sido acionados. Você também pode usar essas instruções se você usar configurações personalizadas de marca d'água atualmente e quiser começar a usar configurações otimizadas, mesmo que nenhum alerta tenha sido acionado.

Antes de começar

- Concluiu a atualização para o StorageGRID 11,6 ou superior.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

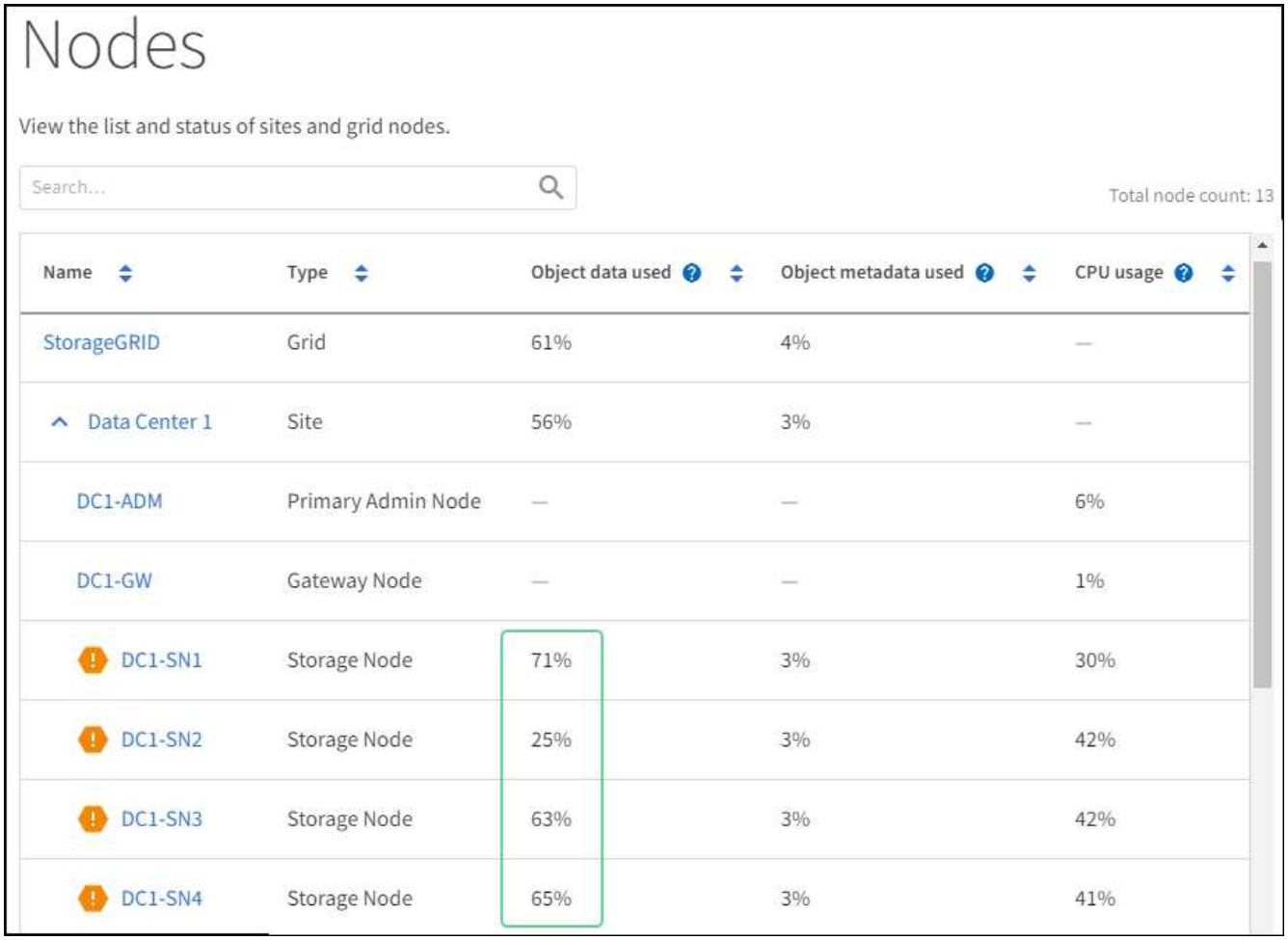
Sobre esta tarefa

Você pode resolver o alerta * baixa substituição de marca d'água somente leitura * atualizando as configurações personalizadas de marca d'água para as novas substituições de marca d'água. No entanto, se um ou mais nós de armazenamento estiverem próximos do cheio ou se você tiver requisitos especiais de ILM, primeiro você deve visualizar as marcas d'água de armazenamento otimizadas e determinar se é seguro usá-las.

Avalie o uso de dados de objeto para toda a grade

Passos

1. Selecione **NODES**.
2. Para cada local na grade, expanda a lista de nós.
3. Revise os valores de porcentagem mostrados na coluna **dados de objeto usados** para cada nó de armazenamento em cada local.



4. Siga o passo apropriado:
   a. Se nenhum dos nós de armazenamento estiver próximo da totalidade (por exemplo, todos os valores **dados de objeto usados** forem inferiores a 80%), você poderá começar a usar as configurações de substituição. Vá para Use marcas de água otimizadas.
   b. Se as regras do ILM usarem comportamento de ingestão rigoroso ou se os pools de armazenamento específicos estiverem próximos de cheio, execute as etapas em Ver marcas de água de armazenamento otimizadas e Determine se você pode usar marcas de água otimizadas.

Ver marcas de água de armazenamento otimizadas

O StorageGRID usa duas métricas Prometheus para mostrar os valores otimizados que calculou para a marca d'água de somente leitura suave do volume de armazenamento. Você pode visualizar os valores otimizados mínimo e máximo para cada nó de storage em sua grade.

Passos

1. Selecione **SUPPORT** > **Tools** > **Metrics**.
2. Na seção Prometheus, selecione o link para acessar a interface do usuário Prometheus.
3. Para ver a marca d'água mínima de leitura suave recomendada, insira a seguinte métrica Prometheus e selecione **execute**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor otimizado mínimo da marca d'água somente leitura suave para todos os

volumes de armazenamento em cada nó de armazenamento. Se esse valor for maior do que a configuração personalizada para a marca d'água de somente leitura suave do volume de armazenamento, o alerta **Substituição da marca d'água somente leitura baixa** será acionado para o nó de armazenamento.

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 otimizado máximo da marca d'água somente leitura suave para todos os volumes de armazenamento em cada nó de armazenamento.

5. Observe o valor otimizado máximo para cada nó de armazenamento.

determine se você pode usar marcas de água otimizadas

Passos

1. Selecione **NODES**.
2. Repita estas etapas para cada nó de armazenamento online:
   a. Selecione ***Storage Node*** > **Storage**.
   b. Role para baixo até a tabela Object Stores.
   c. Compare o valor **disponível** para cada armazenamento de objetos (volume) com a marca d'água máxima otimizada que você anotou para esse nó de armazenamento.
3. Se pelo menos um volume em cada nó de armazenamento online tiver mais espaço disponível do que a marca d'água máxima otimizada para esse nó, vá para começar a usar as marcas d'Use marcas de água otimizadaságua otimizadas.

   Caso contrário, expanda a grade o mais rápido possível. "adicione volumes de armazenamento"Para um nó existente ou "Adicionar novos nós de storage". Em seguida, aceda a Use marcas de água otimizadas para atualizar as definições da marca de água.

4. Se você precisar continuar usando valores personalizados para as marcas d'água do volume de armazenamento, "silêncio" ou "desativar" o alerta **Sobreposição de marca d'água somente leitura baixa**.

   > Os mesmos valores de marca d'água personalizados são aplicados a cada volume de armazenamento em cada nó de armazenamento. O uso de valores menores que os recomendados para marcas d'água de volume de armazenamento pode fazer com que alguns volumes de armazenamento fiquem inacessíveis (desmontados automaticamente) quando o nó atinge a capacidade.

[[marcas de água otimizadas para uso]]Use marcas de água otimizadas

Passos

1. Aceda a **SUPPORT** > **Other** > **Storage watermarks**.
2. Marque a caixa de seleção **usar valores otimizados**.
3. Selecione **Guardar**.

As configurações de marca d'água de volume de armazenamento otimizadas estão agora em vigor para cada

volume de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

Solucionar problemas de metadados

Se ocorrerem problemas de metadados, os alertas informam sobre a origem dos problemas e as ações recomendadas a serem tomadas. Em particular, você deve adicionar novos nós de storage se o alerta de storage de metadados baixos for acionado.

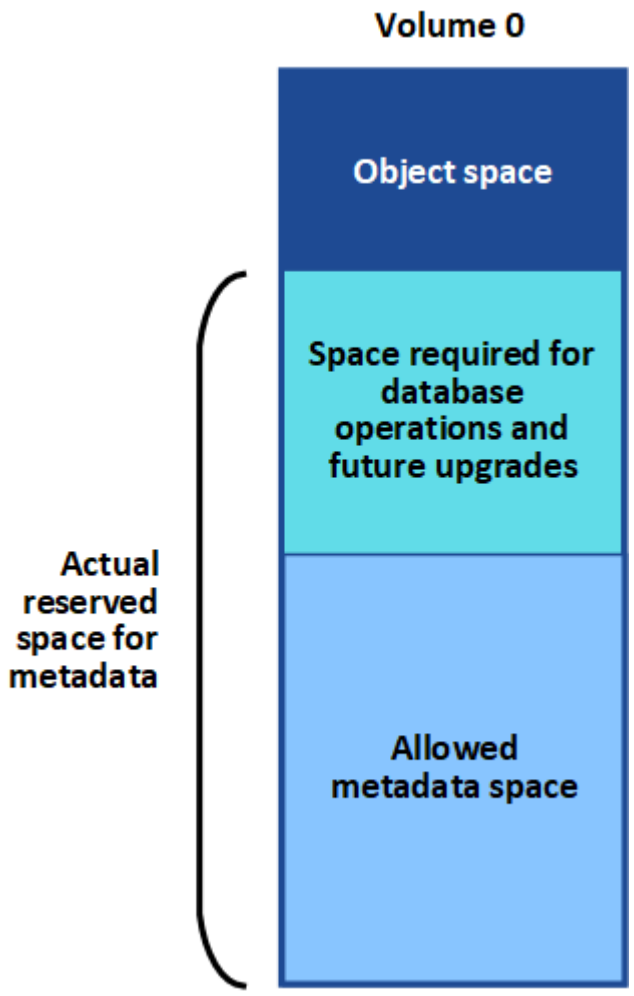
Antes de começar

Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

Sobre esta tarefa

Siga as ações recomendadas para cada alerta relacionado a metadados que é acionado. Se o alerta **armazenamento de metadados baixo** for acionado, você deverá adicionar novos nós de armazenamento.

O StorageGRID reserva uma certa quantidade de espaço no volume 0 de cada nó de storage para metadados de objetos. Esse espaço, conhecido como *espaço reservado real*, é subdividido no espaço permitido para metadados de objetos (o espaço permitido de metadados) e no espaço necessário para operações essenciais de banco de dados, como compactação e reparo. O espaço de metadados permitido rege a capacidade geral do objeto.



Se os metadados de objetos consumirem mais de 100% do espaço permitido para metadados, as operações do banco de dados não poderão ser executadas de forma eficiente e ocorrerão erros.

Você pode "Monitore a capacidade dos metadados de objetos para cada nó de storage"ajudá-lo a antecipar erros e corrigi-los antes que eles ocorram.

O StorageGRID usa a seguinte métrica Prometheus para medir o quão cheio é o espaço permitido de metadados:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

Quando essa expressão Prometheus atinge certos limites, o alerta **armazenamento de metadados baixo** é acionado.

- **Minor**: Metadados de objetos estão usando 70% ou mais do espaço de metadados permitido. Você deve adicionar novos nós de storage o mais rápido possível.
- **Major**: Metadados de objetos estão usando 90% ou mais do espaço permitido de metadados. Você deve adicionar novos nós de storage imediatamente.

> Quando os metadados de objetos estão usando 90% ou mais do espaço permitido de metadados, um aviso aparece no painel. Se esse aviso for exibido, você deverá adicionar novos nós de storage imediatamente. Você nunca deve permitir que os metadados de objetos usem mais de 100% do espaço permitido.

- **Crítico**: Metadados de objetos estão usando 100% ou mais do espaço permitido de metadados e estão começando a consumir o espaço necessário para operações essenciais de banco de dados. Você deve interromper a ingestão de novos objetos e adicionar novos nós de storage imediatamente.

> Se o tamanho do volume 0 for menor do que a opção de armazenamento de espaço reservado de metadados (por exemplo, em um ambiente não-produção), o cálculo do alerta **armazenamento de metadados baixo** pode ser impreciso.

Passos

1. Selecione **ALERTAS** > **atual**.
2. Na tabela de alertas, expanda o grupo de alertas **armazenamento de metadados baixo**, se necessário, e selecione o alerta específico que deseja exibir.
3. Reveja os detalhes na caixa de diálogo de alerta.
4. Se um alerta importante ou crítico de **armazenamento de metadados baixo** tiver sido acionado, execute uma expansão para adicionar nós de armazenamento imediatamente.

> Como o StorageGRID mantém cópias completas de todos os metadados de objetos em cada local, a capacidade de metadados de toda a grade é limitada pela capacidade de metadados do menor local. Se você precisar adicionar capacidade de metadados a um local, também deverá "expanda quaisquer outros sites"pelo mesmo número de nós de storage.

Após a expansão, o StorageGRID redistribui os metadados de objetos existentes para os novos nós, o que aumenta a capacidade geral de metadados da grade. Nenhuma ação do usuário é necessária. O

alerta **armazenamento de metadados baixo** é apagado.

Solucionar erros de certificado

Se você vir um problema de segurança ou certificado ao tentar se conetar ao StorageGRID usando um navegador da Web, um cliente S3 ou uma ferramenta de monitoramento externa, verifique o certificado.

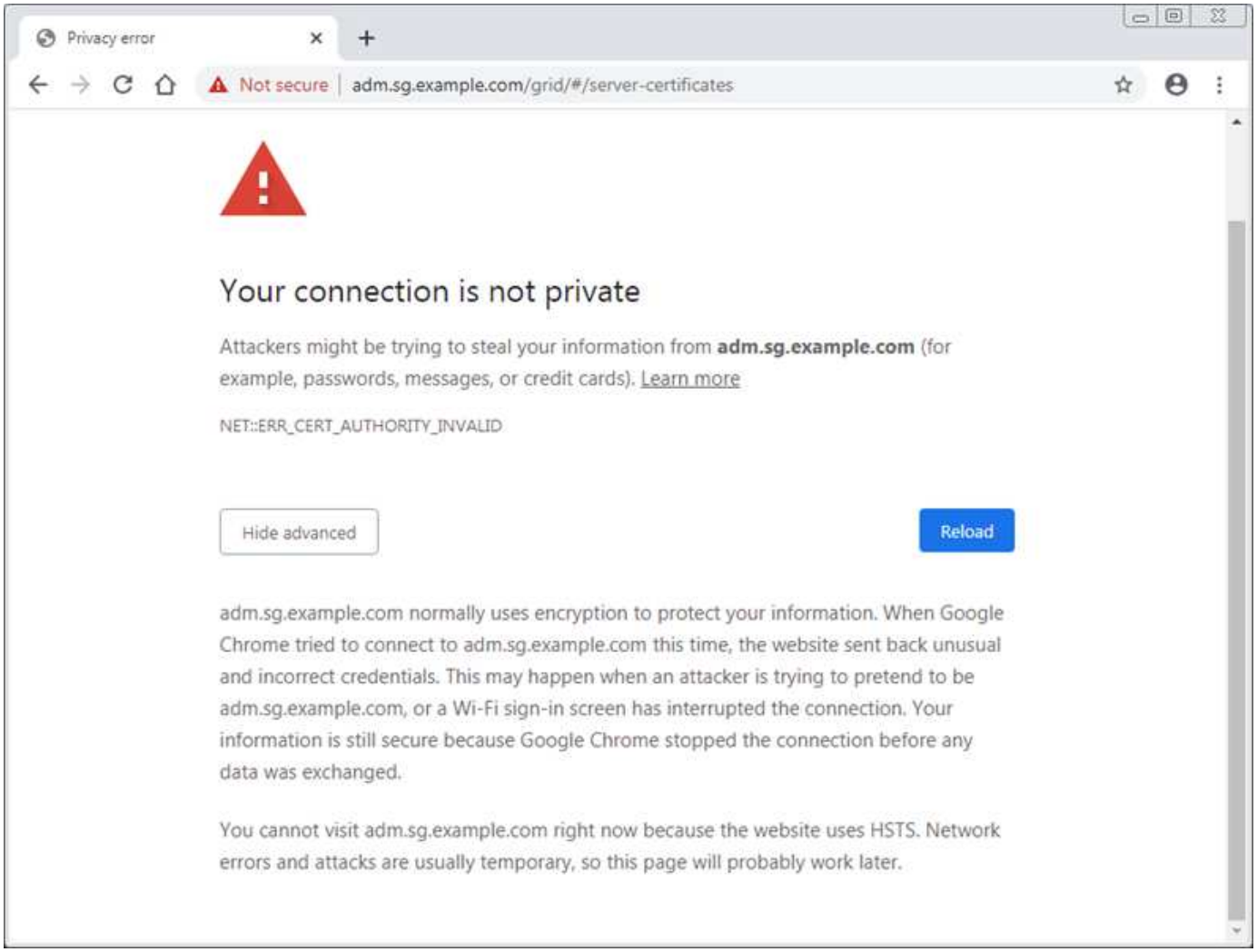
Sobre esta tarefa

Os erros de certificado podem causar problemas quando você tenta se conetar ao StorageGRID usando o Gerenciador de Grade, a API de Gerenciamento de Grade, o Gerenciador de Locatário ou a API de Gerenciamento de Locatário. Erros de certificado também podem ocorrer quando você tenta se conetar com um cliente S3 ou 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 não aceitam certificados com um período de validade superior a 398 dias.
2. Se o certificado tiver expirado ou expirar em breve, carregue ou gere um novo certificado.
   - Para obter um certificado de servidor, consulte as etapas "Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"do .
   - Para obter um certificado de cliente, consulte as etapas "configurando um certificado de cliente"do .
3. Para erros de certificado de servidor, tente uma ou ambas as opções a seguir:

- Certifique-se de que o nome alternativo do assunto (SAN) do certificado esteja preenchido e que a SAN corresponda ao endereço IP ou ao nome do host do nó ao qual você está se conetando.
- Se você estiver tentando se conetar ao StorageGRID usando um nome de domínio:
  i. Insira o endereço IP do nó Admin em vez do nome de domínio para ignorar o erro de conexão e acessar o Gerenciador de Grade.
  ii. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida"selecione a guia certificado apropriado", instale um novo certificado personalizado ou continue com o certificado padrão.
  iii. Nas instruções de administração do StorageGRID, consulte as etapas "Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"do .

Solucionar problemas de nó de administração e interface do usuário

Você pode executar várias tarefas para ajudar a determinar a origem dos problemas relacionados aos nós de administração e à interface de usuário do StorageGRID.

Erros de login do nó de administrador

Se ocorrer um erro ao iniciar sessão num nó de administração do StorageGRID, o sistema poderá ter um problema com um problema "rede"ou, um problema com ou "hardware""Serviços do Admin Node" um "Problema com o banco de dados Cassandra" em nós de armazenamento ligados.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o `Passwords.txt` arquivo.
- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

Use estas diretrizes de solução de problemas se você vir qualquer uma das seguintes mensagens de erro ao tentar entrar em um nó de administrador:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Passos

1. Aguarde 10 minutos e tente iniciar sessão novamente.

   Se o erro não for resolvido automaticamente, vá para a próxima etapa.

2. Se o seu sistema StorageGRID tiver mais de um nó de administrador, tente iniciar sessão no Gestor de grelha a partir de outro nó de administrador para verificar o estado de um nó de administrador indisponível.

- Se você conseguir entrar, você pode usar as opções **Dashboard**, **Nodes**, **Alerts** e **SUPPORT** para ajudar a determinar a causa do erro.
- Se você tiver apenas um nó Admin ou ainda não conseguir entrar, vá para a próxima etapa.

3. Determine se o hardware do nó está offline.
4. Se o logon único (SSO) estiver ativado para o sistema StorageGRID, consulte as etapas para "configurando logon único".

   Talvez seja necessário desativar e reativar temporariamente o SSO para um único nó de administração para resolver quaisquer problemas.

   > Se o SSO estiver ativado, você não poderá fazer logon usando uma porta restrita. Tem de utilizar a porta 443.

5. Determine se a conta que você está usando pertence a um usuário federado.

   Se a conta de usuário federada não estiver funcionando, tente fazer login no Gerenciador de Grade como um usuário local, como root.

   - Se o utilizador local puder iniciar sessão:
     i. Reveja alertas.
     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
```

```
# gpt-list-services adc
```

Os nós de administração usam o serviço ADC durante o processo de autenticação.

12. A partir do nó Admin, use ssh para efetuar login em cada um dos nós de armazenamento ADC, usando os endereços IP identificados.
13. Veja o status de todos os serviços em execução no nó da grade: `storagegrid-status`

Certifique-se de que os serviços idnt, acct, nginx e cassandra estejam todos em execução.

14. Repita as etapas Use Lumberjack para coletar logs e Rever registos para revisar os logs nos nós de storage.
15. Se você não conseguir resolver o problema, entre em Contato com o suporte técnico.

Forneça os Registros que você coletou para o suporte técnico. Consulte também "Referência de ficheiros de registo".

Problemas na interface do usuário

A interface de usuário do Gerenciador de Grade ou do Gerenciador de Locatário pode não responder como esperado após o upgrade do software StorageGRID.

Passos

1. Certifique-se de que está a utilizar um "navegador da web suportado".
2. Limpe o cache do navegador da Web.

Limpar o cache remove recursos desatualizados usados pela versão anterior do software StorageGRID e permite que a interface do usuário funcione corretamente novamente. Para obter instruções, consulte a documentação do navegador da Web.

Solucionar problemas de rede, hardware e plataforma

Há várias tarefas que você pode executar para ajudar a determinar a origem dos problemas relacionados a problemas de rede, hardware e plataforma StorageGRID.

"422: Entidade não processável" erros

O erro 422: Entidade não processável pode ocorrer por diferentes razões. Verifique a mensagem de erro para determinar o que causou o problema.

Se você vir uma das mensagens de erro listadas, execute a ação recomendada.

Mensagem de erro	Causa raiz e ação corretiva

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires`
`binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Esta mensagem pode ocorrer se você selecionar a opção **não usar TLS** para Segurança da camada de Transporte (TLS) ao configurar a federação de identidade usando o Windows ative Directory (AD).
	
	O uso da opção **não usar TLS** não é suportado para uso com servidores AD que imponham a assinatura LDAP. Você deve selecionar a opção **usar STARTTLS** ou a opção **usar LDAPS** para TLS.

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed`
`(EOF)`
	Essa mensagem será exibida se você tentar usar uma cifra não suportada para fazer uma conexão TLS (Transport Layer Security) do StorageGRID para um sistema externo usado para identificar pools de federação ou armazenamento em nuvem.
	
	Verifique as cifras que são oferecidas pelo sistema externo. O sistema deve usar um dos "Cifras suportadas por StorageGRID" para conexões TLS de saída, como mostrado nas instruções de administração do StorageGRID.

Alerta de incompatibilidade da MTU da rede de Grade

O alerta **Grid Network MTU mismatch** é acionado quando a configuração MTU (unidade máxima de transmissão) para a interface Grid Network (eth0) difere significativamente entre nós na grade.

Sobre esta tarefa

As diferenças nas configurações de MTU podem indicar que algumas, mas não todas, redes eth0 são configuradas para quadros jumbo. Uma incompatibilidade de tamanho da MTU superior a 1000 pode causar problemas de desempenho da rede.

Passos

1. Liste as configurações de MTU para eth0 em todos os nós.
   - Use a consulta fornecida no Gerenciador de Grade.
   - Navegue para *primary Admin Node IP address*`/metrics/graph` e insira a seguinte consulta: `node_network_mtu_bytes{device="eth0"}`
2. "Modifique as configurações MTU" Conforme necessário para garantir que eles sejam iguais para a interface de rede de Grade (eth0) em todos os nós.
   - Para nós baseados em Linux e VMware, use o seguinte comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     Exemplo: `change-ip.py -n node 1500 grid admin`

     Nota: Em nós baseados em Linux, se o valor MTU desejado para a rede no contentor exceder o valor já configurado na interface do host, você deve primeiro configurar a interface do host para ter o valor MTU desejado e, em seguida, usar o `change-ip.py` script para alterar o valor MTU da rede no contentor.

     Use os seguintes argumentos para modificar a MTU em nós baseados em Linux ou VMware.

Argumentos posicionais	Descrição
`mtu`	A MTU a definir. Deve estar na faixa de 1280 a 9216.
`network`	As redes às quais aplicar a MTU. Inclua um ou mais dos seguintes tipos de rede: • grelha • administrador • cliente

+

Argumentos opcionais	Descrição
`-h, - help`	Mostrar a mensagem de ajuda e sair.
`-n node, --node node`	O nó. O padrão é o nó local.

Alerta de erro do quadro de receção de rede do nó

Os alertas de erro de quadro de receção de rede podem ser causados por problemas de conetividade entre o StorageGRID e o hardware de rede. Este alerta é apagado por conta própria depois que o problema subjacente é resolvido.

Sobre esta tarefa

Os alertas de erro de quadro de receção de rede podem ser causados pelos seguintes problemas com o hardware de rede que se coneta ao StorageGRID:

- A correção de erro de avanço (FEC) é necessária e não está em uso
- Incompatibilidade da MTU da porta do switch e da NIC
- Altas taxas de erro de link
- Buffer de anel NIC excedido

Passos

1. Siga as etapas de solução de problemas para todas as possíveis causas desse alerta, dada a configuração da rede.
2. Execute as seguintes etapas, dependendo da causa do erro:

Incompatibilidade de FEC

Estas etapas são aplicáveis somente aos alertas de erro de quadro de receção de rede de nós* causados por incompatibilidade de FEC em dispositivos StorageGRID.

a. Verifique o status do FEC da porta no switch conetado ao seu dispositivo StorageGRID.
b. Verifique a integridade física dos cabos do aparelho ao interrutor.
c. Se você quiser alterar as configurações do FEC para tentar resolver o alerta, primeiro verifique se o aparelho está configurado para o modo **Automático** na página Configuração de conexão do Instalador de dispositivos StorageGRID (consulte as instruções do seu aparelho:
   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 e SG1100"
   - "SG100 e SG1000"
d. Altere as configurações do FEC nas portas do switch. As portas do dispositivo StorageGRID ajustarão suas configurações FEC para corresponder, se possível.

   Não é possível configurar as configurações do FEC nos dispositivos StorageGRID. Em vez disso, os aparelhos tentam descobrir e espelhar as configurações FEC nas portas do switch às quais estão conetados. Se os links forem forçados a velocidades de rede de 25 GbE ou 100 GbE, o switch e a NIC poderão não conseguir negociar uma configuração FEC comum. Sem uma configuração FEC comum, a rede voltará para o modo "no-FEC". Quando o FEC não está ativado, as conexões são mais suscetíveis a erros causados por ruído elétrico.

   A StorageGRID Appliances apoia a FEC (FC) e a FEC (RS), bem como a FEC.

Incompatibilidade da MTU da porta do switch e da NIC

Se o alerta for causado por uma falha de correspondência entre a porta do switch e a MTU da NIC, verifique se o tamanho da MTU configurado no nó é o mesmo que a configuração da MTU para a porta do switch.

O tamanho da MTU configurado no nó pode ser menor do que a configuração na porta do switch à qual o nó está conetado. Se um nó StorageGRID receber um quadro Ethernet maior do que o MTU, o que é possível com esta configuração, o alerta **erro de quadro de receção de rede** do nó pode ser comunicado. Se você acredita que isso está acontecendo, altere a MTU da porta do switch para corresponder à MTU da interface de rede da StorageGRID ou altere a MTU da interface de rede StorageGRID para corresponder à porta do switch, dependendo dos seus objetivos ou requisitos de MTU de ponta a ponta.

Para obter o melhor desempenho de rede, todos os nós devem ser configurados com valores MTU semelhantes em suas interfaces de rede de Grade. O alerta **incompatibilidade de MTU da rede de Grade** é acionado se houver uma diferença significativa nas configurações de MTU para a rede de Grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede. Consulte Solucione o alerta de incompatibilidade da MTU da rede de Grade para obter mais informações.

Consulte também "Altere a definição MTU" .

Altas taxas de erro de link

a. Ative o FEC, se ainda não estiver ativado.
b. Verifique se o cabeamento de rede é de boa qualidade e não está danificado ou conetado incorretamente.
c. Se os cabos parecerem não ser o problema, contacte o suporte técnico.

Você pode notar altas taxas de erro em um ambiente com alto ruído elétrico.

Buffer de anel NIC excedido

Se o erro for uma sobrecarga do buffer do anel da NIC, entre em Contato com o suporte técnico.

O buffer de anel pode ser excedido quando o sistema StorageGRID está sobrecarregado e não consegue processar eventos de rede em tempo hábil.

3. Monitore o problema e entre em Contato com o suporte técnico se o alerta não resolver.

Erros de sincronização de tempo

Você pode ver problemas com a sincronização de tempo em sua grade.

Se você encontrar problemas de sincronização de tempo, verifique se você especificou pelo menos quatro fontes de NTP externas, cada uma fornecendo uma referência estrato 3 ou melhor, e se todas as fontes de NTP externas estão operando normalmente e são acessíveis por seus nós de StorageGRID.

"Especificando a fonte NTP externa"Quando for uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, como o StorageGRID.

Linux: Problemas de conetividade de rede

Você pode ver problemas com a conetividade de rede para nós StorageGRID hospedados em hosts Linux.

Clonagem de endereços MAC

Em alguns casos, os problemas de rede podem ser resolvidos usando a clonagem de endereços MAC. Se você estiver usando hosts virtuais, defina o valor da chave de clonagem de endereços MAC para cada uma de suas redes como "verdadeiro" no arquivo de configuração do nó. Esta configuração faz com que o endereço MAC do contentor StorageGRID use o endereço MAC do host. Para criar arquivos de configuração de nó,

consulte as instruções para "Red Hat Enterprise Linux" ou "Ubuntu ou Debian".

> Crie interfaces de rede virtuais separadas para uso pelo sistema operacional host Linux. Usar as mesmas interfaces de rede para o sistema operacional host Linux e o contentor StorageGRID pode fazer com que o sistema operacional do host se torne inacessível se o modo promíscuo não tiver sido ativado no hypervisor.

Para obter mais informações sobre como ativar a clonagem MAC, consulte as instruções para "Red Hat Enterprise Linux" ou "Ubuntu ou Debian".

Modo promíscuo

Se você não quiser usar a clonagem de endereços MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes dos atribuídos pelo hypervisor, verifique se as propriedades de segurança nos níveis de switch virtual e grupo de portas estão definidas como **Accept** para modo promíscuo, alterações de endereço MAC e transmissões forjadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Para obter mais informações sobre como usar o modo promíscuo, consulte as instruções para "Red Hat Enterprise Linux" ou "Ubuntu ou Debian".

Linux: O status do nó é "órfão"

Um nó Linux em um estado órfão geralmente indica que o serviço StorageGRID ou o daemon de nó StorageGRID que controla o contentor do nó morreram inesperadamente.

Sobre esta tarefa

Se um nó Linux relata que ele está em um estado órfão, você deve:

- Verifique os logs para ver se há erros e mensagens.
- Tente iniciar o nó novamente.
- Se necessário, use comandos do mecanismo do contentor para parar o contentor do nó existente.
- Reinicie o nó.

Passos

1. Verifique os logs do serviço daemon e do nó órfão para ver se há erros óbvios ou mensagens sobre sair inesperadamente.
2. Faça login no host como root ou usando uma conta com permissão sudo.
3. Tente iniciar o nó novamente executando o seguinte comando: `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   Se o nó estiver órfão, a resposta será

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. A partir do Linux, pare o mecanismo de container e quaisquer processos de controle do StorageGRID-node. Por exemplo:`sudo docker stop --time secondscontainer-name`

   Para `seconds`, introduza o número de segundos que pretende aguardar que o recipiente pare (normalmente, 15 minutos ou menos). Por exemplo:

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. Reinicie o nó: `storagegrid node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

Linux: Solucione problemas de suporte ao IPv6

Talvez seja necessário habilitar o suporte IPv6 no kernel se você tiver instalado nós do StorageGRID em hosts Linux e notar que os endereços IPv6 não foram atribuídos aos contentores do nó como esperado.

Sobre esta tarefa

Para ver o endereço IPv6 que foi atribuído a um nó de grade:

1. Selecione **NÓS** e selecione o nó.
2. Selecione **Mostrar endereços IP adicionais** ao lado de **endereços IP** na guia Visão geral.

Se o endereço IPv6 não for exibido e o nó estiver instalado em um host Linux, siga estas etapas para habilitar o suporte a IPv6 no kernel.

Passos

1. Faça login no host como root ou usando uma conta com permissão sudo.
2. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

   ```
   root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
   ```

   O resultado deve ser 0.

   ```
   net.ipv6.conf.all.disable_ipv6 = 0
   ```

   > Se o resultado não for 0, consulte a documentação do sistema operacional para alterar `sysctl` as configurações. Em seguida, altere o valor para 0 antes de continuar.

3. Insira o contentor do nó StorageGRID: `storagegrid node enter node-name`
4. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

O resultado deve ser 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

Se o resultado não for 1, este procedimento não se aplica. Entre em Contato com o suporte técnico.

5. Saia do recipiente: `exit`

```
root@DC1-S1:~ # exit
```

6. Como root, edite o seguinte arquivo: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localize as duas linhas a seguir e remova as tags de comentário. Em seguida, salve e feche o arquivo.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Execute estes comandos para reiniciar o contentor StorageGRID:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Solucionar problemas de um servidor syslog externo

A tabela a seguir descreve as mensagens de erro que podem estar relacionadas ao uso de um servidor syslog externo e lista as ações corretivas.

Para obter mais informações sobre como enviar informações de auditoria para um servidor syslog externo, consulte:

- "Considerações para usar um servidor syslog externo"

- "Configurar mensagens de auditoria e servidor syslog externo"

Mensagem de erro	Descrição e ações recomendadas
Não é possível resolver o nome do host	O FQDN inserido para o servidor syslog não pôde ser resolvido para um endereço IP. 1. Verifique o nome do host que você inseriu. Se você inseriu um endereço IP, certifique-se de que é um endereço IP válido na notação W.X.Y.Z ("decimal pontilhado"). 2. Verifique se os servidores DNS estão configurados corretamente. 3. Confirme se cada nó pode acessar os endereços IP do servidor DNS.
Ligação recusada	Uma conexão TCP ou TLS ao servidor syslog foi recusada. Pode não haver nenhum serviço escutando na porta TCP ou TLS para o host, ou um firewall pode estar bloqueando o acesso. 1. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo para o servidor syslog. 2. Confirme se o host do serviço syslog está executando um daemon syslog que está escutando na porta especificada. 3. Confirme se um firewall não está bloqueando o acesso a conexões TCP/TLS dos nós para o IP e a porta do servidor syslog.
Rede inacessível	O servidor syslog não está em uma sub-rede conetada diretamente. Um roteador retornou uma mensagem de falha ICMP para indicar que não foi possível encaminhar as mensagens de teste dos nós listados para o servidor syslog. 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de sub-redes de rede de Grade, as listas de sub-redes de Admin e os gateways de rede de cliente. Confirme que estão configurados para rotear o tráfego para o servidor syslog através da interface de rede e gateway esperados (Grid, Admin ou Client).
Host inalcançável	O servidor syslog está em uma sub-rede conetada diretamente (sub-rede usada pelos nós listados para seus endereços IP de Grade, Admin ou Cliente). Os nós tentaram enviar mensagens de teste, mas não receberam respostas a solicitações ARP para o endereço MAC do servidor syslog. 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Verifique se o host que executa o serviço syslog está ativo.

Mensagem de erro	Descrição e ações recomendadas
Tempo de ligação esgotado	Uma tentativa de conexão TCP/TLS foi feita, mas nenhuma resposta foi recebida do servidor syslog por um longo tempo. Pode haver uma configuração incorreta de roteamento ou um firewall pode estar deixando cair o tráfego sem enviar qualquer resposta (uma configuração comum). 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de sub-redes de rede de Grade, as listas de sub-redes de Admin e os gateways de rede de cliente. Confirme que estão configurados para rotear o tráfego para o servidor syslog usando a interface de rede e gateway (Grid, Admin ou Client) sobre o qual você espera que o servidor syslog seja alcançado. 3. Confirme se um firewall não está bloqueando o acesso a conexões TCP/TLS dos nós listados para o IP e a porta do servidor syslog.
Conexão fechada pelo parceiro	Uma conexão TCP ao servidor syslog foi estabelecida com êxito, mas foi fechada mais tarde. As razões para isso podem incluir: • O servidor syslog pode ter sido reiniciado ou reiniciado. • O nó e o servidor syslog podem ter configurações diferentes de TCP/TLS. • Um firewall intermediário pode estar fechando conexões TCP ociosas. • Um servidor que não seja syslog escutando na porta do servidor syslog pode ter fechado a conexão. Para resolver este problema: 1. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo para o servidor syslog. 2. Se você estiver usando TLS, confirme se o servidor syslog também está usando TLS. Se você estiver usando TCP, confirme se o servidor syslog também está usando TCP. 3. Verifique se um firewall intermediário não está configurado para fechar conexões TCP ociosas.
Erro de certificado TLS	O certificado de servidor recebido do servidor syslog não era compatível com o pacote de certificados CA e o certificado de cliente fornecido. 1. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor syslog. 2. Confirme se as identidades no certificado de servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Reencaminhamento suspenso	Os Registros do syslog não estão mais sendo encaminhados para o servidor syslog e o StorageGRID não consegue detetar o motivo. Revise os logs de depuração fornecidos com esse erro para tentar determinar a causa raiz.

Mensagem de erro	Descrição e ações recomendadas
Sessão TLS terminada	O servidor syslog encerrou a sessão TLS e o StorageGRID não consegue detetar o motivo. 1. Revise os logs de depuração fornecidos com esse erro para tentar determinar a causa raiz. 2. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo para o servidor syslog. 3. Se você estiver usando TLS, confirme se o servidor syslog também está usando TLS. Se você estiver usando TCP, confirme se o servidor syslog também está usando TCP. 4. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor syslog. 5. Confirme se as identidades no certificado de servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Falha na consulta de resultados	O nó Admin usado para configuração e teste do servidor syslog não consegue solicitar resultados de teste dos nós listados. Um ou mais nós podem estar inativos. 1. Siga as etapas padrão de solução de problemas para garantir que os nós estejam online e que todos os serviços esperados estejam em execução. 2. Reinicie o serviço miscd nos nós listados.

Rever registos de auditoria

Auditar mensagens e logs

Estas instruções contêm informações sobre a estrutura e o conteúdo das mensagens de auditoria e registos de auditoria do StorageGRID. Você pode usar essas informações para ler e analisar a trilha de auditoria da atividade do sistema.

Estas instruções destinam-se aos administradores responsáveis pela produção de relatórios de atividade e utilização do sistema que exijam a análise das mensagens de auditoria do sistema StorageGRID.

Para usar o arquivo de log de texto, você deve ter acesso ao compartilhamento de auditoria configurado no nó Admin.

Para obter informações sobre como configurar níveis de mensagens de auditoria e usar um servidor syslog externo, "Configurar mensagens de auditoria e destinos de log"consulte .

Auditoria de fluxo e retenção de mensagens

Todos os serviços StorageGRID geram mensagens de auditoria durante a operação normal do sistema. Você deve entender como essas mensagens de auditoria se movem pelo sistema StorageGRID para `audit.log` o arquivo.

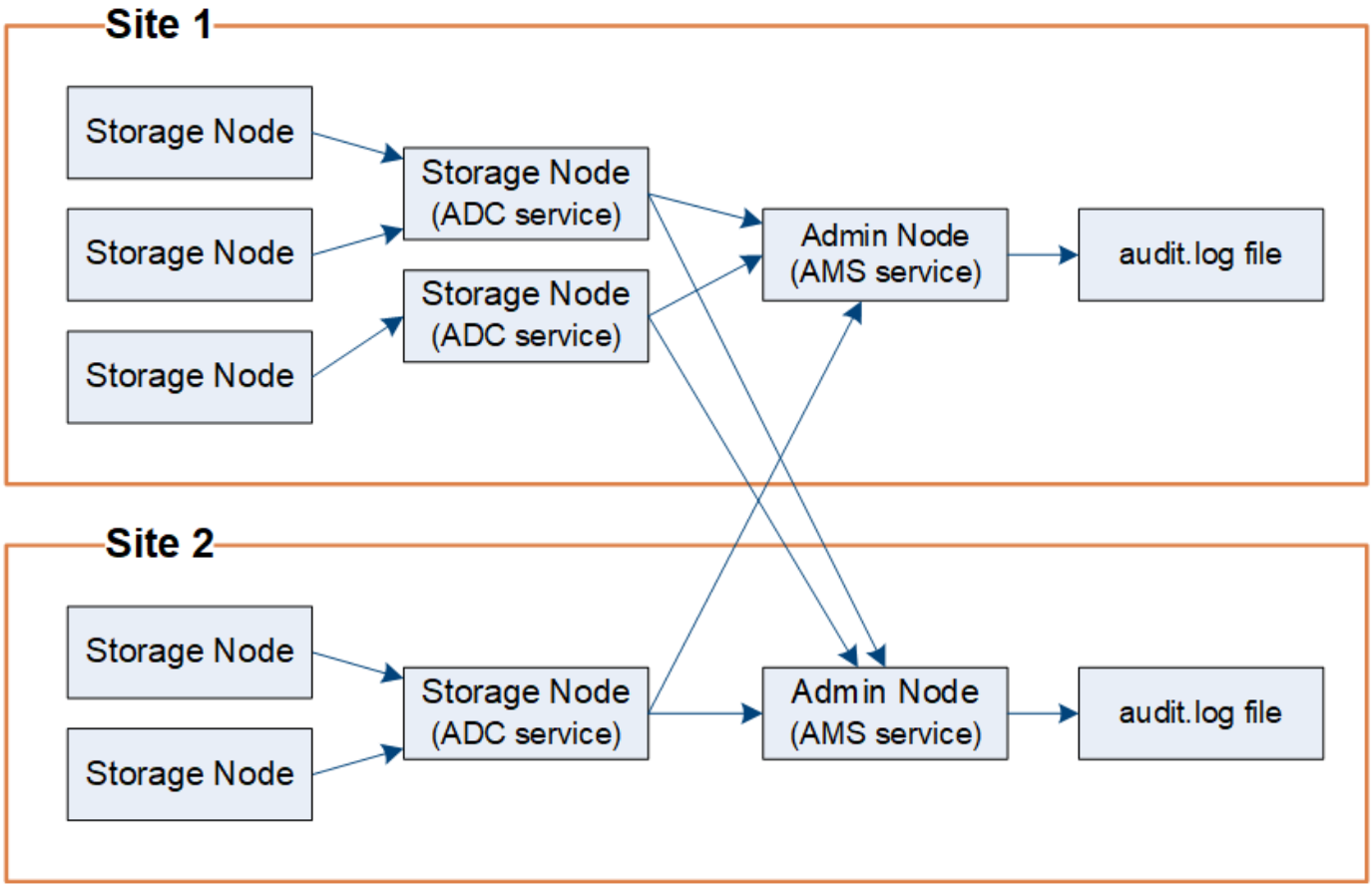
Auditoria do fluxo de mensagens

As mensagens de auditoria são processadas pelos nós de administração e pelos nós de armazenamento que têm um serviço de controlador de domínio administrativo (ADC).

Conforme mostrado no diagrama de fluxo de mensagens de auditoria, cada nó StorageGRID envia suas mensagens de auditoria para um dos serviços ADC no local do data center. O serviço ADC é ativado automaticamente para os três primeiros nós de storage instalados em cada local.

Por sua vez, cada serviço ADC atua como um relé e envia sua coleção de mensagens de auditoria para cada nó de administração no sistema StorageGRID, o que dá a cada nó de administração um Registro completo da atividade do sistema.

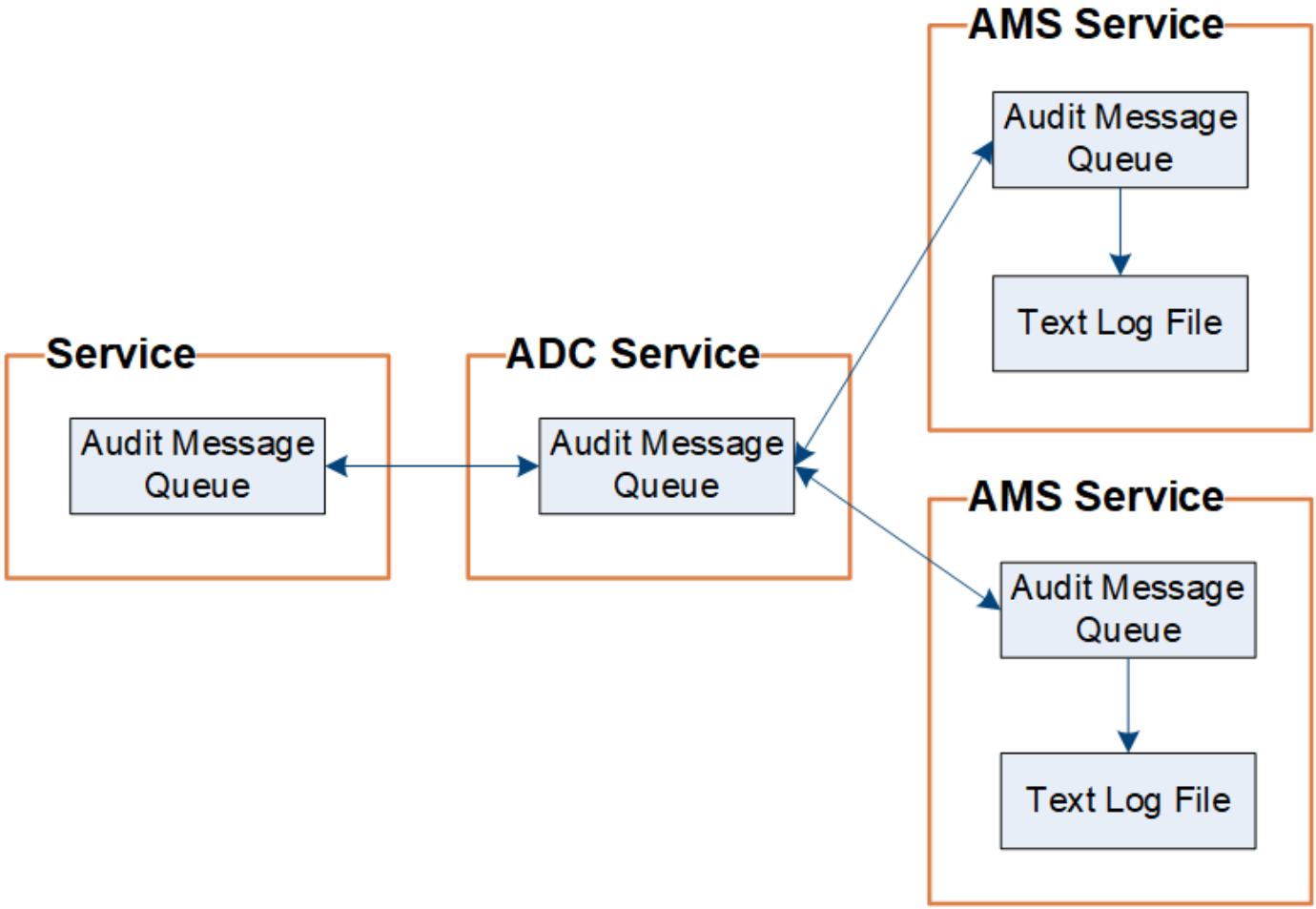
Cada nó Admin armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é `audit.log` nomeado .



Retenção de mensagens de auditoria

O StorageGRID usa um processo de cópia e exclusão para garantir que nenhuma mensagem de auditoria seja perdida antes que ela possa ser gravada no log de auditoria.

Quando um nó gera ou retransmite uma mensagem de auditoria, a mensagem é armazenada em uma fila de mensagens de auditoria no disco do sistema do nó da grade. Uma cópia da mensagem é sempre mantida em uma fila de mensagens de auditoria até que a mensagem seja gravada no arquivo de log de auditoria no diretório do Admin Node `/var/local/log`. Isso ajuda a evitar a perda de uma mensagem de auditoria durante o transporte.



A fila de mensagens de auditoria pode aumentar temporariamente devido a problemas de conetividade de rede ou capacidade de auditoria insuficiente. À medida que as filas aumentam, elas consomem mais espaço disponível no diretório de cada nó `/var/local/`. Se o problema persistir e o diretório de mensagens de auditoria de um nó ficar muito cheio, os nós individuais priorizarão o processamento de seu backlog e ficarão temporariamente indisponíveis para novas mensagens.

Especificamente, você pode ver os seguintes comportamentos:

- Se o `/var/local/log` diretório usado por um nó Admin ficar cheio, o nó Admin será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações do cliente S3 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 cliente S3 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 com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria cresçam muito grandes:

- A interrupção de um nó de administração ou de um nó de storage com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes podem ficar com backlogged.
- Uma taxa de atividade contínua que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC se torna cheio por razões não relacionadas às mensagens de auditoria. Quando isso acontece, o nó pára de aceitar novas mensagens de auditoria e prioriza seu backlog atual, o que pode causar backlogs em outros nós.

Alerta de fila de auditoria grande e alarme de mensagens de auditoria enfileiradas (AMQS)

Para ajudá-lo a monitorar o tamanho das filas de mensagens de auditoria ao longo do tempo, o alerta **fila de auditoria grande** e o alarme AMQS legado são acionados quando o número de mensagens em uma fila de nó de armazenamento ou fila de nó de administrador atinge determinados limites.

Se o alerta **fila de auditoria grande** ou o alarme AMQS legado for acionado, comece verificando a carga no sistema - se houver um número significativo de transações recentes, o alerta e o alarme devem ser resolvidos com o tempo e podem ser ignorados.

Se o alerta ou o alarme persistir e aumentar a gravidade, veja um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para gravações do cliente e leituras do cliente para erro ou Desativado. "Configurar mensagens de auditoria e destinos de log"Consulte .

Mensagens duplicadas

O sistema StorageGRID adota uma abordagem conservadora se ocorrer uma falha de rede ou nó. Por esse motivo, mensagens duplicadas podem existir no log de auditoria.

Acessar o arquivo de log de auditoria

O compartilhamento de auditoria contém o arquivo ativo `audit.log` e todos os arquivos de log de auditoria compatados. Você pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Vá para o diretório que contém os arquivos de log de auditoria:

```
cd /var/local/log
```

3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

Rotação do arquivo de log de auditoria

Os arquivos de logs de auditoria são salvos no diretório de um nó de administrador `/var/local/log`. Os arquivos de log de auditoria ativos são `audit.log` nomeados .

> Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos Registros de auditoria continuam a ser gerados e armazenados quando um servidor syslog externo é configurado. "Configurar mensagens de auditoria e destinos de log"Consulte .

Uma vez por dia, o arquivo ativo `audit.log` é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato *`yyyy-mm-dd.txt`*. Se mais de um log de auditoria for criado em um único dia, os nomes de arquivo usarão a data em que o arquivo foi salvo, anexado por um número, no formato *`yyyy-mm-dd.txt.n`*. Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são os primeiros e segundos arquivos de log criados e salvos em 15 de abril de 2018.

Após um dia, o arquivo salvo é compactado e renomeado, no formato *`yyyy-mm-dd.txt.gz`*, que preserva a data original. Com o tempo, isso resulta no consumo de storage alocado para logs de auditoria no nó Admin. Um script monitora o consumo de espaço do log de auditoria e exclui arquivos de log conforme necessário para liberar espaço no `/var/local/log` diretório. Os logs de auditoria são excluídos com base na data em que foram criados, sendo os mais antigos excluídos primeiro. Você pode monitorar as ações do script no seguinte arquivo: `/var/local/log/manage-audit.log`.

Este exemplo mostra o `audit.log` ficheiro ativo, o ficheiro do dia anterior (`2018-04-15.txt`) e o ficheiro comprimido para o dia anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato de arquivo de log de auditoria

Formato de arquivo de log de auditoria

Os arquivos de log de auditoria são encontrados em cada nó Admin e contêm uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O tempo Universal coordenado (UTC) do evento que acionou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido de um espaço:

YYYY-MM-DDTHH:MM:SS.UUUUUU, onde *UUUUUU* estão microssegundos.

- A própria mensagem de auditoria, entre colchetes e começando com `AUDT`.

O exemplo a seguir mostra três mensagens de auditoria em um arquivo de log de auditoria (quebras de linha adicionadas para legibilidade). Essas mensagens foram geradas quando um locatário criou um bucket do S3 e adicionou dois objetos a esse bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Em seu formato padrão, as mensagens de auditoria nos arquivos de log de auditoria não são fáceis de ler ou

interpretar. Você pode usar o "ferramenta de auditoria-explicação" para obter resumos simplificados das mensagens de auditoria no log de auditoria. Você pode usar o "ferramenta de soma de auditoria" para resumir quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.

Utilize a ferramenta de auditoria-explicação

Você pode usar a `audit-explain` ferramenta para traduzir as mensagens de auditoria no login de auditoria para um formato fácil de ler.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

Sobre esta tarefa

A `audit-explain` ferramenta, disponível no nó de administração principal, fornece resumos simplificados das mensagens de auditoria em um log de auditoria.

> ⓘ A `audit-explain` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-explain` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-explain` ferramenta. Essas quatro "SPUT"mensagens de auditoria foram geradas quando o locatário S3 com ID de conta 92484777680322627870 usou S3 SOLICITAÇÕES PUT para criar um bucket chamado "bucket1" e adicionar três objetos a esse bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

A `audit-explain` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compatados. Por exemplo:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Processe vários arquivos simultaneamente. Por exemplo:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- Aceite a entrada de um pipe, que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep SPUT audit.log | audit-explain

grep bucket-name audit.log | audit-explain
```

Como os logs de auditoria podem ser muito grandes e lentos para analisar, você pode economizar tempo filtrando partes que você deseja olhar e executar `audit-explain` nas partes, em vez de todo o arquivo.

> A `audit-explain` ferramenta não aceita arquivos compatados como entrada pipeada. Para processar arquivos compatados, forneça seus nomes de arquivo como argumentos de linha de comando ou use a `zcat` ferramenta para descomprimir os arquivos primeiro. Por exemplo:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Utilize a `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-explain -h
```

Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   A `audit-explain` ferramenta imprime interpretações humanamente legíveis de todas as mensagens no arquivo ou arquivos especificados.

   > Para reduzir o comprimento das linhas e facilitar a legibilidade, os carimbos de data/hora não são apresentados por predefinição. Se você quiser ver os carimbos de data/hora, use a opção carimbo de data/hora (`-t`).

Use a ferramenta audit-sum

Você pode usar a `audit-sum` ferramenta para contar as mensagens de auditoria de gravação, leitura, cabeçalho e exclusão e ver o tempo mínimo, máximo e médio (ou tamanho) para cada tipo de operação.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

Sobre esta tarefa

A `audit-sum` ferramenta, disponível no nó de administração principal, resume quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.

> A `audit-sum` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-sum` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações de protocolo demoraram.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

A `audit-sum` ferramenta fornece contagens e tempos para as seguintes mensagens de auditoria S3, Swift e ILM em um log de auditoria.

> Os códigos de auditoria são removidos do produto e da documentação, à medida que os recursos são obsoletos. Se você encontrar um código de auditoria que não está listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, "StorageGRID 11,8 usando a documentação da ferramenta de soma de auditoria".

Código	Descrição	Consulte
IDEL	ILM iniciado Excluir: Registra quando ILM inicia o processo de exclusão de um objeto.	"IDEL: ILM iniciou Excluir"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket.	"SDEL: S3 DELETE"

Código	Descrição	Consulte
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	"SHEA: S3 CABEÇA"
SPUT	S3 put: Registra uma transação bem-sucedida para criar um novo objeto ou bucket.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contentor.	"WDEL: Swift DELETE"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contentor.	"WGET: Rápido"
BEM-VINDO	Swift head: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contentor.	"WHEA: CABEÇA rápida"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contentor.	"WPUT: Swift PUT"

A `audit-sum` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compatados. Por exemplo:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Processe vários arquivos simultaneamente. Por exemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- Aceite a entrada de um pipe, que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

Esta ferramenta não aceita arquivos compatados como entrada pipeada. Para processar arquivos compatados, forneça seus nomes de arquivo como argumentos de linha de comando ou use a `zcat` ferramenta para descomprimir os arquivos primeiro. Por exemplo:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Você pode usar as opções de linha de comando para resumir as operações em intervalos separadamente das operações em objetos ou agrupar resumos de mensagens por nome de intervalo, por período de tempo ou por tipo de destino. Por padrão, os resumos mostram o tempo de operação mínimo, máximo e médio, mas você pode usar a `size (-s)` opção para olhar o tamanho do objeto.

Utilize a `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-sum -h
```

Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Se você quiser analisar todas as mensagens relacionadas às operações de gravação, leitura, cabeçalho e exclusão, siga estas etapas:
   a. Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações de protocolo demoraram.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Neste exemplo, as operações de SGET (S3 GET) são as mais lentas em média em 1,13 segundos, mas as operações de SGET e SPUT (S3 PUT) mostram tempos piores longos de cerca de 1.770 segundos.

b. Para mostrar as operações de recuperação 10 mais lentas, use o comando grep para selecionar apenas mensagens SGET e adicionar a opção de saída longa (`-l`) para incluir caminhos de objeto:

   ```
   grep SGET audit.log | audit-sum -l
   ```

   Os resultados incluem o tipo (objeto ou bucket) e o caminho, que permite que você grep o log de auditoria para outras mensagens relacionadas a esses objetos específicos.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
A partir deste exemplo de saída, você pode ver que os três pedidos mais lentos de S3 GET foram para objetos de tamanho de cerca de 5 GB, que é muito maior do que os outros objetos. O tamanho grande é responsável pelos tempos de recuperação lentos do pior caso.

3. Se você quiser determinar em que tamanhos de objetos estão sendo ingeridos e recuperados da grade, use a opção tamanho (`-s`):

   ```
   audit-sum -s audit.log
   ```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

Neste exemplo, o tamanho médio do objeto para SPUT é inferior a 2,5 MB, mas o tamanho médio para SGET é muito maior. O número de mensagens SPUT é muito maior do que o número de mensagens SGET, indicando que a maioria dos objetos nunca são recuperados.

4. Se você quiser determinar se as recuperações foram lentas ontem:

   a. Emita o comando no log de auditoria apropriado e use a opção Group-by-time (`-gt`), seguida pelo período de tempo (por exemplo, 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Esses resultados mostram que S3 RECEBEM tráfego aumentado entre 06:00 e 07:00. Os tempos máximos e médios são consideravelmente mais elevados nestes tempos também, e eles não aumentaram gradualmente à medida que a contagem aumentou. Isso sugere que a capacidade foi excedida em algum lugar, talvez na rede ou na capacidade da grade de processar solicitações.

b. Para determinar que objetos de tamanho estavam sendo recuperados a cada hora ontem, adicione a opção tamanho (`-s`) ao comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Esses resultados indicam que algumas recuperações muito grandes ocorreram quando o tráfego geral de recuperação estava no seu máximo.

c. Para ver mais detalhes, use o "ferramenta de auditoria-explicação" para rever todas as operações SGET durante essa hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se a saída do comando grep for esperada para ser muitas linhas, adicione o `less` comando para mostrar o conteúdo do arquivo de log de auditoria uma página (uma tela) de cada vez.

5. Se você quiser determinar se as operações do SPUT em buckets são mais lentas do que as operações do SPUT para objetos:

a. Comece usando a `-go` opção, que agrupa as mensagens para operações de objeto e bucket separadamente:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Os resultados mostram que as operações do SPUT para buckets têm caraterísticas de desempenho diferentes das operações do SPUT para objetos.

b. Para determinar quais buckets têm as operações de SPUT mais lentas, use a `-gb` opção, que agrupa as mensagens por bucket:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Para determinar quais buckets têm o maior tamanho de objeto SPUT, use as `-gb` opções e `-s`:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Formato da mensagem de auditoria

Formato da mensagem de auditoria

As mensagens de auditoria trocadas no sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico que descreve o evento ou a atividade que está sendo relatada.

Se as informações resumidas fornecidas pelas "auditoria-explicar"ferramentas e "soma de auditoria"forem insuficientes, consulte esta secção para compreender o formato geral de todas as mensagens de auditoria.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no arquivo de log de auditoria:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Cada mensagem de auditoria contém uma cadeia de elementos de atributo. Toda a cadeia de carateres está entre colchetes (`[ ]`), e cada elemento de atributo na cadeia de carateres tem as seguintes caraterísticas:

- Entre os suportes `[ ]`
- Introduzido pela cadeia de carateres `AUDT`, que indica uma mensagem de auditoria
- Sem delimitadores (sem vírgulas ou espaços) antes ou depois
- Terminado por um caractere de alimentação de linha `\n`

Cada elemento inclui um código de atributo, um tipo de dados e um valor que são relatados neste formato:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

O número de elementos de atributo na mensagem depende do tipo de evento da mensagem. Os elementos de atributo não são listados em nenhuma ordem específica.

A lista a seguir descreve os elementos do atributo:

- `ATTR` é um código de quatro carateres para o atributo que está sendo relatado. Existem alguns atributos que são comuns a todas as mensagens de auditoria e outros que são específicos para eventos.
- `type` É um identificador de quatro carateres do tipo de dados de programação do valor, como UI64, FC32 e assim por diante. O tipo está entre parênteses `( )`.
- `value` é o conteúdo do atributo, normalmente um valor numérico ou de texto. Os valores seguem sempre dois pontos (`:`). Os valores do tipo de dados CSTR são cercados por aspas duplas " ".

Tipos de dados

Diferentes tipos de dados são usados para armazenar informações em mensagens de auditoria.

Tipo	Descrição
UI32	Inteiro longo não assinado (32 bits); ele pode armazenar os números de 0 a 4.294.967.295.
UI64	Número inteiro duplo longo não assinado (64 bits); pode armazenar os números de 0 a 18.446.744.073.709.551.615.
FC32	Constante de quatro carateres; um valor inteiro não assinado de 32 bits representado como quatro carateres ASCII, como "ABCD".
IPAD	Usado para endereços IP.
CSTR	Um array de comprimento variável de carateres UTF-8. Os carateres podem ser escapados com as seguintes convenções: • Barra invertida é. • O retorno do carro é r. • Aspas duplas. • A alimentação de linha (nova linha) é n. • Os carateres podem ser substituídos por seus equivalentes hexadecimais (no formato HH, onde HH é o valor hexadecimal que representa o caractere).

Dados específicos do evento

Cada mensagem de auditoria no log de auditoria Registra dados específicos para um evento do sistema.

Após o contentor de abertura `[AUDT:` que identifica a própria mensagem, o próximo conjunto de atributos fornece informações sobre o evento ou ação descrito pela mensagem de auditoria. Esses atributos são destacados no exemplo a seguir:

2018 11454 S3AI SGKH4 6002562159561124649 9 UI64-12 10.224.0 6002562159561124649 E6DYZKLUMRSKJA S3BK-05T08:24 100 S3AK 6002562159561124649 S3KY [AUDT:*[RSLT(FC32):SUCS]* *[TIME STR(UI64):45,921845 E4DA UI64 30720 UI32 10 UI64 1543998285921845 FC32 UI32 12281045 FC32 S3RQ UI64 15552417629170647261

O `ATYP` elemento (sublinhado no exemplo) identifica qual evento gerou a mensagem. Esta mensagem de exemplo inclui o "SHEA"código de mensagem ([ATYP(FC32):SHEA]), indicando que foi gerado por uma solicitação DE CABEÇALHO S3 bem-sucedida.

Elementos comuns em mensagens de auditoria

Todas as mensagens de auditoria contêm os elementos comuns.

Código	Tipo	Descrição
NO MEIO	FC32	ID do módulo: Um identificador de quatro carateres do ID do módulo que gerou a mensagem. Isso indica o segmento de código no qual a mensagem de auditoria foi gerada.
ANID	UI32	ID do nó: O ID do nó da grade atribuído ao serviço que gerou a mensagem. Cada serviço recebe um identificador exclusivo no momento em que o sistema StorageGRID é configurado e instalado. Esta ID não pode ser alterada.
ASES	UI64	Identificador de sessão de auditoria: Em versões anteriores, este elemento indicou o momento em que o sistema de auditoria foi inicializado após o início do serviço. Este valor de tempo foi medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). **Nota:** este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ASQN	UI64	Contagem de sequência: Em versões anteriores, esse contador foi incrementado para cada mensagem de auditoria gerada no nó de grade (ANID) e redefinido para zero na reinicialização do serviço. **Nota:** este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ATID	UI64	ID de rastreamento: Um identificador que é compartilhado pelo conjunto de mensagens que foram acionadas por um único evento.

Código	Tipo	Descrição
ATIM	UI64	Timestamp: A hora em que o evento foi gerado, que acionou a mensagem de auditoria, medida em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o carimbo de data/hora para data e hora locais são baseadas em milissegundos. Pode ser necessário arredondar ou truncar o carimbo de data/hora registado. O tempo legível por humanos que aparece no início da mensagem de auditoria no `audit.log` arquivo é o atributo ATIM no formato ISO 8601. A data e a hora são representadas como *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, onde o `T` é um caractere de cadeia de carateres literal indicando o início do segmento de tempo da data. *`UUUUUU`* são microssegundos.
ATYP	FC32	Tipo de evento: Um identificador de quatro carateres do evento que está sendo registrado. Isso rege o conteúdo "payload" da mensagem: Os atributos que estão incluídos.
AVER	UI32	Versão: A versão da mensagem de auditoria. À medida que o software StorageGRID evolui, novas versões de serviços podem incorporar novos recursos em relatórios de auditoria. Este campo permite a compatibilidade retroativa no serviço AMS para processar mensagens de versões mais antigas de serviços.
RSLT	FC32	Resultado: O resultado de evento, processo ou transação. Se não for relevante para uma mensagem, NENHUM será usado em vez DE SUCS para que a mensagem não seja filtrada acidentalmente.

Exemplos de mensagens de auditoria

Você pode encontrar informações detalhadas em cada mensagem de auditoria. Todas as mensagens de auditoria usam o mesmo formato.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no `audit.log` arquivo:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

A mensagem de auditoria contém informações sobre o evento que está sendo gravado, bem como informações sobre a própria mensagem de auditoria.

Para identificar qual evento é gravado pela mensagem de auditoria, procure o atributo ATYP (destacado abaixo):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

O valor do atributo ATYP é SPUT. "SPUT" Representa uma transação S3 PUT, que Registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o intervalo ao qual o objeto está associado:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Para descobrir quando o evento PUT ocorreu, observe o carimbo de data/hora Universal coordenada (UTC) no início da mensagem de auditoria. Este valor é uma versão legível por humanos do atributo ATIM da própria mensagem de auditoria:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM Registra o tempo, em microssegundos, desde o início da época UNIX. No exemplo, o valor `1405631878959669` é traduzido para Quinta-feira, 17-Jul-2014 21:17:59 UTC.

Auditar mensagens e o ciclo de vida do objeto

Quando são geradas mensagens de auditoria?

As mensagens de auditoria são geradas sempre que um objeto é ingerido, recuperado ou excluído. Você pode identificar essas transações no log de auditoria localizando mensagens de auditoria específicas da API do S3.

As mensagens de auditoria são vinculadas por meio de identificadores específicos a cada protocolo.

Protocolo	Código
Ligar S3 operações	S3BK (balde), S3KY (chave) ou ambos
Ligando as operações Swift	WCON (container), WOBJ (objeto), ou ambos
Vinculação de operações internas	CBID (identificador interno do objeto)

Calendário das mensagens de auditoria

Devido a fatores como diferenças de tempo entre nós de grade, tamanho do objeto e atrasos na rede, a ordem das mensagens de auditoria geradas pelos diferentes serviços pode variar da mostrada nos exemplos nesta seção.

Transações de ingestão de objetos

Você pode identificar transações de ingestão de clientes no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de ingestão 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 fazer 2 cópias ILM.

> Nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Apenas os relacionados à transação de ingestão S3 (SPUT) estão listados.

Este exemplo assume que um bucket do S3 foi criado anteriormente.

SPUT: S3 PUT

A mensagem SPUT é gerada para indicar que uma transação S3 PUT foi emitida para criar um objeto em um intervalo específico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Regras Objeto cumpridas

A mensagem ORLM indica que a política ILM foi satisfeita para este objeto. A mensagem inclui o CBID do objeto e o nome da regra ILM aplicada.

Para objetos replicados, o campo LOCS inclui o ID do nó LDR e o ID do volume das localizações do objeto.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Para objetos codificados por apagamento, o campo LOCS inclui o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

O campo PATH inclui informações de bucket e chave do S3 ou informações de contentor e objeto do Swift, dependendo de qual API foi usada.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Eliminar transações

Você pode identificar transações de exclusão de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de exclusão são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de exclusão são incluídas.

S3 exclua mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
SDEL	S3 Eliminar	Solicitação feita para excluir o objeto de um intervalo.	CBID, S3KY	"SDEL: S3 DELETE"

Swift delete mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
WDEL	Eliminação rápida	Solicitação feita para excluir o objeto de um recipiente ou do recipiente.	CBID, WOBJ	"WDEL: Swift DELETE"

Exemplo: Exclusão de objeto S3

Quando um cliente S3 exclui um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

> Nem todas as mensagens de auditoria geradas durante uma transação de exclusão são listadas no exemplo abaixo. Apenas os relacionados com a transação de exclusão S3 (SDEL) são listados.

SDEL: S3 Excluir

A exclusão de objeto começa quando o cliente envia uma solicitação DeleteObject a um serviço LDR. A mensagem contém o intervalo do qual excluir o objeto e a chave S3 do objeto, que é usada para identificar o objeto.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Recuperar transações objeto

Você pode identificar transações de recuperação de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de recuperação são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de recuperação são incluídas.

S3 mensagens de auditoria de recuperação

Código	Nome	Descrição	Traçado	Consulte
SGET	S3 GET	Solicitação feita para recuperar um objeto de um bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Mensagens de auditoria de recuperação rápida

Código	Nome	Descrição	Traçado	Consulte
WGET	Swift GET	Solicitação feita para recuperar um objeto de um contentor.	CBID, WCON, WOBJ	"WGET: Rápido"

Exemplo: Recuperação de objeto S3D.

Quando um cliente S3 recupera um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Apenas os relacionados à transação de recuperação S3 (SGET) estão listados.

SGET: S3 GET

A recuperação de objetos começa quando o cliente envia uma solicitação GetObject a um serviço LDR. A mensagem contém o intervalo do qual recuperar o objeto e a chave S3 do objeto, que é usada para identificar o objeto.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se a política de bucket permitir, um cliente pode recuperar objetos anonimamente ou recuperar objetos de um bucket que é de propriedade de uma conta de locatário diferente. A mensagem de auditoria contém informações sobre a conta de locatário do proprietário do bucket para que você possa rastrear essas solicitações anônimas e entre contas.

Na mensagem de exemplo a seguir, o cliente envia uma solicitação GetObject para um objeto armazenado em um bucket que ele não possui. Os valores para SBAI e SBAC Registram o ID e o nome da conta do locatário do proprietário do bucket, que difere do ID da conta do locatário e do nome do cliente registrado em S3AI e SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Exemplo: S3 Selecione em um objeto

Quando um cliente S3 emite uma consulta S3 Select em um objeto, as mensagens de auditoria são geradas e salvas no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Somente aqueles relacionados à transação S3 Select (SelectObjectContent) são listados.

Cada consulta resulta em duas mensagens de auditoria: Uma que executa a autorização da solicitação Select S3 (o campo S3SR está definido como "Select") e uma operação GET padrão subsequente que recupera os dados do armazenamento durante o processamento.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):13630097093968959 85]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Mensagens de atualização de metadados

As mensagens de auditoria são geradas quando um cliente S3 atualiza os metadados de um objeto.

Mensagens de auditoria de atualização de metadados do S3

Código	Nome	Descrição	Traçado	Consulte
SUPD	S3 metadados atualizados	Gerado quando um cliente S3 atualiza os metadados de um objeto ingerido.	CBID, S3KY, HTRH	"SUPD: S3 metadados atualizados"

Exemplo: Atualização de metadados S3

O exemplo mostra uma transação bem-sucedida para atualizar os metadados de um objeto S3 existente.

SUPD: Atualização de metadados S3

O cliente S3 faz uma solicitação (SUPD) para atualizar os metadados especificados (`x-amz-meta-\*`) para o objeto S3 (S3KY). Neste exemplo, cabeçalhos de solicitação são incluídos no campo HTRH porque ele foi configurado como um cabeçalho de protocolo de auditoria (**CONFIGURAÇÃO** > **Monitoramento** > **Auditoria e servidor syslog**). "Configurar mensagens de auditoria e destinos de log"Consulte .

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Auditar mensagens

Descrições de mensagens de auditoria

Descrições detalhadas das mensagens de auditoria retornadas pelo sistema são listadas nas seções a seguir. Cada mensagem de auditoria é listada primeiramente em uma tabela que agrupa mensagens relacionadas pela classe de atividade que a mensagem

representa. Esses agrupamentos são úteis tanto para entender os tipos de atividades auditadas quanto para selecionar o tipo desejado de filtragem de mensagens de auditoria.

As mensagens de auditoria também são listadas alfabeticamente por seus códigos de quatro carateres. Esta lista alfabética permite-lhe encontrar informações sobre mensagens específicas.

Os códigos de quatro carateres utilizados ao longo deste capítulo são os valores ATYP encontrados nas mensagens de auditoria, como mostrado na seguinte mensagem de exemplo:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Para obter informações sobre como definir níveis de mensagens de auditoria, alterar destinos de log e usar um servidor syslog externo para suas informações de auditoria, consulte "Configurar mensagens de auditoria e destinos de log"

Auditar categorias de mensagens

Mensagens de auditoria do sistema

As mensagens de auditoria pertencentes à categoria de auditoria do sistema são usadas para eventos relacionados ao próprio sistema de auditoria, estados de nó de grade, atividade de tarefas em todo o sistema (tarefas de grade) e operações de backup de serviço.

Código	Título e descrição da mensagem	Consulte
ECMC	Fragmento de dados com codificação de apagamento em falta: Indica que um fragmento de dados com codificação de apagamento em falta foi detetado.	"ECMC: Fragmento de dados codificado de apagamento em falta"
ECOC	Fragmento de dados codificado por apagamento corrompido: Indica que um fragmento de dados codificado por apagamento corrompido foi detetado.	"ECOC: Fragmento de dados codificado por apagamento corrompido"
ETAF	Falha na autenticação de segurança: Uma tentativa de conexão usando TLS (Transport Layer Security) falhou.	"ETAF: Falha na autenticação de segurança"
GNRG	Registro GNDS: Um serviço atualizado ou registrado informações sobre si mesmo no sistema StorageGRID.	"GNRG: Registro GNDS"
GNUR	GNDS Unregistration: Um serviço não se registrou a partir do sistema StorageGRID.	"GNUR: GNDS Unregistration"

Código	Título e descrição da mensagem	Consulte
GTED	Tarefa de grelha terminada: O serviço CMN terminou de processar a tarefa de grelha.	"GTED: Tarefa de grelha terminada"
GTST	Tarefa de grade iniciada: O serviço CMN começou a processar a tarefa de grade.	"GTST: Tarefa de grade iniciada"
GTSU	Tarefa de grelha enviada: Uma tarefa de grelha foi enviada para o serviço CMN.	"GTSU: Tarefa de grelha enviada"
LLST	Localização perdida: Esta mensagem de auditoria é gerada quando um local é perdido.	"LLST: Localização perdida"
OLST	Objeto perdido: Um objeto solicitado não pode ser localizado dentro do sistema StorageGRID.	"OLST: O sistema detetou Objeto perdido"
ADICIONAR	Desativação da auditoria de segurança: O registo de mensagens de auditoria foi desativado.	"ADICIONAR: Desativação da auditoria de segurança"
SADE	Ativação da auditoria de segurança: O registo de mensagens de auditoria foi restaurado.	"SADE: Ativação da auditoria de segurança"
SVRF	Falha na verificação do armazenamento de objetos: Um bloco de conteúdo falhou verificações.	"SVRF: Falha na verificação do armazenamento de objetos"
SVRU	Verificação desconhecido: Dados de objeto inesperados detetados no armazenamento de objetos.	"SVRU: Verificação do armazenamento de objetos desconhecido"
SYSD	Paragem nó: Foi solicitado um encerramento.	"SYSD: Parada do nó"
SIST	Parada do nó: Um serviço iniciou uma parada graciosa.	"SIST: Paragem do nó"
SYSU	Início do nó: Um serviço foi iniciado; a natureza do desligamento anterior é indicada na mensagem.	"SYSU: Início do nó"

Mensagens de auditoria de armazenamento de objetos

As mensagens de auditoria pertencentes à categoria de auditoria de armazenamento de objetos são usadas para eventos relacionados ao armazenamento e gerenciamento de objetos dentro do sistema StorageGRID. Isso inclui armazenamento de objetos e recuperações, transferências de nó de grade para nó de grade e verificações.

Os códigos de auditoria são removidos do produto e da documentação, à medida que os recursos são obsoletos. Se você encontrar um código de auditoria que não está listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, "Mensagens de auditoria de storage de objetos do StorageGRID 11,8".

Código	Descrição	Consulte
BROR	Pedido apenas de leitura do balde: Um balde entrou ou saiu do modo só de leitura.	"BROR: Pedido apenas de leitura do balde"
CBSE	Fim de envio de objeto: A entidade de origem concluiu uma operação de transferência de dados de nó de grade para nó de grade.	"CBSE: Fim de envio de objeto"
CBRE	Fim de recebimento de objeto: A entidade de destino concluiu uma operação de transferência de dados de nó de grade para nó de grade.	"CBRE: Fim de recebimento do objeto"
CGRR	Solicitação de replicação entre grades: O StorageGRID tentou uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de grade.	"CGRR: Solicitação de replicação de Grade cruzada"
EBDL	Esvaziar balde Excluir: O scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazia).	"EBDL: Apagar balde vazio"
EBKR	Solicitação de balde vazio: Um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou parar de excluir objetos).	"EBKR: Pedido de balde vazio"
SCMT	Object Store commit: Um bloco de conteúdo foi completamente armazenado e verificado, e agora pode ser solicitado.	"SCMT: Solicitação de confirmação do armazenamento de objetos"
SREM	Remoção do armazenamento de objetos: Um bloco de conteúdo foi excluído de um nó de grade e não pode mais ser solicitado diretamente.	"SREM: Armazenamento de objetos Remover"

O cliente lê mensagens de auditoria

As mensagens de auditoria de leitura do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para recuperar um objeto.

Código	Descrição	Usado por	Consulte
S3SL	S3 Selecionar solicitação: Registra uma conclusão após uma solicitação S3 Select ter sido retornada ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.	Cliente S3	"S3SL: S3 Selecione o pedido"
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket. **Nota:** se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SGET: S3 GET"
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	Cliente S3	"SHEA: S3 CABEÇA"
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 faz uma solicitação para criar ou modificar um objeto.

Código	Descrição	Usado por	Consulte
OVWR	Object Overwrite: Registra uma transação para sobrescrever um objeto com outro objeto.	Clientes S3 e Swift	"OVWR: Substituição de objetos"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket. **Nota:** se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SDEL: S3 DELETE"
SPOS	S3 POST: Registra uma transação bem-sucedida para restaurar um objeto do armazenamento do AWS Glacier para um pool de armazenamento em nuvem.	Cliente S3	"SPOS: S3 POST"

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"

Mensagens de auditoria ILM

As mensagens de auditoria pertencentes à categoria de auditoria ILM são usadas para eventos relacionados às operações de gerenciamento do ciclo de vida da informação (ILM).

Código	Título e descrição da mensagem	Consulte
IDEL	Exclusão iniciada ILM: Esta mensagem de auditoria é gerada quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: ILM iniciou Excluir"
LKCU	Limpeza Objeto sobrescrita. Esta mensagem de auditoria é gerada quando um objeto substituído é removido automaticamente para liberar espaço de armazenamento.	"LKCU: Limpeza de objetos sobrescritos"
ORLM	Regras Objeto atendidas: Esta mensagem de auditoria é gerada quando os dados do objeto são armazenados conforme especificado pelas regras ILM.	"ORLM: Regras Objeto cumpridas"

BROR: Pedido apenas de leitura do balde

O serviço LDR gera essa mensagem de auditoria quando um intervalo entra ou sai do modo somente leitura. Por exemplo, um intervalo entra no modo somente leitura enquanto todos os objetos estão sendo excluídos.

Código	Campo	Descrição
BKHD	UUID do balde	A ID do balde.
BROV	Valor da solicitação somente leitura do balde	Se o intervalo está sendo feito somente leitura ou está deixando o estado somente leitura (1: Somente leitura, 0: Não-somente leitura).
JOGOS DE BROS	Motivo apenas de leitura do balde	A razão pela qual o intervalo está sendo feito somente leitura ou deixando o estado somente leitura. Por exemplo, emptyBucket.
S3AI	S3 ID da conta do locatário	O ID da conta de locatário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.

CBRB: Início de recebimento de objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre nós diferentes à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, essa mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.

Código	Campo	Descrição
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.

Código	Campo	Descrição
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.
RSLT	Resultado da transferência	O resultado da operação de transferência (do ponto de vista da entidade de envio): SUCS: Transferência concluída com êxito; todas as contagens de sequência solicitadas foram enviadas. CONL: Conexão perdida durante a transferência CTMO: Tempo limite de conexão durante o estabelecimento ou transferência UNRE: ID do nó de destino inalcançável CRPT: A transferência terminou devido à receção de dados corrompidos ou inválidos

Essa mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi concluída. Se o resultado da transferência tiver sido bem-sucedido, a operação transferiu dados de "Start Sequence Count" (contagem de sequência de início) para "Real End Sequence Count" (contagem de sequência final real). Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, ele também pode ser usado para verificar contagens de réplicas.

CBSB: Início do envio de objetos

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre nós diferentes à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, essa mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.

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.

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.

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 contagem de sequência com a qual a transferência foi iniciada.
CTAS	Contagem sequência fim Real	Indica a última contagem de sequência transferida com êxito. Se a contagem de sequência final real for a mesma que a contagem de sequência inicial e o resultado da transferência não tiver sido bem-sucedido, não foram trocados dados.
RSLT	Resultado da transferência	O resultado da operação de transferência (do ponto de vista da entidade de envio): SUCS: Transferência concluída com êxito; todas as contagens de sequência solicitadas foram enviadas. CONL: Conexão perdida durante a transferência CTMO: Tempo limite de conexão durante o estabelecimento ou transferência UNRE: ID do nó de destino inalcançável CRPT: A transferência terminou devido à receção de dados corrompidos ou inválidos

Essa mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi concluída. Se o resultado da transferência tiver sido bem-sucedido, a operação transferiu dados de "Start Sequence Count" (contagem de sequência de início) para "Real End Sequence Count" (contagem de sequência final real). Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, ele também pode ser usado para verificar contagens de réplicas.

CGRR: Solicitação de replicação de Grade cruzada

Essa mensagem é gerada quando o StorageGRID tenta uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de grade.

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes. O atributo CSIZ foi introduzido no StorageGRID 11,8. Como resultado, as solicitações de replicação entre grade que abrangem uma atualização do StorageGRID 11,7 para 11,8 podem ter um tamanho total de objeto impreciso.
S3AI	S3 ID da conta do locatário	O ID da conta de locatário que possui o bucket do qual o objeto está sendo replicado.
GFID	ID de ligação da federação da grelha	O ID da conexão de federação de grade sendo usado para replicação entre grade.
OPER	Operação CGR	O tipo de operação de replicação entre redes que foi tentada: • 0: Replique objeto • 1: Replique objeto multipart • 2: Replique o marcador de exclusão
S3BK	Balde S3	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo.
VSID	ID da versão	O ID da versão da versão específica de um objeto que estava sendo replicado.
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou erro geral (GERR).

EBDL: Apagar balde vazio

O scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazia).

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes.

Código	Campo	Descrição
CAMINHO	S3 balde/chave	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
RSLT	Resultado da operação de eliminação	O resultado de evento, processo ou transação. Se não for relevante para uma mensagem, NENHUM será usado em vez DE SUCS para que a mensagem não seja filtrada acidentalmente.

EBKR: Pedido de balde vazio

Essa mensagem indica que um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou parar de excluir objetos).

Código	Campo	Descrição
BUID	UUID do balde	A ID do balde.
EBJS	Configuração JSON do bucket vazio	Contém o JSON que representa a configuração atual de bucket vazio.
S3AI	S3 ID da conta do locatário	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.

ECMC: Fragmento de dados codificado de apagamento em falta

Esta mensagem de auditoria indica que o sistema detetou um fragmento de dados codificado de apagamento em falta.

Código	Campo	Descrição
VCMC	ID VCS	O nome do VCS que contém o pedaço em falta.
MCID	Código bloco	O identificador do fragmento codificado de apagamento em falta.
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatória, mas não é relevante para esta mensagem em particular. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ECOC: Fragmento de dados codificado por apagamento corrompido

Essa mensagem de auditoria indica que o sistema detetou um fragmento de dados codificado de apagamento corrompido.

Código	Campo	Descrição
VCCO	ID VCS	O nome do VCS que contém o bloco corrompido.
VLID	ID do volume	O volume RangeDB que contém o fragmento corrompido codificado de apagamento.
CCID	Código bloco	O identificador do fragmento codificado de apagamento corrompido.
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatória, mas não é relevante para esta mensagem em particular. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ETAF: Falha na autenticação de segurança

Esta mensagem é gerada quando uma tentativa de conexão usando TLS (Transport Layer Security) falhou.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP sobre a qual a autenticação falhou.
RUIDA	Identidade do usuário	Um identificador dependente do serviço que representa a identidade do utilizador remoto.

Código	Campo	Descrição
RSLT	Código de motivo	O motivo da falha: SCNI: Falha no estabelecimento de conexão segura. CERM: O certificado estava ausente. CERT: Certificado inválido. CERE: O certificado expirou. CERR: O certificado foi revogado. CSGN: A assinatura do certificado era inválida. CSGU: O signatário do certificado era desconhecido. UCRM: As credenciais do usuário estavam ausentes. UCRI: As credenciais do usuário eram inválidas. UCRU: As credenciais do usuário não foram permitidas. TOUT: A autenticação expirou.

Quando uma conexão é estabelecida com um serviço seguro que usa TLS, as credenciais da entidade remota são verificadas usando o perfil TLS e a lógica adicional incorporada ao serviço. Se esta autenticação falhar devido a certificados ou credenciais inválidos, inesperados ou não permitidos, é registada uma mensagem de auditoria. Isso permite consultas para tentativas de acesso não autorizado e outros problemas de conexão relacionados à segurança.

A mensagem pode resultar de uma entidade remota ter uma configuração incorreta ou de tentativas de apresentar credenciais inválidas ou não permitidas ao sistema. Essa mensagem de auditoria deve ser monitorada para detetar tentativas de obter acesso não autorizado ao sistema.

GNRG: Registro GNDS

O serviço CMN gera essa mensagem de auditoria quando um serviço atualizou ou registrou informações sobre si mesmo no sistema StorageGRID.

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID de nó	O ID do nó do serviço que iniciou a solicitação de atualização.

Código	Campo	Descrição
GNTP	Tipo de dispositivo	O tipo de dispositivo do nó de grade (por exemplo, BLDR para um serviço LDR).
GNDV	Versão do modelo do dispositivo	A cadeia de carateres que identifica a versão do modelo do dispositivo do nó de grade no pacote DMDL.
GNGP	Grupo	O grupo ao qual o nó da grade pertence (no contexto de custos de link e classificação de consulta de serviço).
GNIA	Endereço IP	O endereço IP do nó da grade.

Essa mensagem é gerada sempre que um nó de grade atualiza sua entrada no Grid Nodes Bundle.

GNUR: GNDS Unregistration

O serviço CMN gera essa mensagem de auditoria quando um serviço tem informações não registradas sobre si mesmo a partir do sistema StorageGRID.

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID de nó	O ID do nó do serviço que iniciou a solicitação de atualização.

GTED: Tarefa de grelha terminada

Esta mensagem de auditoria indica que o serviço CMN terminou de processar a tarefa de grade especificada e moveu a tarefa para a tabela Histórico. Se o resultado for SUCS, ABRT ou ROLF, haverá uma mensagem de auditoria Grid Task Started correspondente. Os outros resultados indicam que o processamento desta tarefa de grade nunca foi iniciado.

Código	Campo	Descrição
TSID	Código tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa de grade seja gerenciada ao longo de seu ciclo de vida. **Observação:** o ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.
RSLT	Resultado	O resultado final do status da tarefa de grade: • SUCS: A tarefa de grade foi concluída com sucesso. • ABRT: A tarefa de grade foi encerrada sem um erro de reversão. • ROLF: A tarefa de grade foi encerrada e não foi possível concluir o processo de reversão. • CANC: A tarefa de grade foi cancelada pelo usuário antes de ser iniciada. • EXPR: A tarefa de grade expirou antes de ser iniciada. • IVLD: A tarefa de grade era inválida. • AUTH: A tarefa de grade não foi autorizada. • DUPL: A tarefa de grade foi rejeitada como uma duplicata.

GTST: Tarefa de grade iniciada

Esta mensagem de auditoria indica que o serviço CMN começou a processar a tarefa de grade especificada. A mensagem de auditoria segue imediatamente a mensagem de tarefa de Grade enviada para tarefas de grade iniciadas pelo serviço de envio de tarefa de Grade interno e selecionadas para ativação automática. Para tarefas de grade enviadas para a tabela pendente, essa mensagem é gerada quando o usuário inicia a tarefa de grade.

Código	Campo	Descrição
TSID	Código tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Observação:** o ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.

Código	Campo	Descrição
RSLT	Resultado	O resultado. Este campo tem apenas um valor: • SUCS: A tarefa de grade foi iniciada com sucesso.

GTSU: Tarefa de grelha enviada

Esta mensagem de auditoria indica que uma tarefa de grade foi enviada ao serviço CMN.

Código	Campo	Descrição
TSID	Código tarefa	Identifica de forma única uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Observação:** o ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.
TTYP	Tipo tarefa	O tipo de tarefa de grade.
TVER	Versão da tarefa	Um número que indica a versão da tarefa de grade.
TDSC	Descrição tarefa	Uma descrição humanamente legível da tarefa de grade.
CUBAS	Válido após Timestamp	A primeira vez (UINT64 microssegundos a partir de 1 de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
VBTS	Válido antes do Timestamp	A última hora (UINT64 microssegundos a partir de 1 de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
TSRC	Fonte	A origem da tarefa: • TXTB: A tarefa de grade foi enviada pelo sistema StorageGRID como um bloco de texto assinado. • GRADE: A tarefa de grade foi enviada através do Serviço interno de envio de tarefa de Grade.
ACTV	Tipo de ativação	O tipo de ativação: • AUTO: A tarefa de grade foi submetida para ativação automática. • PEND: A tarefa de grade foi enviada para a tabela pendente. Esta é a única possibilidade para a fonte TXTB.

Código	Campo	Descrição
RSLT	Resultado	O resultado da submissão: • SUCS: A tarefa de grade foi enviada com sucesso. • FALHA: A tarefa foi movida diretamente para a tabela histórica.

IDEL: ILM iniciou Excluir

Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto.

A mensagem IDEL é gerada em qualquer uma destas situações:

- **Para objetos em buckets S3 compatíveis**: Esta mensagem é gerada quando o ILM inicia o processo de exclusão automática de um objeto porque seu período de retenção expirou (assumindo que a configuração de exclusão automática esteja ativada e a retenção legal esteja desativada).
- **Para objetos em buckets S3 não compatíveis**. Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto porque nenhuma instrução de posicionamento nas políticas ativas do ILM se aplica atualmente ao objeto.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CMPA	Conformidade: Eliminação automática	Apenas para objetos em buckets compatíveis com S3. 0 (falso) ou 1 (verdadeiro), indicando se um objeto compatível deve ser excluído automaticamente quando seu período de retenção terminar, a menos que o intervalo esteja sob uma retenção legal.
CMPL	Conformidade: Guarda legal	Apenas para objetos em buckets compatíveis com S3. 0 (falso) ou 1 (verdadeiro), indicando se o balde está atualmente sob uma retenção legal.
CMPR	Conformidade: Período de retenção	Apenas para objetos em buckets compatíveis com S3. O comprimento do período de retenção do objeto em minutos.
CTME	Conformidade: Tempo de ingestão	Apenas para objetos em buckets compatíveis com S3. O tempo de ingestão do objeto. Você pode adicionar o período de retenção em minutos a esse valor para determinar quando o objeto pode ser excluído do intervalo.
DMRK	Eliminar ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket com versão. As operações em baldes não incluem este campo.

Código	Campo	Descrição
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 balde/chave	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	• 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 grava um objeto em um caminho que já contém um objeto. O processo de remoção ocorre automaticamente e em segundo plano.

Código	Campo	Descrição
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LTYP	Tipo de limpeza	*Somente uso interno.*
LUID	UUUID Objeto removido	O identificador do objeto que foi removido.
CAMINHO	S3 balde/chave	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
UUID	Identificador universal único	O identificador do objeto que ainda existe. Este valor só está disponível se o objeto não tiver sido excluído.

LKDM: Limpeza de objetos vazados

Esta mensagem é gerada quando um pedaço vazado foi limpo ou excluído. Um bloco pode fazer parte de um objeto replicado ou de um objeto codificado por apagamento.

Código	Campo	Descrição
CLOC	Localização de chunk	O caminho do arquivo da parte vazada que foi excluída.

CTYP	Tipo de bloco	Tipo de pedaço:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

Código	Campo	Descrição

LTYP	Tipo de fuga	Os cinco tipos de fugas que podem ser detetadas:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	Chunk criar tempo	Tempo em que o pedaço vazado foi criado.
UUID	Identificador universal único	O identificador do objeto ao qual o bloco pertence.
CBID	Identificador do bloco de conteúdo	CBID do objeto ao qual o pedaço vazado pertence.
CSIZ	Tamanho do conteúdo	O tamanho do bloco em bytes.

LLST: Localização perdida

Essa mensagem é gerada sempre que um local para uma cópia de objeto (replicado ou codificado por apagamento) não pode ser encontrado.

Código	Campo	Descrição
CBIL	CBID	O CBID afetado.
ECPR	Perfil de codificação de apagamento	Para dados de objetos codificados por apagamento. O ID do perfil de codificação de apagamento usado.

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
NOID	Código nó origem	O ID do nó no qual os locais foram perdidos.
PCLD	Caminho para o objeto replicado	O caminho completo para a localização do disco dos dados do objeto perdido. Somente retornado quando LTYP tem um valor de CLDI (ou seja, para objetos replicados). Toma a forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Resultado	Sempre NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.
TSRC	Fonte de acionamento	UTILIZADOR: Utilizador acionado SIST: Sistema acionado
UUID	ID universal única	O identificador do objeto afetado no sistema StorageGRID.

MGAU: Mensagem de auditoria de gestão

A categoria Gerenciamento Registra as solicitações do usuário para a API de gerenciamento. Cada solicitação HTTP que não é uma solicitação GET ou HEAD para um URI de API válido Registra uma resposta contendo o nome de usuário, IP e tipo de solicitação para a API. URIs API inválidas (como /api/v3-autorize) e solicitações inválidas para URIs API válidas não são registradas.

Código	Campo	Descrição
MDIP	Endereço IP de destino	O endereço IP do servidor (destino).
MDNA	Nome de domínio	O nome de domínio do host.
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	O conteúdo do corpo do pedido. Enquanto o corpo da resposta é registrado por padrão, o corpo da solicitação é registrado em certos casos quando o corpo da resposta está vazio. Como as seguintes informações não estão disponíveis no corpo de resposta, elas são retiradas do corpo de solicitação para os seguintes métodos POST: • Nome de usuário e ID de conta em **POST autorize** • Nova configuração de sub-redes em **POST /grid/grid-networks/update** • Novos servidores NTP em **POST /Grid/ntp-server/update** • IDs de servidor desativadas em **POST /Grid/Servers/Deactivation** **Nota:** as informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MRMD	Método de solicitação	O método de solicitação HTTP: • POST • COLOQUE • ELIMINAR • PATCH
MRSC	Código de resposta	O código de resposta.
MRSP	Corpo de resposta	O conteúdo da resposta (o corpo da resposta) é registrado por padrão. **Nota:** as informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MSIP	Endereço IP de origem	O endereço IP do cliente (origem).
MUUN	URN de utilizador	A URNA (nome uniforme do recurso) do usuário que enviou a solicitação.
RSLT	Resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.

OLST: O sistema detetou Objeto perdido

Esta mensagem é gerada quando o serviço DDS não consegue localizar cópias de um objeto dentro do sistema StorageGRID.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto perdido.
NOID	ID de nó	Se disponível, a última localização direta ou próxima do objeto perdido conhecida. É possível ter apenas o ID do nó sem um ID de volume se as informações do volume não estiverem disponíveis.
CAMINHO	S3 balde/chave	Se disponível, o nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.
UUID	ID universal única	O identificador do objeto perdido dentro do sistema StorageGRID.
VOLI	ID do volume	Se disponível, o ID de volume do nó de armazenamento para o último local conhecido do objeto perdido.

ORLM: Regras Objeto cumpridas

Esta mensagem é gerada quando o objeto é armazenado e copiado com sucesso, conforme especificado pelas regras ILM.

> A mensagem ORLM não é gerada quando um objeto é armazenado com êxito pela regra de fazer cópias 2 padrão se outra regra na política usar o filtro avançado tamanho do objeto.

Código	Campo	Descrição
BUID	Colhedor do balde	Campo ID do balde. Usado para operações internas. Aparece apenas se STAT for PRGD.
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.

Código	Campo	Descrição
LOCALIZAÇÃO	Locais	O local de armazenamento de dados de objetos no sistema StorageGRID. O valor para LOCS é "" se o objeto não tiver locais (por exemplo, ele foi excluído). CLEC: Para objetos codificados por apagamento, o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento que é aplicado aos dados do objeto. CLDI: Para objetos replicados, o ID do nó LDR e o ID do volume da localização do objeto. CLNL: ARC node ID da localização do objeto se os dados do objeto forem arquivados.
CAMINHO	S3 balde/chave	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	O rótulo legível 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.
VSID	ID da versão	A ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

A mensagem de auditoria ORLM pode ser emitida mais de uma vez para um único objeto. Por exemplo, ele é

emitido sempre que ocorrer um dos seguintes eventos:

- As regras de ILM para o objeto são satisfeitas para sempre.
- As regras de ILM para o objeto são satisfeitas para esta época.
- As regras do ILM excluíram o objeto.
- O processo de verificação em segundo plano deteta que uma cópia dos dados de objetos replicados está corrompida. O sistema StorageGRID executa uma avaliação ILM para substituir o objeto corrompido.

Informações relacionadas

- "Transações de ingestão de objetos"
- "Eliminar transações"

OVWR: Substituição de objetos

Esta mensagem é gerada quando uma operação externa (solicitada pelo cliente) faz com que um objeto seja substituído por outro objeto.

Código	Campo	Descrição
CBID	Identificador de bloco de conteúdo (novo)	O CBID para o novo objeto.
CSIZ	Tamanho Objeto anterior	O tamanho, em bytes, do objeto que está sendo substituído.
OCBD	Identificador de bloco de conteúdo (anterior)	O CBID para o objeto anterior.
UUID	ID universal única (novo)	O identificador do novo objeto dentro do sistema StorageGRID.
OUID	ID universal única (anterior)	O identificador para o objeto anterior dentro do sistema StorageGRID.
CAMINHO	S3 caminho do objeto	O caminho do objeto S3 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.

S3SL: S3 Selecione o pedido

Esta mensagem regista uma conclusão depois de uma solicitação de seleção S3 ter sido devolvida ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.

Código	Campo	Descrição
BYSC	Bytes digitalizados	Número de bytes verificados (recebidos) dos nós de storage. BYSC e BYPR provavelmente serão diferentes se o objeto estiver compactado. Se o objeto for compactado, o BYSC teria a contagem de bytes compatados e o BYPR seria os bytes após a descompressão.
BYPR	Bytes processados	Número de bytes processados. Indica quantos bytes de "bytes digitalizados" foram realmente processados ou agidos por uma tarefa S3 Select.
BYRT	Bytes retornados	Número de bytes que um trabalho S3 Select retornou ao cliente.
REPR	Registos processados	Número de Registros ou linhas que uma tarefa S3 Select recebeu de nós de storage.
RERT	Registos devolvidos	Número de Registros ou linhas que um trabalho S3 Select retornou ao cliente.
JOFI	Trabalho concluído	Indica se o S3 Select job finished processing or not (Selecionar trabalho concluído ou não). Se isso for falso, a tarefa não foi concluída e os campos de erro provavelmente terão dados neles. O cliente pode ter recebido resultados parciais ou nenhum resultado.
REID	ID da solicitação	Identificador para a solicitação S3 Select.
EXTM	Tempo de execução	O tempo, em segundos, levou para que o S3 Select Job fosse concluído.
ERMG	Mensagem de erro	Mensagem de erro gerada pela tarefa S3 Select.
ERTY	Tipo de erro	Tipo de erro que o S3 Select job gerou.
ERST	Erro Stacktrace	Erro Stacktrace gerado pela tarefa S3 Select.
S3BK	Balde S3	O nome do bucket S3.

Código	Campo	Descrição
S3AK	S3 ID da chave de acesso (remetente do pedido)	O ID da chave de acesso S3 para o usuário que enviou a solicitação.
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo.

ADICIONAR: Desativação da auditoria de segurança

Essa mensagem indica que o serviço de origem (ID do nó) desativou o Registro de mensagens de auditoria; as mensagens de auditoria não estão mais sendo coletadas ou entregues.

Código	Campo	Descrição
AETM	Ativar método	O método utilizado para desativar a auditoria.
AEUN	Nome de utilizador	O nome de usuário que executou o comando para desativar o log de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

A mensagem implica que o registo foi anteriormente ativado, mas agora foi desativado. Normalmente, isso é usado apenas durante a ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada (SADE) e a capacidade de desativar a auditoria é então permanentemente bloqueada.

SADE: Ativação da auditoria de segurança

Esta mensagem indica que o serviço de origem (ID do nó) restaurou o registo de mensagens de auditoria; as mensagens de auditoria estão novamente a ser recolhidas e entregues.

Código	Campo	Descrição
AETM	Ativar método	O método utilizado para ativar a auditoria.
AEUN	Nome de utilizador	O nome de usuário que executou o comando para ativar o log de auditoria.

Código	Campo	Descrição
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

A mensagem implica que o registo foi anteriormente desativado (SADD), mas foi agora restaurado. Isso geralmente é usado apenas durante a ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada e a capacidade de desativar a auditoria é então permanentemente bloqueada.

SCMT: Confirmação de armazenamento de objetos

O conteúdo da grade não é disponibilizado ou reconhecido como armazenado até que ele tenha sido comprometido (ou seja, ele foi armazenado persistentemente). O conteúdo armazenado persistentemente foi completamente gravado no disco e passou por verificações de integridade relacionadas. Essa mensagem é emitida quando um bloco de conteúdo é comprometido com o armazenamento.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo comprometido com o armazenamento permanente.
RSLT	Código do resultado	Status no momento em que o objeto foi armazenado no disco: SUCS: Objeto armazenado com sucesso.

Esta mensagem significa que um determinado bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado. Ele pode ser usado para rastrear o fluxo de dados dentro do sistema.

SDEL: S3 DELETE

Quando um cliente S3 emite uma transação DE EXCLUSÃO, uma solicitação é feita para remover o objeto ou bucket especificado ou para remover um subrecurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.
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 excluído em bytes. As operações em baldes não incluem este campo.
DMRK	Eliminar ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket com versão. As operações em baldes não incluem este campo.
GFID	ID ligação Federação grelha	O ID de conexão da conexão de federação de grade associada a uma solicitação de exclusão de replicação entre grade. Incluído apenas nos registos de auditoria na grelha de destino.
GFSA	Código conta origem Federação grelha	O ID da conta do locatário na grade de origem para uma solicitação de exclusão de replicação entre grade. Incluído apenas nos registos de auditoria na grelha de destino.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `` `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). `` `x-amz-bypass-governance-retention` é incluído automaticamente se estiver presente na solicitação.
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do resultado	Resultado da transação DE EXCLUSÃO. O resultado é sempre: SUCS: Bem-sucedido
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.

Código	Campo	Descrição
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SGRP	Local (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o local onde o objeto foi ingerido.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.

Código	Campo	Descrição
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUDM	Identificador único universal para um marcador de exclusão	O identificador de um marcador de exclusão. As mensagens de log de auditoria especificam UUDM ou UUUUID, onde UUDM indica um marcador de exclusão criado como resultado de uma solicitação de exclusão de objeto, e UUID indica um objeto.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SGET: S3 GET

Quando um cliente S3 emite uma transação GET, uma solicitação é feita para recuperar um objeto ou listar os objetos em um bucket ou remover um subrecurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em baldes não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
LITY	ListObjectsV2	Foi solicitada uma resposta *v2 format*. Para obter detalhes, "AWS ListObjectsV2" consulte . Apenas para operações DO balde GET.
NCHD	Número de crianças	Inclui chaves e prefixos comuns. Apenas para operações DO balde GET.
RANG	Leitura de intervalo	Apenas para operações de leitura de gama. Indica o intervalo de bytes que foi lido por esta solicitação. O valor após a barra (/) mostra o tamanho de todo o objeto.
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.

Código	Campo	Descrição
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
TRNC	Truncado ou não truncado	Defina como false se todos os resultados foram retornados. Defina como verdadeiro se mais resultados estiverem disponíveis para retornar. Apenas para operações DO balde GET.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SHEA: S3 CABEÇA

Quando um cliente S3 emite uma TRANSAÇÃO PRINCIPAL, uma solicitação é feita para verificar a existência de um objeto ou bucket e recuperar os metadados sobre um objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto verificado em bytes. As operações em baldes não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `` `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). ``
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.

Código	Campo	Descrição
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPOS: S3 POST

Quando um cliente S3 emite uma solicitação POST Object, essa mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). (Não esperado para SPOS).
RSLT	Código do resultado	Resultado da solicitação de RestoreObject. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.

Código	Campo	Descrição
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável. Defina como "Select" (selecionar) para uma operação de seleção S3D.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SRCF	Configuração de sub-recurso	Restaurar informações.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.

Código	Campo	Descrição
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPUT: S3 PUT

Quando um cliente S3 emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou bucket, ou para remover um subrecurso bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.
CMPS	Definições de conformidade	As configurações de conformidade usadas ao criar o bucket, se estiverem presentes na solicitação (truncadas para os primeiros 1024 carateres).
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em baldes não incluem este campo.
GFID	ID ligação Federação grelha	O ID de conexão da conexão de federação de grade associada a uma solicitação PUT DE replicação entre grade. Incluído apenas nos registos de auditoria na grelha de destino.
GFSA	Código conta origem Federação grelha	O ID da conta do locatário na grade de origem para uma solicitação DE COLOCAÇÃO DE replicação entre grade. Incluído apenas nos registos de auditoria na grelha de destino.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). `x-amz-bypass-governance-retention` é incluído automaticamente se estiver presente na solicitação.
LKEN	Bloqueio Objeto ativado	Valor do cabeçalho da solicitação `x-amz-bucket-object-lock-enabled` , se presente na solicitação.
LKLH	Bloqueio Objeto retenção legal	Valor do cabeçalho da solicitação `x-amz-object-lock-legal-hold` , se estiver presente na solicitação PutObject.
LKMD	Modo de retenção de bloqueio de objetos	Valor do cabeçalho da solicitação `x-amz-object-lock-mode` , se estiver presente na solicitação PutObject.
LKRU	Reter Data até bloqueio Objeto	Valor do cabeçalho da solicitação `x-amz-object-lock-retain-until-date` , se estiver presente na solicitação PutObject. Os valores são limitados a 100 anos a partir da data em que o objeto foi ingerido.
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.

Código	Campo	Descrição
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SRCF	Configuração de sub-recurso	A nova configuração de subrecursos (truncada para os primeiros 1024 carateres).
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UID	ID de carregamento	Incluído apenas nas mensagens SPUT para operações CompleteMultipartUpload. Indica que todas as peças foram carregadas e montadas.

Código	Campo	Descrição
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	A ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.
VSST	Estado de controle de versão	O novo estado de controle de versão de um bucket. Dois estados são usados: "Habilitado" ou "suspenso". As operações em objetos não incluem este campo.

SREM: Armazenamento de objetos Remover

Essa mensagem é emitida quando o conteúdo é removido do armazenamento persistente e não é mais acessível por meio de APIs regulares.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo excluído do armazenamento permanente.
RSLT	Código do resultado	Indica o resultado das operações de remoção de conteúdo. O único valor definido é: SUCS: Conteúdo removido do armazenamento persistente

Essa mensagem de auditoria significa que um determinado bloco de conteúdo foi excluído de um nó e não pode mais ser solicitado diretamente. A mensagem pode ser usada para rastrear o fluxo de conteúdo excluído dentro do sistema.

SUPD: S3 metadados atualizados

Essa mensagem é gerada pela API S3 quando um cliente S3 atualiza os metadados de um objeto ingerido. A mensagem é emitida pelo servidor se a atualização de metadados for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação, ao atualizar as configurações de conformidade de um bucket.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em baldes não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.

Código	Campo	Descrição
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto cujos metadados foram atualizados. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SVRF: Falha na verificação do armazenamento de objetos

Esta mensagem é emitida sempre que um bloco de conteúdo falha no processo de verificação. Cada vez que os dados de objeto replicados são lidos ou gravados no disco, várias verificações e verificações de integridade são realizadas para garantir que os dados enviados ao usuário solicitante sejam idênticos aos dados originalmente ingeridos no sistema. Se alguma dessas verificações falhar, o sistema coloca automaticamente em quarentena os dados de objeto replicados corrompidos para impedir que sejam recuperados novamente.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que falhou a verificação.

Código	Campo	Descrição
RSLT	Código do resultado	Tipo de falha de verificação: CRCF: Falha na verificação de redundância cíclica (CRC). HMAC: Falha na verificação HMAC (hash-based message Authentication code). EHSH: Hash de conteúdo criptografado inesperado. PHSH: Hash de conteúdo original inesperado. SEQC: Sequência de dados incorreta no disco. PERR: Estrutura inválida do arquivo de disco. DERR: Erro de disco. FNAM: Nome de arquivo ruim.

Esta mensagem deve ser monitorada de perto. Falhas de verificação de conteúdo podem indicar falhas iminentes de hardware.

Para determinar que operação acionou a mensagem, consulte o valor do campo AID (ID do módulo). Por exemplo, um valor SVFY indica que a mensagem foi gerada pelo módulo Storage Verifier, ou seja, verificação em segundo plano e STOR indica que a mensagem foi acionada pela recuperação de conteúdo.

SVRU: Verificação do armazenamento de objetos desconhecido

O componente de armazenamento do serviço LDR verifica continuamente todas as cópias de dados de objetos replicados no armazenamento de objetos. Esta mensagem é emitida quando uma cópia desconhecida ou inesperada de dados de objetos replicados é detetada no armazenamento de objetos e movida para o diretório de quarentena.

Código	Campo	Descrição
FPTH	Caminho do ficheiro	O caminho do arquivo da cópia de objeto inesperada.
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

A mensagem de auditoria SVRU: Object Store Verify Unknown deve ser monitorada de perto. Isso significa que cópias inesperadas de dados de objetos foram detetadas no armazenamento de objetos. Essa situação deve ser investigada imediatamente para determinar como essas cópias foram criadas, pois pode indicar falhas iminentes de hardware.

SYSD: Parada do nó

Quando um serviço é parado graciosamente, essa mensagem é gerada para indicar que o desligamento foi solicitado. Normalmente, esta mensagem é enviada apenas após um reinício subsequente, porque a fila de mensagens de auditoria não é eliminada antes do encerramento. Procure a mensagem DO SISTEMA, enviada no início da sequência de encerramento, se o serviço não tiver sido reiniciado.

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O RSLT de um SYSD não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SIST: Paragem do nó

Quando um serviço é parado graciosamente, essa mensagem é gerada para indicar que o desligamento foi solicitado e que o serviço iniciou sua sequência de desligamento. O SYST pode ser usado para determinar se o desligamento foi solicitado, antes que o serviço seja reiniciado (ao contrário do SYSD, que normalmente é enviado após o reinício do serviço).

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O código RSLT de uma mensagem DO SISTEMA não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SYSU: Início do nó

Quando um serviço é reiniciado, essa mensagem é gerada para indicar se o desligamento anterior foi limpo (comandado) ou desordenado (inesperado).

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa. DSDN: O sistema não foi desligado corretamente. VRGN: O sistema foi iniciado pela primeira vez após a instalação do servidor (ou reinstalação).

A mensagem não indica se o servidor host foi iniciado, apenas o serviço de relatórios. Esta mensagem pode ser usada para:

- Detecte a descontinuidade na trilha de auditoria.
- Determine se um serviço está falhando durante a operação (uma vez que a natureza distribuída do sistema StorageGRID pode mascarar essas falhas). O Server Manager reinicia automaticamente um serviço com falha.

WDEL: Swift DELETE

Quando um cliente Swift emite uma transação DE EXCLUSÃO, uma solicitação é feita para remover o objeto ou contentor especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contentores não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. As operações em contentores não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.

Código	Campo	Descrição
RSLT	Código do resultado	Resultado da transação DE EXCLUSÃO. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
SGRP	Local (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o local onde o objeto foi ingerido.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contentores não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WGET: Rápido

Quando um cliente Swift emite uma transação GET, uma solicitação é feita para recuperar um objeto, listar os objetos em um contentor ou listar os contentores em uma conta. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contas e containers não incluem esse campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contas e containers não incluem esse campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift. As operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contas e containers não incluem esse campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WHEA: CABEÇA rápida

Quando um cliente Swift emite uma TRANSAÇÃO PRINCIPAL, uma solicitação é feita para verificar a existência de uma conta, contentor ou objeto e recuperar quaisquer metadados relevantes. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contas e containers não incluem esse campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contas e containers não incluem esse campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO PRINCIPAL. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift. As operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contas e containers não incluem esse campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WPUT: Swift PUT

Quando um cliente Swift emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou contentor. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contentores não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contentores não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift.

Código	Campo	Descrição
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contentores não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

Expanda uma grade

Tipos de expansão

Você pode expandir a capacidade ou as funcionalidades do sistema StorageGRID sem interromper as operações do sistema.

Uma expansão StorageGRID permite adicionar:

- Volumes de storage para nós de storage
- Novos nós de grade para um local existente
- Um novo site inteiro

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.

Siga as etapas para o tipo de expansão que você está executando:

Adicione volumes de armazenamento

Siga os passos para "Adição de volumes de storage aos nós de storage".

Adicionar nós de grade

1. Siga os passos para "adicionando nós de grade a um local existente".
2. "Atualize as sub-redes".
3. Implantar nós de grade:
   - "Aparelhos"
   - "VMware"
   - "Linux"

   > ⓘ "Linux" refere-se a uma implantação Red Hat Enterprise Linux, Ubuntu ou Debian. Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

4. "Execute a expansão".
5. "Configure o sistema expandido".

Adicionar novo site

1. Siga os passos para "Adicionar um novo site".
2. "Atualize as sub-redes".
3. Implantar nós de grade:
   - "Aparelhos"
   - "VMware"
   - "Linux"

   > ⓘ "Linux" refere-se a uma implantação Red Hat Enterprise Linux, Ubuntu ou Debian. Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

4. "Execute a expansão".
5. "Configure o sistema expandido".

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 as regras atuais do ILM para determinar onde e quando "adicione volumes de armazenamento"aumentar o armazenamento disponível para "objetos replicados" ou "objetos com codificação de apagamento".
- Não é possível aumentar a capacidade de metadados do sistema adicionando volumes de armazenamento 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. Cada compartimento de expansão adiciona 16 volumes de storage. Com ambas as gavetas de expansão instaladas, o SG6060 dá suporte a um total de 48 volumes de storage.
- Você pode adicionar uma ou duas gavetas de expansão a cada dispositivo SG6160. Cada compartimento de expansão adiciona 60 volumes de storage. Com ambas as gavetas de expansão instaladas, o SG6160 dá suporte a um total de 180 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 você está executando uma atualização do sistema, 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, vá para "Adicione o compartimento de expansão ao SG6060 implantado".
- Para adicionar uma ou duas gavetas de expansão a um dispositivo de storage SG6160, vá para "Adicione o compartimento de expansão ao SG6160 implantado"
- 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 as regras atuais do ILM para determinar onde e quando adicionar nós de storage para aumentar o storage disponível para "objetos replicados" ou "objetos com codificação de apagamento".
- 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.
- Não é possível 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 tem uma grade de dois locais e uma regra ILM que cria uma cópia de objeto em cada local, você deve "adicione armazenamento" para cada local para aumentar a capacidade geral de objeto da grade. Para obter informações sobre replicação de objetos, "O que é replicação"consulte .

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".

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. "O que são esquemas de codificação de apagamento"Consulte para obter informações sobre perfis de codificação de apagamento.

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 levaram a esta recomendação ou para desenvolver um plano mais preciso para o seu site, "Considerações para rebalanceamento de dados codificados por apagamento"consulte . Para obter uma recomendação personalizada otimizada para a sua situação, entre em Contato com o consultor de Serviços profissionais da NetApp.

Considerações para rebalanceamento de dados codificados por apagamento

Se você estiver executando uma expansão para adicionar nós de storage e usar regras de ILM para apagar dados de código, talvez seja necessário executar o procedimento de rebalanceamento de codificação de apagamento (EC) se não for possível adicionar nós de storage suficientes para o esquema de codificação de apagamento que você está usando.

Depois de analisar estas considerações, execute a expansão e, em seguida, vá para 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-adicionados em um local.

O procedimento de reequilíbrio CE:

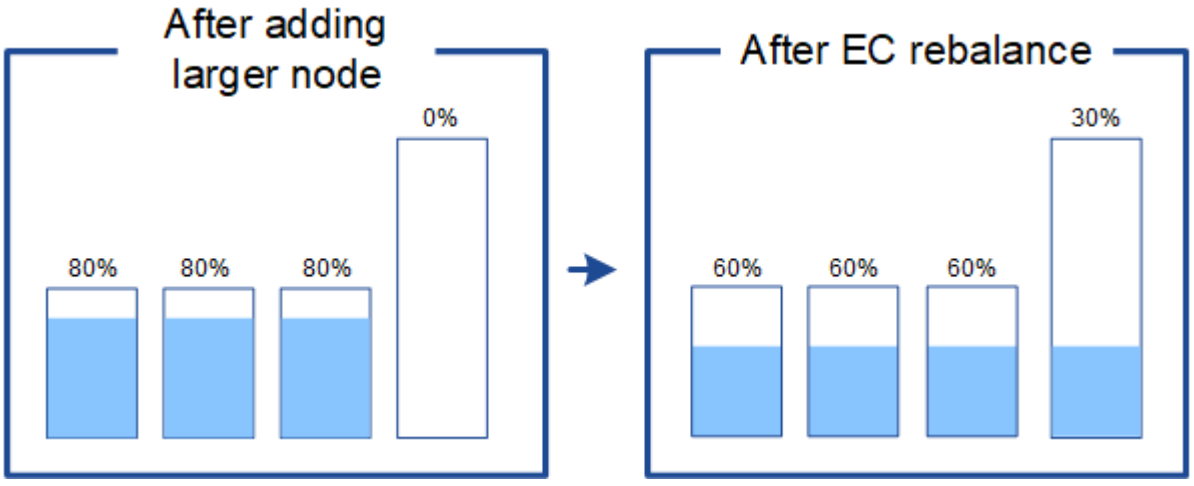
- Move apenas dados de objetos codificados por apagamento. Ele não move dados de objetos replicados.

- 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.
- Redistribui uniformemente os dados codificados por apagamento entre os nós de storage, sem considerar as capacidades relativas de cada nó.
- Não distribuirá dados codificados por apagamento para nós de storage que estejam mais de 80% cheios.
- Pode diminuir o desempenho das operações ILM e das operações de cliente S3 quando executa& n.o 8212;recursos adicionais são necessários para redistribuir os fragmentos de codificação de apagamento.

Quando o procedimento de reequilíbrio CE estiver concluído:

- Os dados codificados por apagamento terão migrado dos nós de storage com menos espaço disponível para os nós de storage com mais espaço disponível.
- A proteção de dados de objetos codificados por apagamento não será alterada.
- Os valores usados (%) podem ser diferentes entre nós de storage por dois motivos:
  - As cópias de objetos replicadas continuarão a consumir espaço nos nós existentes& n.o 8212; o procedimento de rebalanceamento EC não move dados replicados.
  - Os nós de maior capacidade ficarão relativamente menos cheios do que os nós de menor capacidade, mesmo que todos os nós acabem com aproximadamente a mesma quantidade de dados codificados por apagamento.

    Por exemplo, suponha que três nós de 200 TB estejam preenchidos a 80% (200 e 215; 0,8: 160 TB em cada nó ou 480 TB para o local). Se você adicionar um nó de 400 TB e executar o procedimento de rebalancear, todos os nós agora terão aproximadamente a mesma quantidade de dados de código de apagamento (480/4: 120 TB). No entanto, o usado (%) para o nó maior será menor do que o usado (%) para os nós menores.

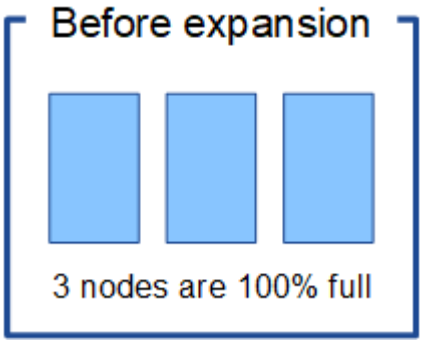


Quando rebalancear os dados codificados por apagamento

Considere o seguinte cenário:

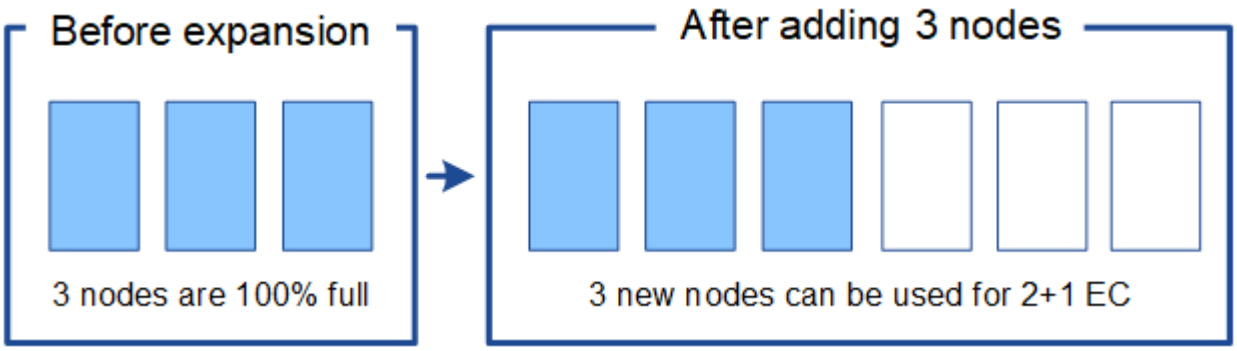
- O StorageGRID é executado em um único local, que contém três nós de storage.

- 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. O alerta **Low Object Storage** foi acionado no nível de gravidade principal.



O rebalancear não será necessário se você adicionar nós suficientes

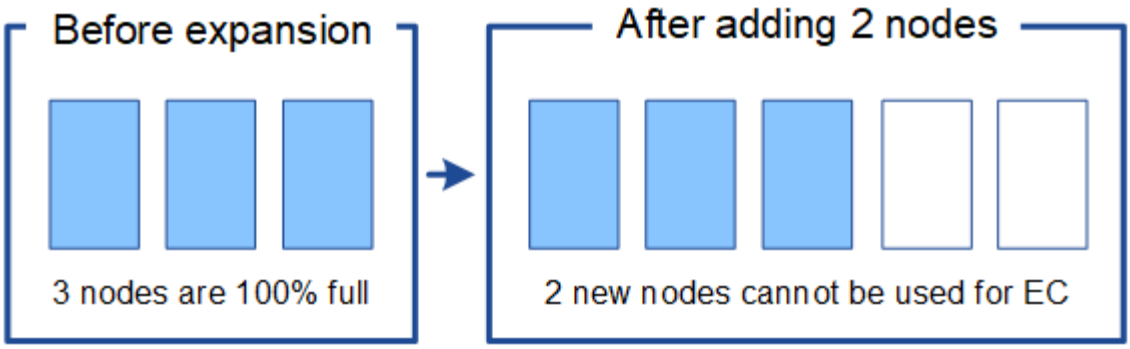
Para entender quando o rebalanceamento de EC não é necessário, suponha que você adicionou três (ou mais) novos nós de storage. Nesse caso, você não precisa executar o EC rebalanceamento. Os nós de storage originais permanecerão cheios, mas novos objetos agora usarão os três novos nós para 2 codificação de apagamento de mais de 1 e 8212; os dois fragmentos de dados e um fragmento de paridade podem ser armazenados em um nó diferente.



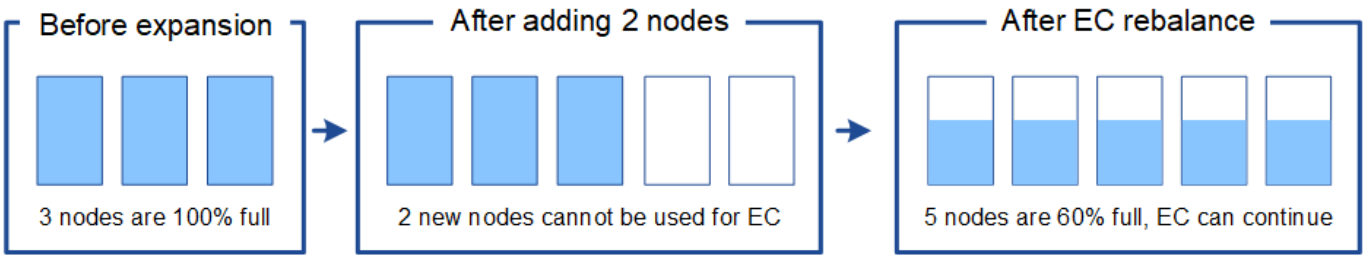
Embora você possa executar o procedimento de rebalanceamento EC nesse caso, mover os dados codificados de apagamento diminuirá temporariamente o desempenho da grade, o que pode afetar as operações do cliente.

O rebalanceamento é necessário se você não puder adicionar nós suficientes

Para entender quando o EC rebalanceamento é necessário, suponha que você só possa adicionar dois nós de storage, em vez de três. Como o esquema 2-1U requer pelo menos três nós de storage para ter espaço disponível, os nós vazios não podem ser usados para novos dados codificados por apagamento.



Para usar os novos nós de storage, execute o procedimento de rebalanceamento de EC. Quando esse procedimento é executado, o StorageGRID redistribui dados codificados por 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% em todos os nós de storage.



Recomendações para o reequilíbrio CE

O NetApp requer rebalanceamento EC se *all* das 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 nós de storage novos suficientes para o esquema de codificação de apagamento em uso. "Adicionar capacidade de storage para objetos codificados por apagamento"Consulte .
- Seus clientes S3 podem tolerar um desempenho inferior para suas operações de gravação e leitura enquanto o procedimento EC Rebalanceance está sendo executado.

Você pode, opcionalmente, executar o procedimento de rebalanceamento de EC se preferir que os nós de storage sejam preenchidos a níveis semelhantes. Além disso, seus clientes do S3 podem tolerar uma performance menor para as operações de gravação e leitura enquanto o procedimento de rebalanceamento de EC estiver em execução.

Como o procedimento EC Rebalanceance interage com outras tarefas de manutenção

Não é possível executar determinados procedimentos de manutenção ao mesmo tempo que executa 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 • 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, execute o procedimento de rebalanceamento do EC depois de adicionar todos os novos nós.
Procedimento de atualização	Não Se você precisar atualizar o software StorageGRID, execute o procedimento de atualização antes ou depois de executar o procedimento EC Rebalanceance. Conforme necessário, você pode encerrar o procedimento EC Rebalanceance para realizar uma atualização de software.
Procedimento de clone de nó do dispositivo	Não Se você precisar clonar um nó de storage de dispositivo, execute o procedimento de rebalanceamento de EC depois de adicionar o novo nó.
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 encerrar 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.
- Não é possível aumentar a capacidade dos metadados adicionando volumes de storage aos nós de storage existentes, porque os metadados são armazenados apenas no volume 0.
- Não é possível aumentar a capacidade dos metadados adicionando um novo site.
- 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.

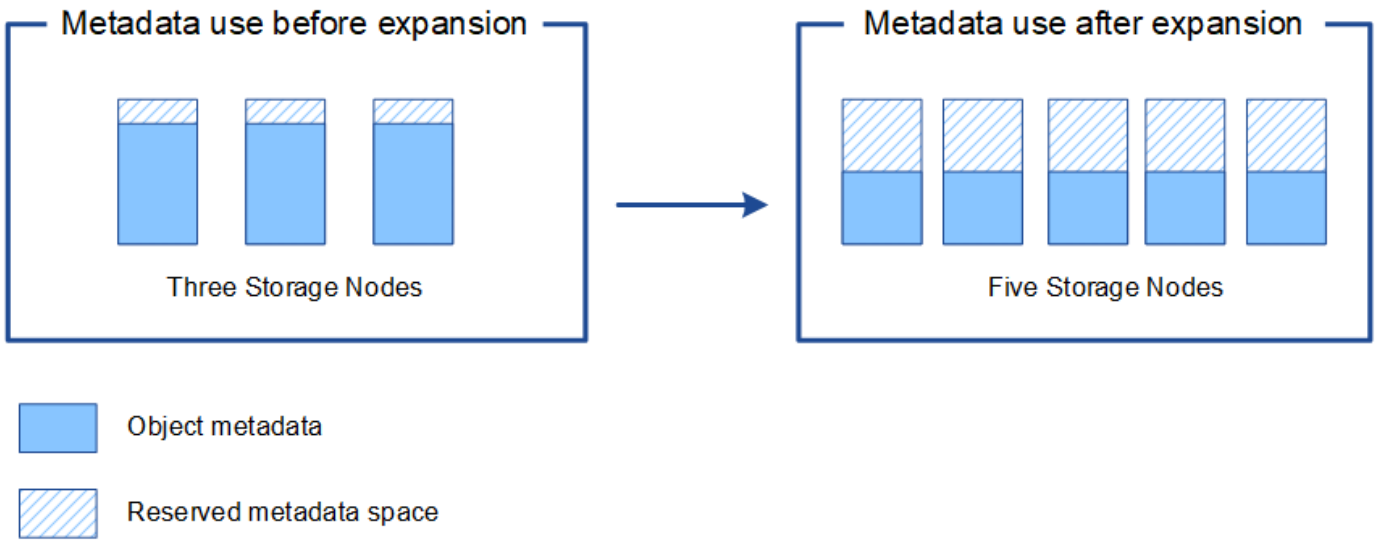
Consulte "Descrição do que é Metadata Reserved Space".

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 a serem usados em um grupo de alta disponibilidade (HA) ou 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

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 a opção **Definir novo nó padrão** for **não confiável** na guia redes de clientes não confiáveis na página de controle do Firewall, os aplicativos clientes que se conetarem a nós de expansão usando a rede de cliente devem se conetar usando uma porta de endpoint do balanceador de carga (**CONFIGURAÇÃO** > **Segurança** > **Controle do Firewall**). Consulte as instruções para "altere a configuração de segurança do novo nó" e para "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 "Exemplo para alterar uma política 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	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. Para obter detalhes, consulte as instruções para Transferir e extrair os ficheiros de instalação do StorageGRID. **Observação:** você não precisa baixar arquivos se estiver adicionando novos volumes de storage aos nós de storage existentes ou instalando um novo dispositivo StorageGRID.
Serviço de laptop	O computador portátil de serviço tem o seguinte: • Porta de rede • Cliente SSH (por exemplo, PuTTY) • "Navegador da Web suportado"
`Passwords.txt` ficheiro	Contém as senhas necessárias para acessar os nós de grade na linha de comando. 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 `Passwords.txt` arquivo.
Documentação do StorageGRID	• "Administrar o StorageGRID" • "Notas de lançamento" • Instruções de instalação para a sua plataforma ◦ "Instale o StorageGRID no Red Hat Enterprise Linux" ◦ "Instale o StorageGRID no Ubuntu ou Debian" ◦ "Instale o StorageGRID no VMware"
Documentação atual para a sua plataforma	Para versões suportadas, consulte "Ferramenta de Matriz de interoperabilidade (IMT)" .

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 "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 Utilizador final, selecione a caixa de verificação e, em seguida, selecione **Accept & continue**.
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	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu ou Debian ou appliances	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`
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 você estiver expandindo um sistema Red Hat Enterprise Linux, 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
	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.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL.
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 `configure-storagegrid.py` 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. Você também pode usar este script para integração Ping federate.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.
	Exemplo de função do Ansible e manual de estratégia para configurar hosts do RHEL para implantação de contêineres do StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.

Caminho e nome do arquivo	Descrição
	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.
	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 `/debs/storagegrid-webscale-images-version-SHA.deb`.
	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. Você também pode usar este script para integração Ping federate.
	Um exemplo de arquivo de configuração para uso com o `configure-storagegrid.py` script.

Caminho e nome do arquivo	Descrição
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` 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.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.
	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 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.

Caminho e nome do arquivo	Descrição
	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 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 `deploy-vsphere-ovftool.sh` 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 entrar na API de Gerenciamento de Grade quando o logon único (SSO) está ativado. Você também pode usar este script para integração Ping federate.
	Um exemplo de arquivo de configuração para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.

Caminho e nome do arquivo	Descrição
	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.
	MD5 checksum para o arquivo `/debs/storagegridwebscale-images-version-SHA.deb`.

> 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). Em particular, confirme se as seguintes portas TCP estão abertas entre os novos nós que você está adicionando na expansão e no nó Admin principal:
  - 1055
  - 7443
  - 8011
  - 10342

  "Comunicações internas do nó da grade"Consulte .
- 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.

Antes de começar

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 implantado"Consulte ou "Adicione o compartimento de expansão ao SG6160 implantado" para saber como adicionar volumes de armazenamento ao SG6060 ou SG6160 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 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 SANtricity os (o software de gerenciamento conetado 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.

Antes de começar

- Você tem acesso às instruções para instalar implantações do StorageGRID para VMware.
  - "Instale o StorageGRID no VMware"
- Você tem o `Passwords.txt` arquivo.
- Você "permissões de acesso específicas"tem .

> 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, mais de 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.

c. Digite **y** para aceitar a formatação.

d. Se algum dos volumes tiver sido formatado anteriormente, decida se deseja reformatá-los.

- Introduza **y** para reformatar.
- Digite **n** para ignorar a reformatação.

O `setup_rangedbs.sh` script é executado automaticamente.

5. 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.

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.

Antes de começar

- Você tem acesso às instruções para instalar o StorageGRID para sua plataforma Linux.
  - "Instale o StorageGRID no Red Hat Enterprise Linux"
  - "Instale o StorageGRID no Ubuntu ou Debian"
- Você tem o `Passwords.txt` arquivo.
- Você "permissões de acesso específicas"tem .

> 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 e atualize a configuração da controladora RAID conforme necessário, ou aloque os novos LUNs SAN nos storages de armazenamento compartilhados e permita que o host Linux as 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 lacuna.

   - 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.

b. Digite **y** para formatar os volumes de armazenamento.

c. Se algum dos volumes tiver sido formatado anteriormente, decida se deseja reformatá-los.

- Introduza **y** para reformatar.
- Digite **n** para ignorar a reformatação.

O `setup_rangedbs.sh` script é executado automaticamente.

14. Verifique se o estado de storage do nó de storage está online:

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**.

15. 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

Siga este procedimento para adicionar nós de grade a sites existentes ou para adicionar um novo site. Você só pode executar um tipo de expansão de cada vez.

Antes de começar

- Você tem o "Acesso root ou permissão de 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.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você 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**.
2. Selecione **Adicionar outra sub-rede** para adicionar uma nova sub-rede na notação CIDR.

   Por exemplo, introduza `10.96.104.0/22`.

3. Insira a senha de provisionamento e selecione **Salvar**.
4. Aguarde até que as alterações sejam aplicadas e, em seguida, faça o download de um novo pacote de recuperação.
   a. Selecione **MAINTENANCE** > **System** > **Recovery package**.
   b. Introduza a **frase-passe de aprovisionamento**.

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. Ele também é usado para recuperar o nó de administração principal.

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 uma 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 conete-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.

Antes de começar

- Você tem as instruções para instalar o StorageGRID para sua versão do Linux e analisou os requisitos de hardware e armazenamento.
  - "Instale o StorageGRID no Red Hat Enterprise Linux"
  - "Instale o StorageGRID no 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 conetar à rede de Grade, à rede Admin e à rede Cliente.

Antes de começar

- O dispositivo foi instalado em um rack ou gabinete, conetado às redes e ligado.
- Concluiu os "Configure o hardware" passos.

  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. 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 conetada.

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	a. Desmarque a caixa de seleção **Ativar descoberta de nó de administrador**. b. Introduza o endereço IP manualmente. c. Clique em **Salvar**. d. Aguarde até que o estado da ligação para que o novo endereço IP fique pronto.
Detecção automática de todos os nós de administração principal conetados	a. Marque a caixa de seleção **Enable Admin Node Discovery** (Ativar descoberta de nó de administrador). b. Aguarde até que a lista de endereços IP descobertos seja exibida. c. Selecione o nó de administração principal para a grade onde este nó de storage do dispositivo será implantado. d. Clique em **Salvar**. e. Aguarde até que o estado da ligação para que o novo endereço IP fique pronto.

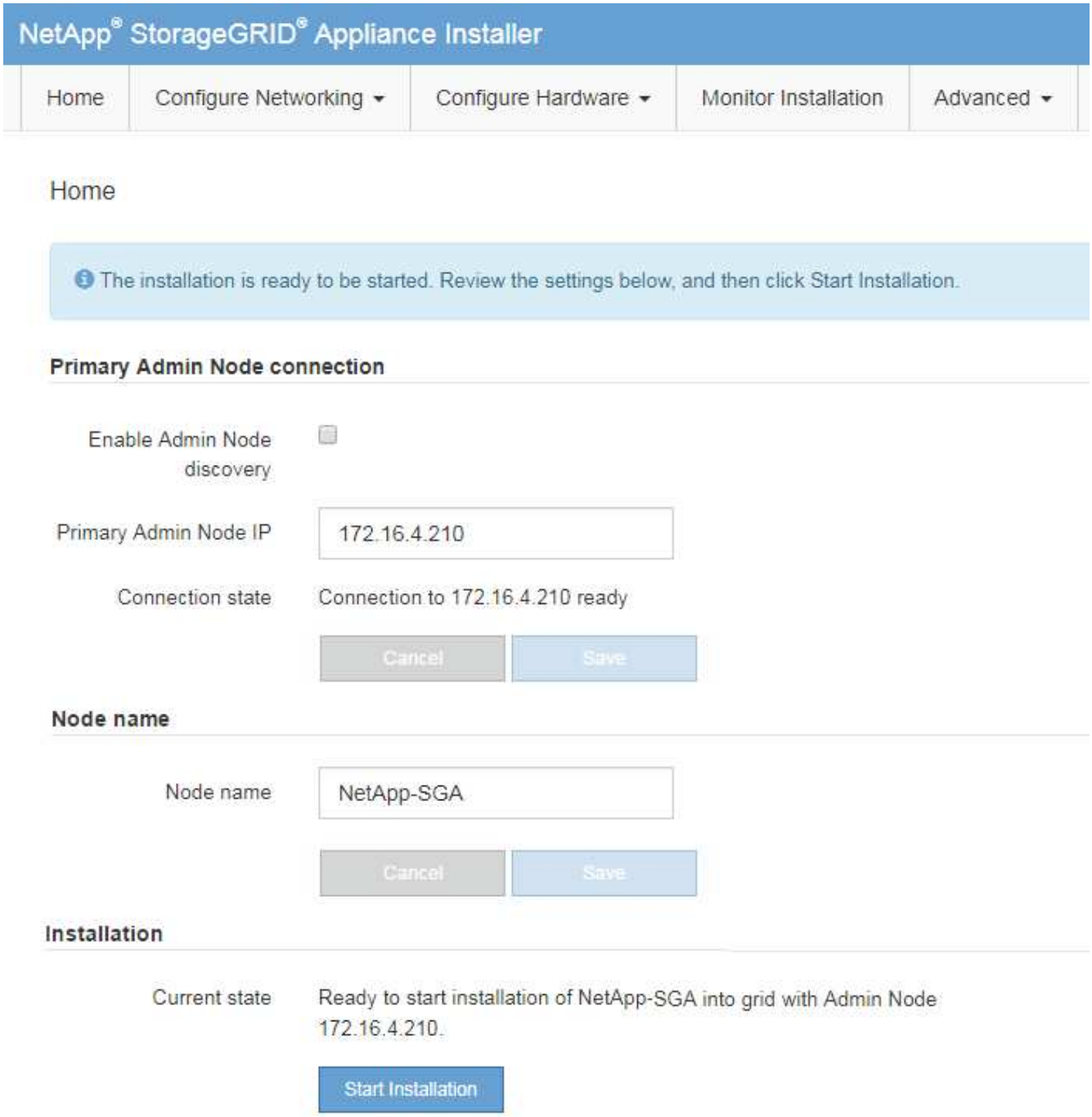
4. No campo **Nome do nó**, insira o nome que deseja usar para este nó de appliance e selecione **Salvar**.

   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.

5. 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 manutenção do seu aparelho.

6. Na página inicial do Instalador de dispositivos StorageGRID, selecione **Iniciar instalação**.



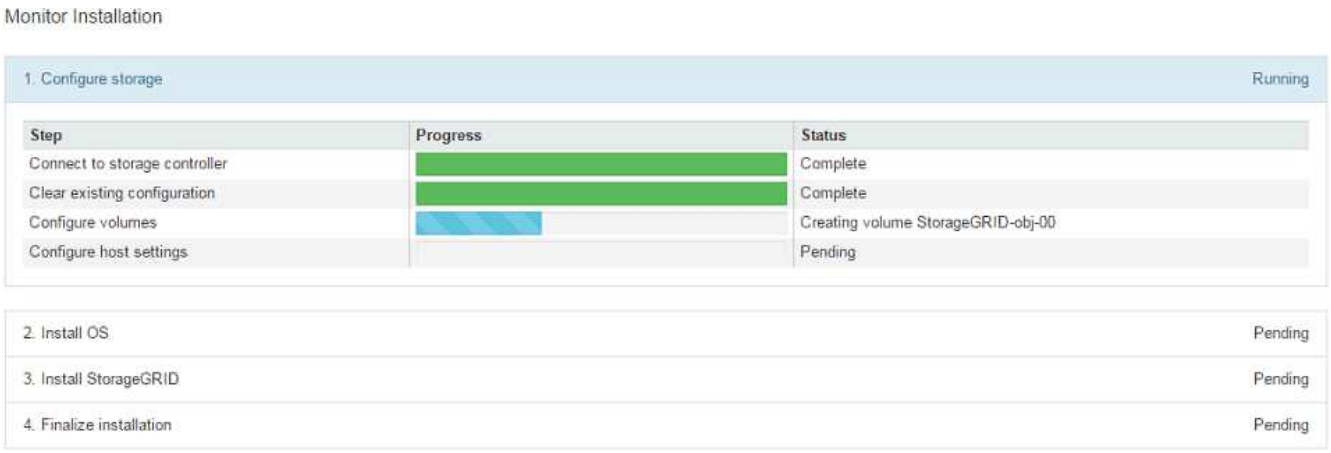
O estado atual muda para "a instalação está em andamento" e a página Instalação do monitor é exibida.

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.



   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 são mostradas com uma barra de status verde e um status de "ignorado".

9. Reveja o progresso das duas primeiras fases de instalação.

   1. Configure o appliance

   Durante esta fase, ocorre um dos seguintes processos:

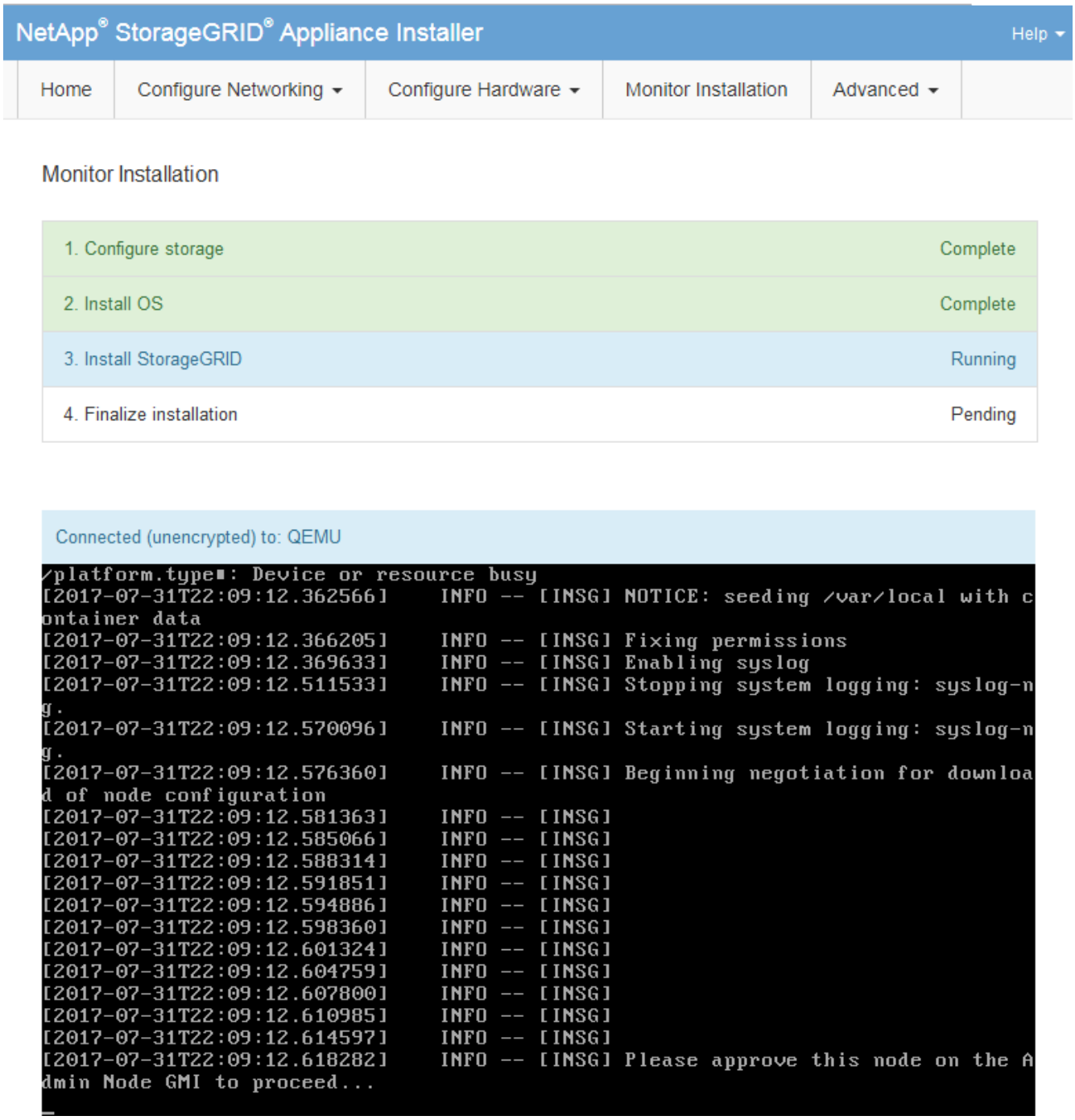
   - Para um dispositivo de armazenamento, o instalador se coneta ao controlador de armazenamento, limpa qualquer configuração existente, comunica com o SANtricity os para configurar volumes e configura as configurações do host.
   - Para um dispositivo de serviços, o instalador limpa qualquer configuração 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.



Execute a expansão

Quando você executa a expansão, os novos nós de grade são adicionados à implantação existente do StorageGRID.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a senha de provisionamento.
- Você implantou todos os nós de grade que estão sendo adicionados a essa expansão.
- Você tem o "Permissão de manutenção ou acesso root".

- 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 nós de storage e quiser atribuir um nível de storage personalizado a esses nós, você já "criou o grau de armazenamento personalizado"o tem . Você também tem a permissão de acesso root ou as permissões Manutenção e ILM.
- Se você estiver adicionando um novo site, você revisou e atualizou as regras do ILM. Você deve garantir que as cópias de objeto não sejam armazenadas no novo local até que a expansão seja concluída. Por exemplo, se uma regra usar o pool de armazenamento padrão (**todos os nós de armazenamento**), você deve "crie um novo pool de armazenamento" que contenha apenas os nós de armazenamento existentes e "Atualizar regras ILM"a política de ILM para usar esse novo pool de armazenamento. Caso contrário, os objetos serão copiados para o novo site assim que o primeiro nó nesse site se tornar ativo.

Sobre esta tarefa

A execução da expansão inclui estas principais tarefas do utilizador:

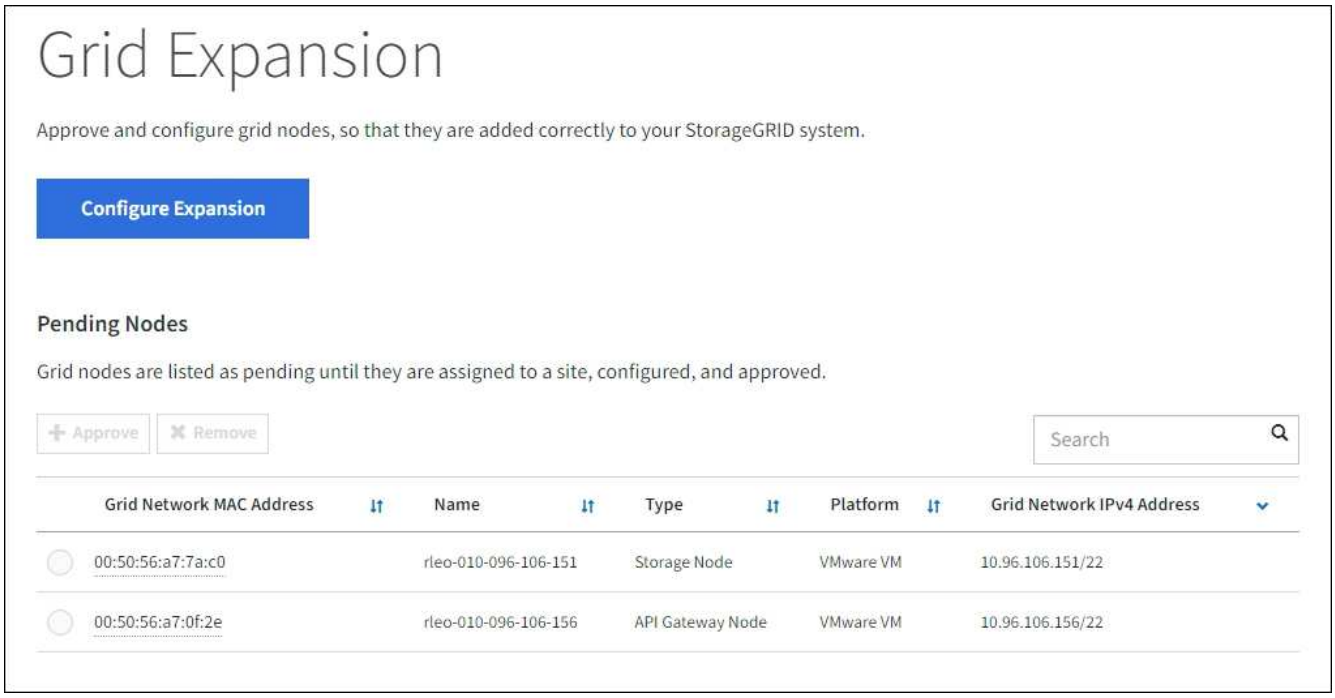
1. Configure a expansão.
2. Inicie a expansão.
3. Faça o download de um novo arquivo de pacote de recuperação.
4. Monitore as etapas e estágios de expansão até que todos os novos nós sejam instalados e configurados e todos os serviços tenham iniciado.

> Alguns passos e estágios de expansão 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 os nós que estão prontos para serem adicionados.

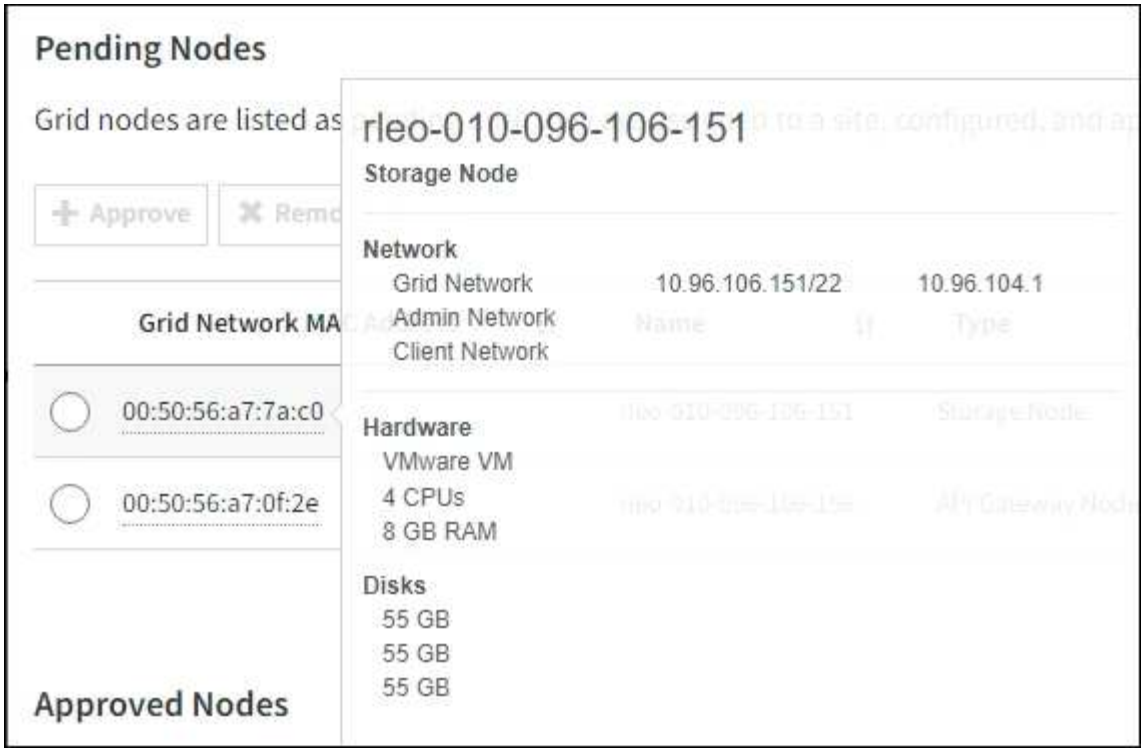


2. Selecione **Configurar expansão**.

   A caixa de diálogo seleção de local é exibida.

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 um ou mais nós 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 posicionar o cursor sobre o **Grid Network MAC Address** de um nó para ver detalhes sobre esse nó.



Se um nó estiver ausente, confirme que ele foi implantado com sucesso.

6. Na lista de nós pendentes, aprove os nós que você deseja adicionar nesta 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.

   c. Conforme necessário, modifique as definições gerais:

Campo	Descrição
Local	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 sistema para o nó. Os nomes de sistema são necessários para operações internas do StorageGRID e não podem ser alterados.
Tipo de storage (somente nós de storage)	• **Dados e metadados** ("combinados"): Nó de armazenamento de dados de objetos e metadados • **Somente dados**: Nó de armazenamento contendo apenas dados de objeto (sem metadados) • **Metadata-only**: Nó de armazenamento contendo apenas metadados (sem dados de objeto)

Campo	Descrição
Função NTP	A função NTP (Network Time Protocol) do nó de grade: • Selecione **Automático** (padrão) para atribuir automaticamente a função NTP ao nó. A função principal será atribuída a nós de administração, nós de storage com serviços ADC, nós de gateway e quaisquer nós de grade que tenham endereços IP não estáticos. A função Cliente será atribuída a todos os outros nós de grade. • Selecione **Primary** para atribuir manualmente a função NTP primária ao nó. Pelo menos dois nós em cada local devem ter a função principal de fornecer acesso redundante ao sistema a fontes de temporização externas. • Selecione **Client** para atribuir manualmente a função NTP do cliente ao nó.
Serviço ADC (nós de storage combinados ou somente metadados)	Se este nó de armazenamento irá executar 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. Não é possível adicionar o serviço ADC a um nó depois que ele é implantado. • Selecione **Sim** se o nó de armazenamento 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. • Selecione **Automático** para permitir que o sistema determine se esse nó requer o serviço ADC. Saiba mais sobre o "Quórum de ADC".
Grau de storage (nós de storage combinados ou somente de dados)	Use o grau de armazenamento **padrão** ou selecione o grau de armazenamento personalizado que você deseja atribuir a este novo nó. As classes de armazenamento são usadas por pools de armazenamento de ILM, portanto, sua seleção pode afetar quais objetos serão colocados no nó de armazenamento.

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

Se você descobrir que os nós têm endereços IP duplicados na rede de Grade enquanto você está aprovando nós, será necessário cancelar a expansão, reimplantar as máquinas ou dispositivos virtuais com um IP não duplicado e reiniciar a expansão.

- **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.

- 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 **Remover**.

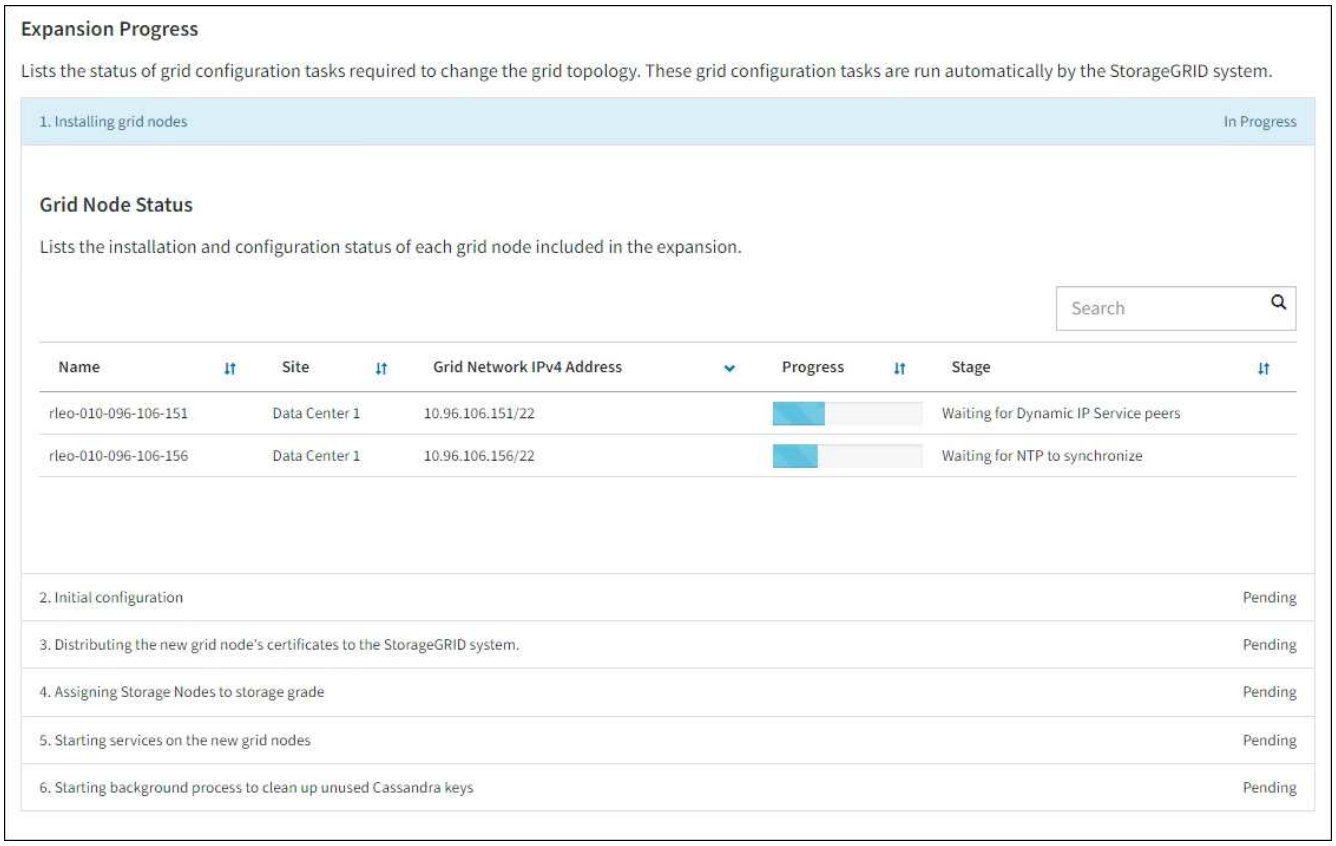
f. Repita estas etapas para cada nó de grade pendente que você deseja aprovar.

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 os nós de grade individuais estão em andamento, a seção Status do nó de grade lista o status atual de cada nó de grade.

Durante a etapa "Instalando nós de grade" para um novo dispositivo, o Instalador de dispositivos StorageGRID mostra a instalação passando do Estágio 3 para o Estágio 4, finalize a instalação. Quando a fase 4 é concluída, o controlador é reinicializado.



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 você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo.
   d. Copie o arquivo do pacote de recuperação baixado (`.zip`) para dois locais seguros, seguros e separados.

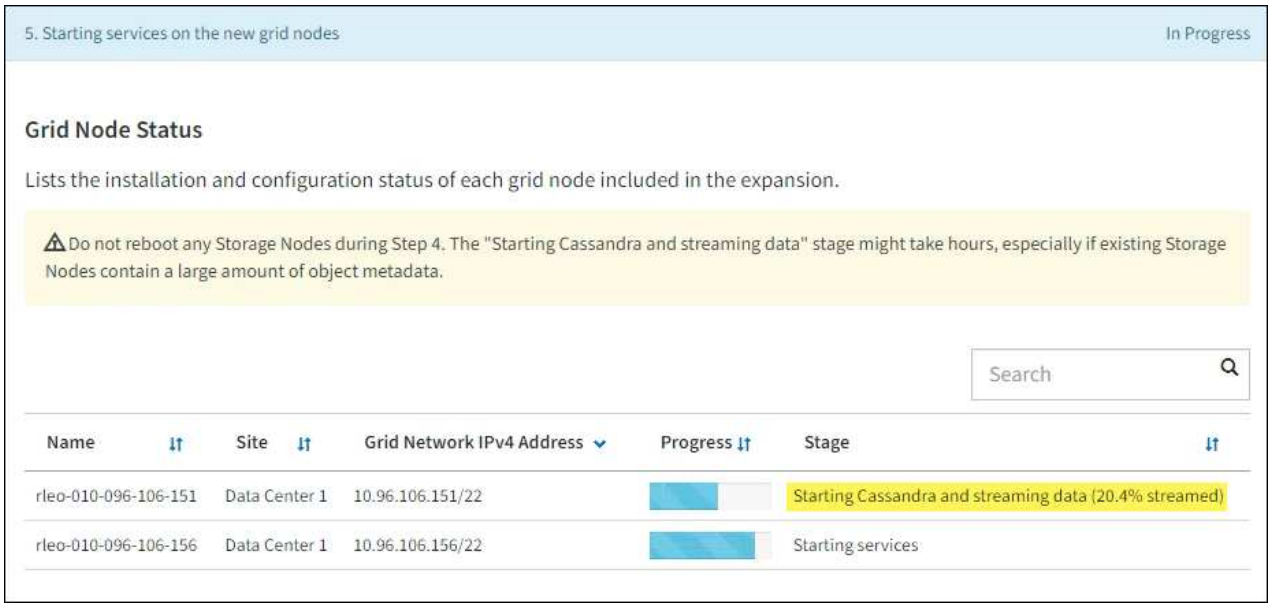
   O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

9. Se você estiver adicionando nós de storage a um site existente ou adicionando um site, monitore os estágios do Cassandra, que ocorrem quando os serviços são iniciados nos novos nós de grade.

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.

Adição de nós de storage

Se você estiver adicionando nós de storage a um site existente, revise a porcentagem mostrada na mensagem de status "iniciando Cassandra e transmissão de dados".



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.

Adicionar 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.

10. 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, execute 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 ou sites 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 e sites adicionados durante a expansão.

Passos

1. Se você adicionou um site:
   - "Crie um pool de armazenamento" Para o local e cada nível de storage selecionado para os novos nós de storage.
   - Confirme se a política ILM atende aos novos requisitos. Se forem necessárias alterações de regra"crie novas regras", e "Atualize a política ILM". Se as regras já estiverem corretas, "ative uma nova política"sem alterações de regra para garantir que o StorageGRID use os novos nós.
   - Confirme se os servidores NTP (Network Time Protocol) estão acessíveis a partir desse site. "Gerenciar 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.

2. Se você adicionou um ou mais nós de storage a um local existente:
   - "Veja os detalhes do pool de armazenamento" Para confirmar que cada nó adicionado está incluído nos pools de storage esperados e usado nas regras de ILM esperadas.
   - Confirme se a política ILM atende aos novos requisitos. Se forem necessárias alterações de regra"crie novas regras", e "Atualize a política ILM". Se as regras já estiverem corretas, "ative uma nova política"sem alterações de regra para garantir que o StorageGRID use os novos nós.
   - "Verifique se o nó de storage está ativo" e capaz de ingerir objetos.
   - Se você não conseguir adicionar o número recomendado de nós de storage, rebalanceamento dos dados codificados por apagamento. "Rebalancear os dados codificados por apagamento após adicionar nós de storage"Consulte .
3. Se você adicionou um nó de gateway:
   - 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. "Configurar grupos de alta disponibilidade"Consulte .
4. Se você adicionou um nó Admin:
   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. "Configurar grupos de alta disponibilidade"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 registos de auditoria"Consulte .

5. Para verificar se os nós de expansão foram adicionados com uma rede cliente não confiável ou para alterar se a rede cliente de um nó não é confiável ou confiável, vá para **CONFIGURATION** > **Security** > **Firewall control**.

   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. "Configurar pontos de extremidade do balanceador de carga"Consulte e "Gerenciar controles de firewall".

6. Configure o 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 .

Para garantir o funcionamento correto, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três serão usados por causa das limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, pode "Personalize a lista de servidores DNS"usar um conjunto diferente de até três servidores DNS para nós individuais (normalmente todos os nós em um site).

Se possível, use servidores DNS que cada site pode acessar localmente para garantir que um site islanded possa resolver os FQDNs para destinos externos.

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. Posicione 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 usado 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.

Antes de começar

- 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
- Dados de atributos históricos, que são usados em gráficos de estilo legado na página de nós

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 Admin*source*) 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.

Antes de começar

- 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 registos 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.

Antes de começar

- 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:
   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. Pare o serviço AMS para impedir que ele crie um novo arquivo: `service ams stop`
3. Navegue até o diretório de exportação de auditoria:

   ```
   cd /var/local/log
   ```

4. Renomeie o arquivo de origem `audit.log` para garantir que ele não substitua o arquivo no nó de administração de expansão para o qual você está copiando:

   ```
   ls -l
   mv audit.log _new_name_.txt
   ```

5. Copie todos os arquivos de log de auditoria para o local de destino no nó de administração de expansão:

   ```
   scp -p * IP_address:/var/local/log
   ```

6. 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.
7. Restaure o arquivo original `audit.log`:

   ```
   mv new_name.txt audit.log
   ```

8. Inicie o serviço AMS:

   ```
   service ams start
   ```

9. Terminar sessão a partir do servidor:

```
exit
```

10. Faça login no nó de administração de expansão:
    a. Introduza o seguinte comando: `ssh admin@expansion_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 `#`.

11. Atualize as configurações de usuário e grupo para os arquivos de log de auditoria:

```
cd /var/local/log

chown ams-user:bycast *
```

12. Terminar sessão a partir do servidor:

```
exit
```

Rebalancear os dados codificados por apagamento após adicionar nós de storage

Depois de adicionar nós de storage, use o procedimento de rebalancear a codificação de apagamento (EC) para redistribuir fragmentos codificados por apagamento entre os nós de storage atuais e novos.

Antes de começar

- Você concluiu as etapas de expansão para adicionar os novos nós de storage.
- Você revisou o "considerações para rebalanceamento de dados codificados por apagamento".
- 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.

O que acontece quando este procedimento é executado

Antes de iniciar o procedimento, tome nota do seguinte:

- O procedimento de reequilíbrio EC não será iniciado se um ou mais volumes estiverem offline (desmontados) ou se estiverem online (montados), mas em estado de erro.
- 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.
- Se um volume ficar offline enquanto o procedimento de reequilíbrio CE estiver em andamento, o procedimento de reequilíbrio será encerrado. Quaisquer fragmentos de dados que já foram movidos permanecerão em seus novos locais e nenhum dado será perdido.

Você pode executar novamente o procedimento depois que todos os volumes estiverem novamente online.

- Quando o procedimento de rebalanceamento EC estiver em execução, o desempenho das operações ILM e das operações do cliente S3 podem ser afetados.

> As operações de API S3D para fazer upload de 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 equilibrado ou rigoroso na ingestão. O seguinte erro será comunicado: `500 Internal Server Error`.

- Durante esse procedimento, todos os nós têm um limite de capacidade de storage de 80%. Os nós que excedem esse limite, mas ainda armazenam abaixo da partição de dados de destino, são excluídos de:
  - O valor de desequilíbrio do local
  - Quaisquer condições de conclusão do trabalho

> A partição de dados de destino é calculada dividindo o total de dados de um site pelo número de nós.

- **Condições de conclusão de trabalho**. O procedimento de reequilíbrio CE é considerado completo quando qualquer uma das seguintes situações for verdadeira:
  - Ele não pode mover mais dados codificados por apagamento.
  - Os dados em todos os nós estão dentro de um desvio de 5% da partição de dados de destino.
  - O procedimento está em execução há 30 dias.

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. Posicione 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. Inicie o procedimento:

'rebalance-data start --site "*site-name*"

Para "*site-name*", especifique o primeiro local onde você adicionou novo nó de storage ou nós. 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. monitore o status do procedimento de rebalanceamento EC.
   - 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`

6. Execute etapas adicionais, com base no status retornado:
   - Se `State` for `In progress`, a operação de reequilíbrio CE ainda está em execução. Você deve monitorar periodicamente o procedimento até que ele seja concluído.

     Use o `Site Imbalance` valor para avaliar o quão desequilibrado é o uso de dados de código de apagamento nos nós de storage no local. Esse valor pode variar de 1,0 a 0, com o 0 indicando que o uso de dados com codificação de apagamento é totalmente equilibrado em todos os nós de storage no local.

   O trabalho EC reequilíbrio é considerado concluído e será interrompido quando os dados em todos os nós estiverem dentro de um desvio de 5% da partição de dados de destino.

   - Se `State` for `Success`, opcionalmente revise o armazenamento de objetos para ver os detalhes atualizados do site.

     Agora, os dados codificados por apagamento devem ser mais equilibrados entre os nós de storage no local.

   - `State`Se for `Failure`:
     i. Confirme se todos os nós de storage no local estão conetados à grade.
     ii. Verifique e resolva quaisquer alertas que possam estar afetando esses nós de storage.
     iii. Reiniciar o procedimento EC Rebalanceance

     `rebalance-data start --job-id job-id`

     iv. Ver o estado do novo procedimento. Se `State` ainda estiver `Failure` , contacte o suporte técnico.

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 em seus novos locais. Os dados não são movidos de volta para o local original.

9. Se você estiver usando codificação de apagamento em mais de um site, execute este procedimento para todos os outros sites afetados.

Solucionar problemas de expansão

Se você encontrar erros durante o processo de expansão da grade que você não consegue resolver, ou se uma tarefa de grade falhar, colete os arquivos de log e entre em Contato com o suporte técnico.

Antes de contactar o suporte técnico, recolha os ficheiros de registo necessários para ajudar na resolução de problemas.

Passos

1. Conete-se ao nó de expansão que sofreu falhas:

   a. 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.

   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 efetuar login como root, o prompt 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	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`

Plataforma	Registos
Linux	• `/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)

Manter um sistema StorageGRID

Manutenção da grelha

As tarefas de manutenção de grade incluem a desativação de um nó ou site, renomeando uma grade, nó ou site e manutenção de redes. Você também pode executar procedimentos de host e middleware e procedimentos de nó de grade.

> Nestas instruções, "Linux" refere-se a uma implementação Red Hat Enterprise Linux, Ubuntu ou Debian. Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

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 "Instruções de manutenção para o seu aparelho StorageGRID" .

Baixar Recovery Package

O arquivo do pacote de recuperação permite restaurar o sistema StorageGRID se ocorrer uma falha.

Antes de começar

- No nó Admin principal, você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a senha de provisionamento.
- Você "permissões de acesso específicas"tem .

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, abra o `.zip` arquivo e confirme que você pode acessar o conteúdo,

incluindo 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.

Desativar nós ou local

Desativar o nó ou o local

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 "desativação do nó de grade" para remover um ou mais nós, que podem estar em um ou mais locais. Os nós removidos podem estar online e conetados ao sistema StorageGRID, ou podem estar offline e desconetados.
- Execute um "desativação do site" para remover um site. Você executa um **desativação do site conetado** se todos os nós estiverem conetados ao StorageGRID. Você executa um **desativação do site desconetada** se todos os nós estiverem desconetados do StorageGRID. Se o site contiver uma mistura de nós conetados e desconetados, você deverá colocar todos os nós off-line novamente.

> Antes de executar uma desativação desconetada do site, entre em Contato com o representante da sua 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.

Desativar nós

Desativação do nó de grade

Você pode usar o procedimento de desativação do nó para remover um ou mais nós de grade em um ou mais locais. Não é possível desativar o nó de administração principal.

Quando desativar um nó

Use o procedimento de desativação do nó quando qualquer uma das seguintes situações for verdadeira:

- Você adicionou um nó de storage maior em uma expansão e deseja remover um ou mais nós de storage menores, ao mesmo tempo em que preserva objetos.

> Se quiser substituir um aparelho mais antigo por um aparelho mais novo, considere "clonar o nó do dispositivo" em vez de adicionar um novo aparelho em uma expansão e, em seguida, desativar o aparelho antigo.

- 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 desconetado que você não pode recuperar ou trazer de volta on-line.
- Sua grade inclui um nó de arquivo.

Como desativar um nó

Você pode desativar os nós de grade conetados ou os nós de grade desconetados.

Desativar os nós conectados

Em geral, você deve desativar os nós de grade somente quando eles estiverem conetados ao sistema StorageGRID e somente quando todos os nós estiverem em estado normal (tenha ícones verdes nas páginas **NÓS** e na página **NÓS de desintegração**).

Para obter instruções, "Desativar os nós de grade conetados"consulte .

Desativar os nós desligados

Em alguns casos, talvez seja necessário desativar um nó de grade que não esteja conetado atualmente à grade (um cuja Saúde é desconhecida ou administrativamente inativo).

Para obter instruções, "Desativar nós de grade desconetados"consulte .

O que considerar antes de desativar um nó

Antes de executar qualquer procedimento, reveja as considerações para cada tipo de nó:

- "Considerações para desativação do nó de administrador ou gateway"
- "Considerações para desativação do nó de storage"

Considerações para a desativação de nós de administração ou de gateway

Reveja as considerações sobre a desativação de um nó de administrador ou de um nó de gateway.

Considerações para Admin Node

- Não é possível desativar o nó de administração principal.
- Não é possível desativar um nó Admin 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 "Gerenciamento de grupos de HA".
- Conforme necessário, você pode alterar com segurança as políticas de ILM ao desativar 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).
- Se utilizar "federação de grade"o , certifique-se de que o endereço IP do nó que está a ser desativado não foi especificado para uma ligação de federação de grelha.
- 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.

Considerações para o Gateway Node

- Não é possível desativar um Gateway Node 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 "Gerenciamento de grupos de HA".
- Conforme necessário, você pode alterar com segurança as políticas de ILM ao desativar um nó de gateway.
- Se utilizar "federação de grade"o , certifique-se de que o endereço IP do nó que está a ser desativado não foi especificado para uma ligação de federação de grelha.
- Você pode desativar um Gateway Node com segurança enquanto ele estiver desconetado.

Considerações para nós de storage

Considerações para a desativação de nós de storage

Antes de desativar um nó de storage, considere se você pode clonar o nó em vez disso. Em seguida, se você decidir desativar o nó, revise como o StorageGRID gerencia objetos e metadados durante o procedimento de desativação.

Quando clonar um nó em vez de desativá-lo

Se você quiser substituir um nó de armazenamento de dispositivo mais antigo por um dispositivo mais novo ou maior, considere clonar o nó do dispositivo em vez de adicionar um novo dispositivo em uma expansão e, em seguida, desativar o dispositivo antigo.

A clonagem do nó do dispositivo permite substituir facilmente um nó do dispositivo existente por um dispositivo compatível no mesmo local do StorageGRID. O processo de clonagem transfere todos os dados para o novo dispositivo, coloca o novo dispositivo em serviço e deixa o dispositivo antigo em um estado de pré-instalação.

Você pode clonar um nó de dispositivo se precisar:

- Substitua um aparelho que esteja chegando ao fim da vida útil.
- Atualize um nó existente 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.
- Melhorar a eficiência do storage, como por exemplo, alterando o modo RAID.

```
https://docs.netapp.com/us-en/storagegrid-appliances/commonhardware/how-appliance-node-cloning-works.html["Clonagem do nó do dispositivo"^]Consulte para obter detalhes.
```

Considerações para nós de storage conectados

Reveja as considerações sobre a desativação de um nó de armazenamento ligado.

- Você não deve desativar mais de 10 nós de storage em um único procedimento de nó de compactação.
- O sistema deve, em todos os momentos, incluir nós de storage suficientes para atender aos requisitos

operacionais, incluindo o "Quórum de ADC" e o "Política de ILM"ativo . 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.

Tenha cuidado ao desativar os nós de storage em uma grade que contém nós somente metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

- Quando você remove um nó de armazenamento, grandes volumes de dados de objetos são transferidos pela rede. Embora essas transferências não devam afetar as operações normais do sistema, elas podem afetar a 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 planeadas do sistema antes de remover nós de grade.
- Se você precisar executar outro procedimento de manutenção durante a remoção dos nós de storage, poderá "interrompa o procedimento de desativação"retomá-lo e retomá-lo após o outro procedimento ser concluído.

> 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.

- 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 em uma política de ILM enquanto um nó de storage estiver sendo desativado.
- Para remover dados de forma permanente e segura, você deve limpar as unidades do nó de armazenamento depois que o procedimento de desativação for concluído.

Considerações para nós de storage desconetados

Reveja as considerações sobre a desativação de um nó de storage desconetado.

- Nunca desative um nó desconetado, a menos que você tenha certeza de que ele não pode ser trazido 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.

- Quando você desativa um nó de storage desconetado, o StorageGRID usa dados de outros nós de storage para reconstruir os dados do objeto e os metadados que estavam no nó desconetado.
- A perda de dados pode ocorrer se você desativar mais de um nó de storage desconetado. 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. Ao desativar os nós de storage em uma grade com nós somente metadados baseados em software, a desativação de todos os nós configurados para armazenar objetos e metadados remove todo o storage de objetos da grade. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

> 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 reparo de dados podem levar dias ou semanas para serem executados e não são monitorados 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 conetados.

O que é o quórum ADC?

Talvez você não consiga desativar determinados nós de armazenamento em um local se poucos serviços do controlador de domínio administrativo (ADC) permanecessem após a desativação.

O serviço ADC, 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 não seja mais atendido. Para satisfazer o quórum de ADC durante a desativação, um mínimo de três nós de armazenamento em cada local deve ter o serviço ADC. Se um local tiver mais de três nós de storage com o serviço ADC, a maioria simples desses nós deve permanecer disponível após a desativação: `((0.5 * Storage Nodes with ADC) + 1)`

> Tenha cuidado ao desativar os nós de storage em uma grade que contém nós somente metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

Por exemplo, suponha que um site 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 storage 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, adicione um novo nó de armazenamento em um "expansão" e especifique que ele deve ter um serviço ADC. Em seguida, desative o nó de storage existente.

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 em cada uma "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? Como 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 atender às políticas ativas de ILM?

> ⓘ Uma política de ILM que não pode ser satisfeita levará a backlogs e alertas 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 as áreas listadas na tabela.

Área a avaliar	O que considerar
Capacidade disponível	Haverá capacidade de storage 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 storage para serem desativados? Haverá capacidade suficiente para lidar com o crescimento previsto nos 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 mover o conteúdo 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.

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 "Expanda o sistema StorageGRID"adiciona nós de storage de capacidade novos e maiores e, em seguida, desativa 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, considere "clonar o nó do dispositivo" (ou use a clonagem do nó do dispositivo e o procedimento de desativação se você 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.

Desativar vários nós de storage

Se você precisar remover mais de um nó de storage, poderá desativá-los sequencialmente ou em paralelo.

Tenha cuidado ao desativar os nós de storage em uma grade que contém nós somente metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

- 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 leitura", 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.

Sobre esta tarefa

Se você 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.

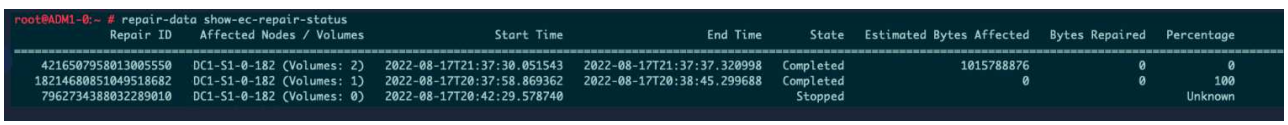
Essas etapas se aplicam somente a sistemas que tenham objetos codificados por apagamento.

Passos

1. Faça login no nó de administração principal:
   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. 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.



Opcionalmente, você pode usar o Gerenciador de Grade para monitorar os processos de restauração em andamento e exibir um histórico de restauração. "Restaure dados de objetos usando o Gerenciador de Grade"Consulte .

3. Se o Estado para todas as reparações for `Completed`, não é necessário reiniciar quaisquer trabalhos de reparação.
4. Se o estado de qualquer reparação for `Stopped`, 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 `Completed`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 `.zip`	Tem de "Baixe o mais recente pacote de recuperação" `.zip` (`sgws-recovery-package-*id-revision*.zip`arquivar). 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 aprovisionamento	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.
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.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

- Você tem o "Permissão de manutenção ou acesso root".

> Tenha cuidado ao desativar os nós de storage em uma grade que contém nós somente metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

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.

     Neste exemplo, a coluna Decmmission possible indica que você pode desativar o Gateway Node e um dos quatro nós de armazenamento.

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-	✓	No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-ARC1	Data Center 1	Archive Node	-	✓	No, you can't decommission an Archive Node unless the node is disconnected.
☐ 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.
☐ DC1-S4	Data Center 1	Storage Node	No	✓	✓

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 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 é mostrado.

Desativar possível motivo	Descrição	Passos para resolver
Não, *node type* desativação não é suportada.	Não é possível desativar o nó de administração principal.	Nenhum.

Desativar possível motivo	Descrição	Passos para resolver
Não, pelo menos um nó de grade está desconetado. **Nota:** esta mensagem é mostrada apenas para nós de grade conetados.	Não é possível desativar um nó de grade conetado se qualquer nó de grade estiver desconetado. A coluna **Saúde** inclui um destes ícones para nós de grade que estão desconetados: • (Cinza): Administrativamente para baixo • (Azul): Desconhecido	Você deve colocar todos os nós desconetados novamente on-line ou "desativar todos os nós desconetados" antes de poder remover um nó conetado. **Nota**: 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.
Não, um ou mais nós necessários estão atualmente desconetados e devem ser recuperados. **Nota:** esta mensagem é mostrada apenas para nós de grade desconetados.	Não é possível desativar um nó de grade desconetado se um ou mais nós necessários também estiverem desconetados (por exemplo, um nó de armazenamento necessário para o quórum de ADC).	a. Reveja as mensagens possíveis de desintegração para todos os nós desconetados. b. Determine quais nós não podem ser desativados porque eles são necessários. ◦ 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.
Não, membro do(s) grupo(s) HA: *Nome do grupo*. Antes de desativar esse nó, você deve removê-lo de todos os grupos de HA.	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).	Edite o grupo de HA para remover a interface do nó ou remover todo o grupo de HA. "Configurar grupos de alta disponibilidade"Consulte .
Não, o local *x* requer um mínimo de *n* nós de armazenamento com serviços ADC.	**Somente nós de storage.** Não é possível desativar um nó de storage se nós insuficientes permanecessem no local para suportar os requisitos de quórum de ADC.	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 de ADC".

Desativar possível motivo	Descrição	Passos para resolver
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.	**Somente nós de storage.** Não é possível desativar um nó de storage a menos que haja nós suficientes para os perfis de codificação de apagamento existentes. Por exemplo, se existir um perfil de codificação 4 de apagamento para codificação de apagamento a mais de 2, pelo menos 6 nós de storage devem permanecer.	Para cada perfil de codificação de apagamento afetado, execute uma das etapas a seguir, com base em como o perfil está sendo usado: • **Usado em políticas ILM ativas**: Execute uma expansão. Adicione nós de storage novos suficientes para permitir que a codificação de apagamento continue. Consulte as instruções para "expandindo sua grade". • **Usado em uma regra ILM, mas não em políticas ILM ativas**: Edite ou exclua a regra e, em seguida, desative o perfil de codificação de apagamento. • **Não usado em nenhuma regra ILM**: Desative o perfil de codificação de apagamento. **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. Saiba mais "desativar um perfil de codificação de apagamento"sobre .
Não, não é possível desativar um nó de arquivo a menos que o nó esteja desconetado.	Se um nó de arquivo ainda estiver conetado, você não poderá removê-lo.	**Nota**: O suporte para nós de arquivo foi removido. Se necessitar de desativar um nó de arquivo, consulte "Desativação do nó de grade (StorageGRID 11,8 doc site)"

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).

Antes de começar

- Compreende as considerações relativas à "Nós de administrador e gateway"desativação e as considerações relativas à desativação "Nós de storage".
- 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 tem a senha de provisionamento.

Sobre esta tarefa

Você pode identificar nós desconetados procurando o ícone desconhecido azul ou o ícone cinza administrativamente para baixo na coluna **Saúde**.

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.

  A perda de dados pode ocorrer se você desativar mais de um nó de storage desconetado de cada vez. "Considerações para nós de storage desconetados"Consulte .

  Tenha cuidado ao desativar os nós de storage em uma grade que contém nós somente metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

- Se um nó desconetado não puder ser removido (por exemplo, um nó de armazenamento que é necessário para o quórum de ADC), nenhum outro nó desconetado poderá ser removido.

Passos

1. A menos que você esteja desativando um nó de arquivo (que deve ser desconetado), tente colocar todos os nós de grade desconetados novamente on-line ou recuperá-los.

   "Procedimentos de recuperação do nó de grade"Consulte 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 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 aprovisionamento.

   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.

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.

6. Assim que o novo pacote de recuperação estiver disponível, clique no link ou selecione **MAINTENANCE** > **System** > **Recovery package** para acessar a página Recovery Package. 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 desconetado, uma mensagem de informações indicará que os trabalhos de reparo foram iniciados.

8. 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.

9. 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 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
  ```

- Para determinar se as reparações estão concluídas:
  a. Selecione **NODES** > ***Storage Node a ser reparado*** > **ILM**.
  b. Reveja os atributos na secção 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.

Dados codificados por 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. Para obter instruções, "Monitore a criptografia do nó no modo de manutenção" consulte .

Desativar os nós de grade conetados

Você pode desativar e remover permanentemente nós que estão conetados à grade.

Antes de começar

- Compreende as considerações relativas à "Nós de administrador e gateway"desativação e as considerações relativas à desativação "Nós de storage".
- Você reuniu todos os materiais necessários.
- Você garantiu que nenhum trabalho de reparo de dados está ativo.
- Você confirmou que a recuperação do nó de storage não está em andamento em nenhum lugar da grade. Se estiver, aguarde 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.
- Você tem a senha de provisionamento.
- Os nós de grade estão conetados.
- A coluna **Decommission possible** para o nó ou nós que você deseja desativar inclui uma marca de seleção verde.

> A desativação não será iniciada se um ou mais volumes estiverem offline (desmontados) ou se estiverem online (montados), mas em estado de erro.

> Se um ou mais volumes ficarem offline enquanto uma desativação estiver em andamento, o processo de desativação será concluído depois que esses volumes voltarem a estar online.

- Todos os nós da grade têm 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 desconetado, 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.

> Tenha cuidado ao desativar os nós de storage em uma grade que contém nós somente metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Consulte "Tipos de nós de storage" para obter mais informações sobre nós de storage somente de metadados.

Sobre esta tarefa

Quando um nó é desativado, seus serviços são desativados e o nó é desligado automaticamente.

Passos

1. Na página Decommission Nodes, marque a caixa de seleção para cada nó de grade que você deseja

desativar.

2. Introduza a frase-passe de aprovisionamento.

   O botão **Start Decommission** está ativado.

3. Selecione **Start Decommission**.
4. Reveja a lista de nós na caixa de diálogo de confirmação e selecione **OK**.

   O procedimento de desativação do nó é iniciado e o progresso é exibido para cada nó.

   > 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, selecione o link Pacote de recuperação no banner ou selecione **MANUTENÇÃO** > **sistema** > **Pacote de recuperação** para acessar a página Pacote de recuperação. Em seguida, baixe o `.zip` arquivo.

   "Transferir o pacote de recuperação"Consulte .

   > 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.

Depois de terminar

Siga estas etapas depois de concluir o procedimento de desativação do nó:

1. 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. "Instale o StorageGRID no Red Hat Enterprise Linux"Consulte e "Instale o StorageGRID no Ubuntu ou Debian".
   - **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.
2. 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.
3. 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. Para obter instruções, "Monitore a criptografia do nó no modo de manutenção" consulte .

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.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".

Passos

1. Selecione **MAINTENANCE** > **Tasks** > **Decommission**.

   A página Decommission é exibida.

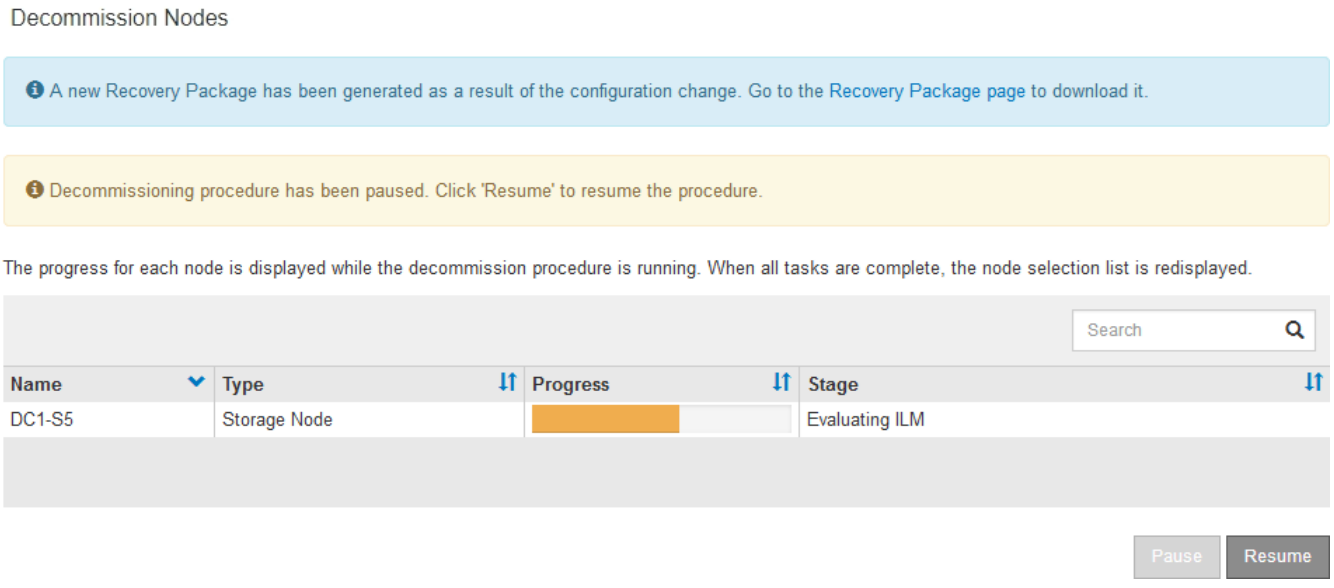
2. Selecione **Decommission Nodes**.

   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 por apagamento

3. Selecione **Pausa** para suspender o procedimento.

   O estágio atual é pausado e o botão **Resume** está ativado.



4. Depois que o outro procedimento de manutenção estiver concluído, selecione **Resume** para prosseguir com a desativação.

Site de desativação

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 referem 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 conetado e do local desconetado

Você pode usar o procedimento de desativação do site para remover um site no qual todos os nós estão conetados ao StorageGRID (chamado de desativação do site conetado) 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 conetados ( ) e desconetados (ou), você deverá colocar todos os nós offline novamente online.

- Uma desativação do site conetado permite remover um site operacional do sistema StorageGRID. Por exemplo, você pode executar uma desativação do site conetado para remover um site funcional, mas não mais necessário.
- Quando o StorageGRID remove um site conetado, 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 conetado ou desconetado

Antes de remover um local conetado ou desconetado, você deve estar ciente dos seguintes requisitos:

- Não é possível desativar um site que inclua o nó Admin principal.
- Não é possível desativar um site se algum dos nós tiver uma interface que pertence 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 site se ele contiver uma mistura de nós conetados ( ) e desconetados (ou).
- Não é possível desativar um site se qualquer nó em qualquer outro local estiver desconetado (ou).
- Não é possível iniciar o procedimento de desativação do local se uma operação de reparo ec-node estiver em andamento. "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:
  - Não é possível 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 conetado, 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 todos os confianças de partes confiáveis para o site dos Serviços de Federação do ative 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 por nenhuma política ILM. Se estiver, você deve editar as políticas ou criar e ativar políticas com novas regras ILM.
- Nenhuma regra ILM se refere ao site, mesmo que essas regras não sejam usadas em nenhuma política. 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 referem ao site e excluirá automaticamente todos os pools de armazenamento não utilizados que se referem ao site. Se o pool de storage de todos os nós de storage existir (StorageGRID 11,6 e anterior), ele será removido porque usará 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 ILM e a simulação e ativação de uma política ILM. "Gerenciar objetos com ILM"Consulte .

Considerações para os dados do objeto em um local conetado

Se você estiver executando uma desativação do site conetado, 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 políticas de ILM, você deve revisar a capacidade em ambos os locais. 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 "expanda uma grade"adicionar volumes de storage ou nós de storage a um local existente ou adicionar um novo local antes de executar este procedimento.

- 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 conetado

Antes que o StorageGRID possa remover um site conetado, 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 conetados.

- 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 "expanda uma grade"adicionar um nó novo equivalente em outro local. Certifique-se de que os clientes podem se conetar 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 conetarem a um grupo de HA que inclua nós do site, você deverá garantir que eles possam continuar se conetando ao StorageGRID após a remoção do site.
- Se os clientes se conetarem diretamente aos nós de storage no local que você está planejando remover, você deverá garantir que eles possam se conetar 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 em qualquer política de ILM ativa. Em alguns casos, talvez seja necessário "expanda uma grade"adicionar nós de storage, volumes de storage ou novos locais 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 (selecionando **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. "Como o suporte técnico recupera um site"Consulte .

- Todos os nós no local devem ter um estado de conexão de um dos seguintes:
  - **Desconhecido** ( ): Por um motivo desconhecido, um nó é desconetado ou os serviços no nó estão inalterados inesperadamente. Por exemplo, um serviço no nó pode ser interrompido ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada.
  - **Administrativamente para baixo** ( ): O nó não está conetado à grade por um motivo esperado. Por exemplo, o nó ou os serviços no nó foram desligados graciosamente.
- 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 sobre consistência quando você remove um site

A consistência de um bucket do S3 determina se o StorageGRID replica totalmente os metadados de objetos a todos os nós e sites antes de informar ao cliente que a ingestão de objetos foi bem-sucedida. A consistência fornece 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 a consistência de cada balde ou recipiente. 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.

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. "Faça o download do pacote de recuperação"
`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.

Item	Notas
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 `Passwords.txt` 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"

Passo 1: Selecione Site

Para determinar se um site pode ser desativado, comece acessando o assistente Decommission Site.

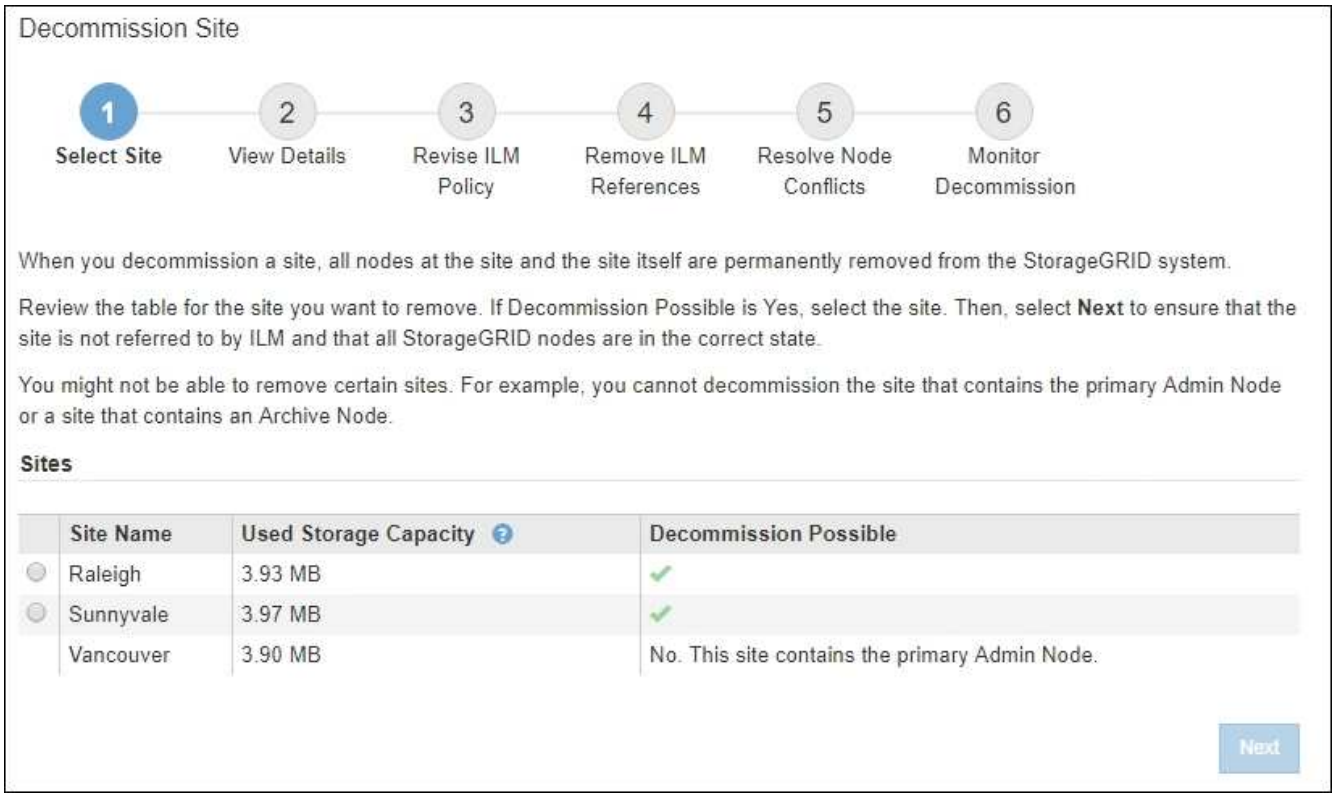
Antes de começar

- Você obteve todos os materiais necessários.
- Você revisou as considerações para remover um site.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "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.



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 conetado, 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 desconetado, 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 contenha 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 de Vancouver porque ele contém o nó de administração 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.

Antes de começar

Antes de desativar um site, você deve rever a quantidade de dados de objeto existentes no site.

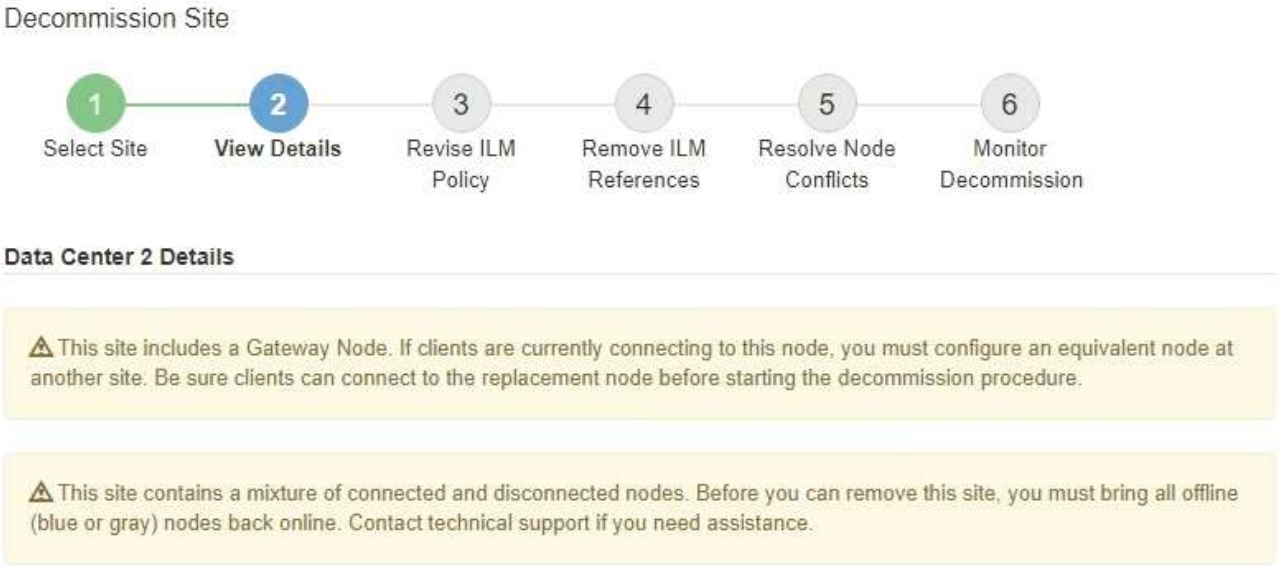
- Se você estiver executando uma desativação de um site conetado, você deve entender a quantidade de dados de objeto atualmente existentes no site antes de atualizar o ILM. Com base nas capacidades do site e nas necessidades de proteção de dados, você pode criar novas regras de ILM para mover dados para 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. "Ativar a proteção contra perda de local"Consulte .

Passos

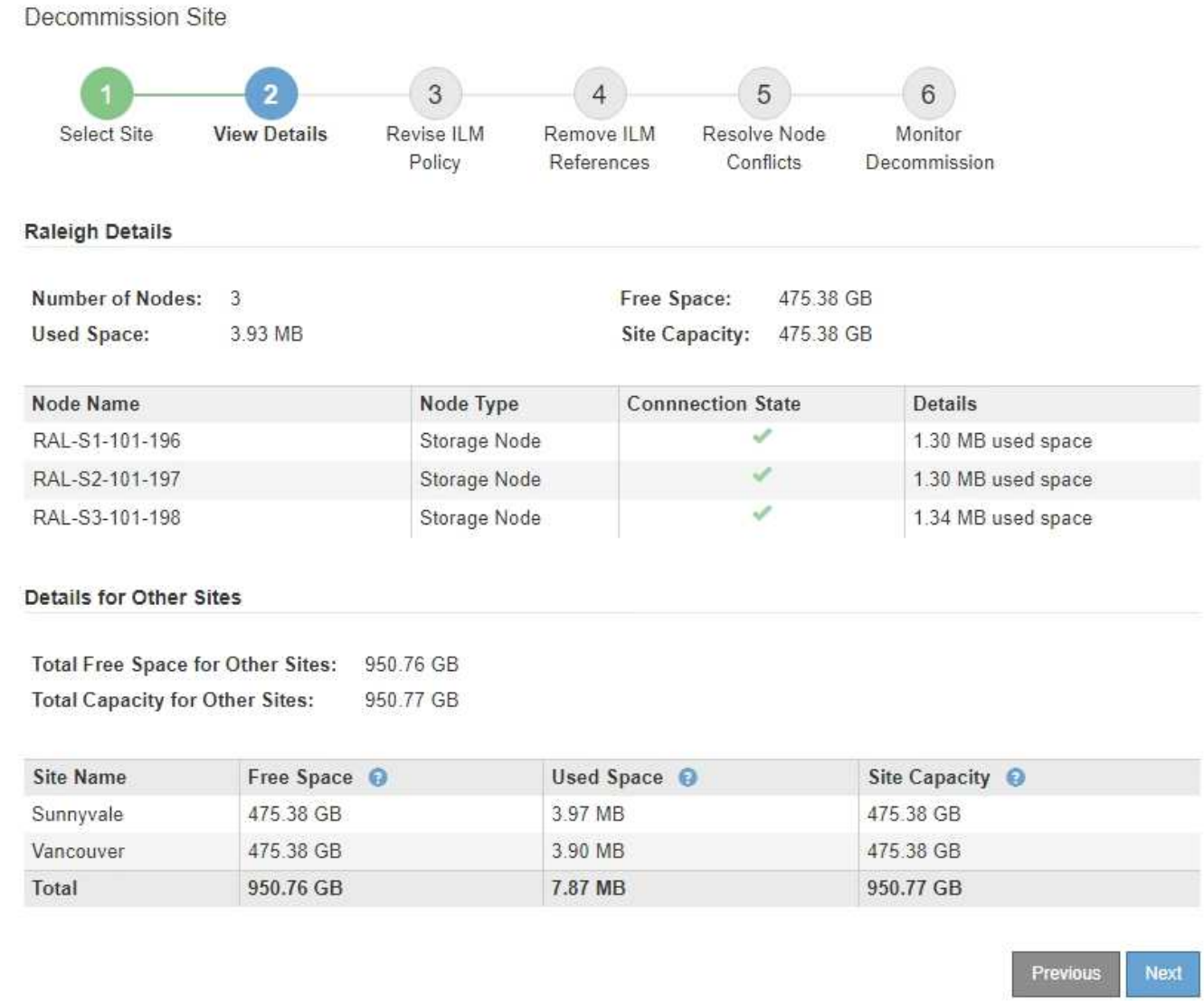
1. No passo 2 (Ver detalhes), reveja quaisquer avisos relacionados com o site que selecionou para remover.



   Nestes casos, aparece um aviso:

   - O site inclui um Gateway Node. Se os clientes S3 estiverem se conetando a esse nó, você deverá configurar um nó equivalente em outro site. Certifique-se de que os clientes podem se conetar ao nó de substituição antes de continuar com o procedimento de desativação.
   - O local contém uma mistura de nós conetados ( ) e desconetados (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.



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 conetado, 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 desconetada, 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, edite grupos de HA para remover todos os nós do local ou remova o grupo de HA se ele incluir somente nós deste local. Para obter instruções, "Gerenciar grupos de alta disponibilidade (HA)"consulte .

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 conetado 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.

Passo 3: Revise as políticas do ILM

A partir do passo 3 (rever as políticas ILM) do assistente do site Decommission, você pode determinar se o site é referido por qualquer política ILM.

Antes de começar

Você tem uma boa compreensão de como "Gerenciar objetos com ILM". Você está familiarizado com a criação de pools de armazenamento e regras ILM e com a simulação e ativação de uma política ILM.

Sobre esta tarefa

O StorageGRID não pode desativar um site se qualquer regra de ILM em qualquer política (ativa ou inativa) fizer referência a esse site.

Se qualquer política de ILM se refere ao site que você deseja desativar, você deve remover essas políticas ou editá-las para que elas atendam a esses requisitos:

- Proteger totalmente todos os dados de objetos.

- Não se refira ao site que você está em desativação.
- Não use pools de armazenamento que se referem ao site ou use a opção todos os sites.
- Não use perfis de codificação de apagamento que se referem ao site.
- Não use a regra fazer cópias 2 do StorageGRID 11,6 ou instalações anteriores.

> 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 deseja remover. Dependendo dos requisitos de proteção de dados, novas regras podem mover dados de objetos existentes para diferentes locais ou excluir quaisquer cópias extras de objetos que não sejam mais necessárias.

Entre em Contato com o suporte técnico se precisar de assistência para projetar uma nova política.

Passos

1. Na Etapa 3 (revisar políticas ILM), determine se alguma política ILM se refere ao site que você selecionou para desativar.
2. Se nenhuma política estiver listada, selecione **Avançar** para ir para "Passo 4: Remover referências ILM".
3. Se uma ou mais políticas *active* ILM estiverem listadas, clonar cada política existente ou criar novas políticas que não façam referência ao site que está sendo desativado:

   a. Selecione o link para a política na coluna Nome da política.

      A página de detalhes da política ILM para a política é exibida em uma nova guia do navegador. A página Decommission Site permanecerá aberta na outra guia.

   b. Siga estas diretrizes e instruções conforme necessário:

      - Trabalhar com regras ILM:
        - "Crie um ou mais pools de armazenamento" isso não se refere ao site.
        - "Editar ou substituir regras" que se referem ao site.

          > Não selecione a regra **Make 2 Copies** porque essa regra usa o pool de armazenamento **All Storage Nodes**, que não é permitido.

      - Trabalhar com políticas ILM:
        - "Clonar uma política de ILM existente" ou "Crie uma nova política ILM".
        - Certifique-se de que a regra padrão e outras regras não se referem ao site.

          > 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.

c. Ingira objetos de teste e simule a política para garantir que as regras corretas sejam aplicadas.

> Erros em uma política ILM podem causar perda de dados irrecuperável. 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.

d. Ative as novas políticas e certifique-se de que as políticas antigas estejam agora inativas.

Se pretender ativar várias políticas, "Siga as etapas para criar tags de política ILM".

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).

4. Para cada política *inativa*, edite-a ou remova-a selecionando primeiro o link para cada política, conforme descrito nas etapas anteriores.
   - "Edite a política" portanto, não se refere ao site para ser desativado.
   - "Remover uma política".
5. Quando você terminar de fazer alterações nas regras e políticas do ILM, não deve haver mais políticas listadas na Etapa 3 (revisar políticas do ILM). Selecione **seguinte**.

   O passo 4 (Remover referências ILM) é exibido.

Passo 4: Remover referências ILM

No passo 4 (Remover referências ILM) do assistente Decommission Site, você deve excluir ou editar quaisquer regras ILM não utilizadas que se referem ao site, mesmo que as regras não sejam usadas em nenhuma política ILM.

Passos

1. Determine se quaisquer regras de ILM não utilizadas se referem ao site.

   Se alguma regra ILM estiver listada, essas regras ainda se referem ao site, mas não são usadas em nenhuma política.

Quando o StorageGRID descompacta o site, ele desativará automaticamente quaisquer perfis de codificação de apagamento não utilizados que se referem ao site e excluirá automaticamente todos os pools de armazenamento não utilizados que se referem ao site. O pool de storage de todos os nós de storage (StorageGRID 11,6 e anterior) é removido porque ele usa o site todos os sites.

2. Edite ou exclua cada regra não utilizada:
   - Para editar uma regra, acesse a página de 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 excluir uma regra, selecione o ícone de lixeira e selecione **OK**.

     Você deve excluir a regra **Make 2 Copies** antes de poder desativar um site.

3. Confirme se nenhuma regra ILM não utilizada se refere ao site e o botão **Next** está ativado.
4. 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 referem ao site e excluirá automaticamente todos os pools de armazenamento não utilizados que se referem ao site. O pool de storage de todos os nós de storage (StorageGRID 11,6 e anterior) 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 desconetado 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.

Antes de começar

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 conetados ( ).

  Se você estiver executando uma desativação do local desconetado, todos os nós do local que você está removendo devem ser desconetados e todos os nós de todos os outros locais devem estar conetados.

  A desativação não será iniciada se um ou mais volumes estiverem offline (desmontados) ou se estiverem online (montados), mas em estado de erro.

  Se um ou mais volumes ficarem offline enquanto uma desativação estiver em andamento, o processo de desativação será concluído depois que esses volumes voltarem a estar online.

- Nenhum nó no local que você está removendo pode ter uma interface que pertence a um grupo de alta disponibilidade (HA).

Sobre esta tarefa

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.

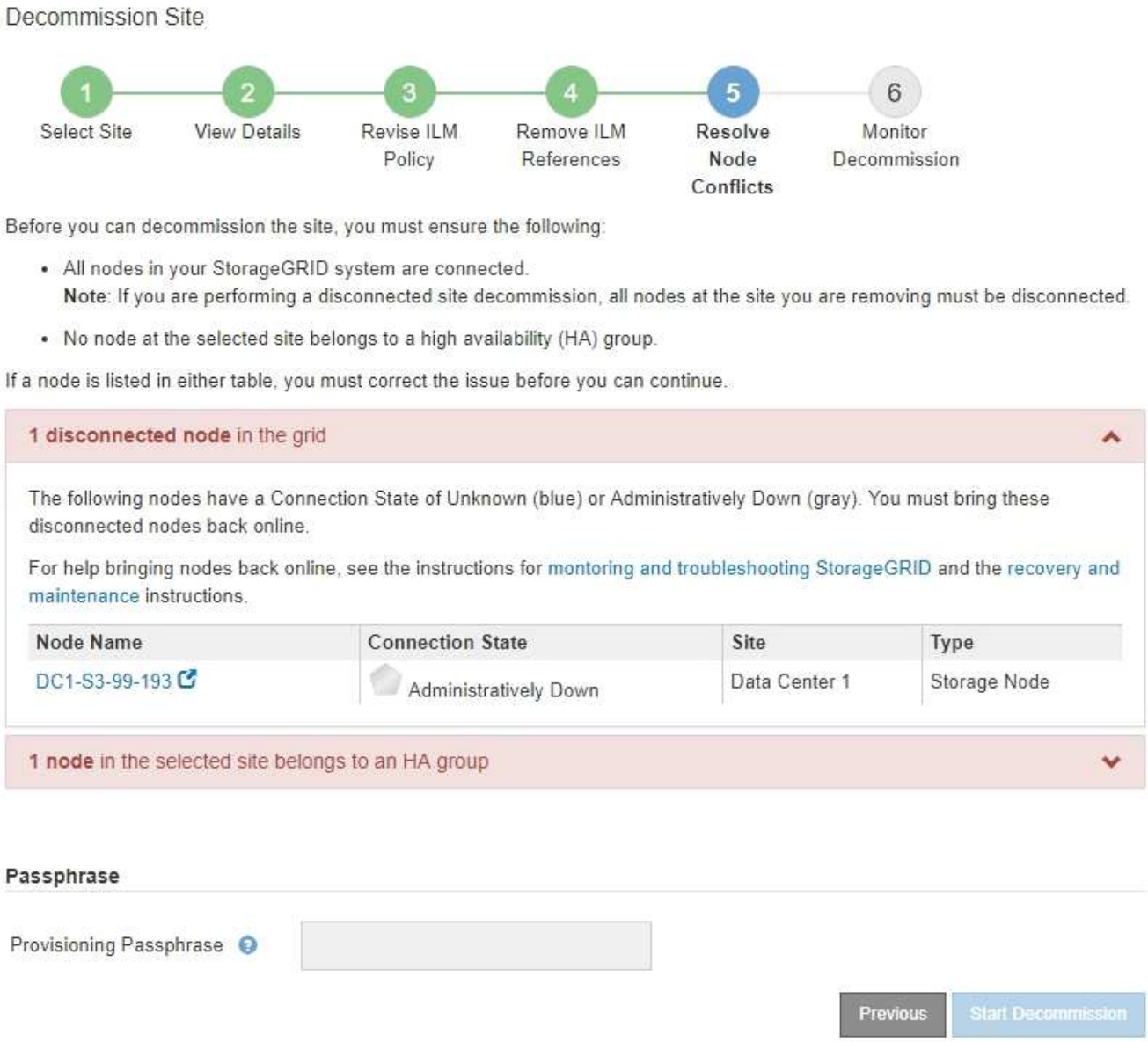
- Enquanto o procedimento de desativação do site está em execução:
  - Não é possível criar regras ILM que se referem ao site que está sendo desativado. Você também não pode editar uma regra ILM existente para se referir ao site.
  - Não é possível executar outros procedimentos de manutenção, como expansão ou atualização.

> Se você precisar executar outro procedimento de manutenção durante a desativação de um site conetado, poderá pausar o procedimento enquanto os nós de storage estiverem sendo removidos. O botão **Pausa** é ativado durante o estágio "Descomissionamento replicados e dados codificados por apagamento".

  - 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 desconetados da Etapa 5 (resolver conflitos de nó) para determinar se algum nó no sistema StorageGRID tem um estado de conexão desconhecido ( ) ou administrativamente inativo ( ).

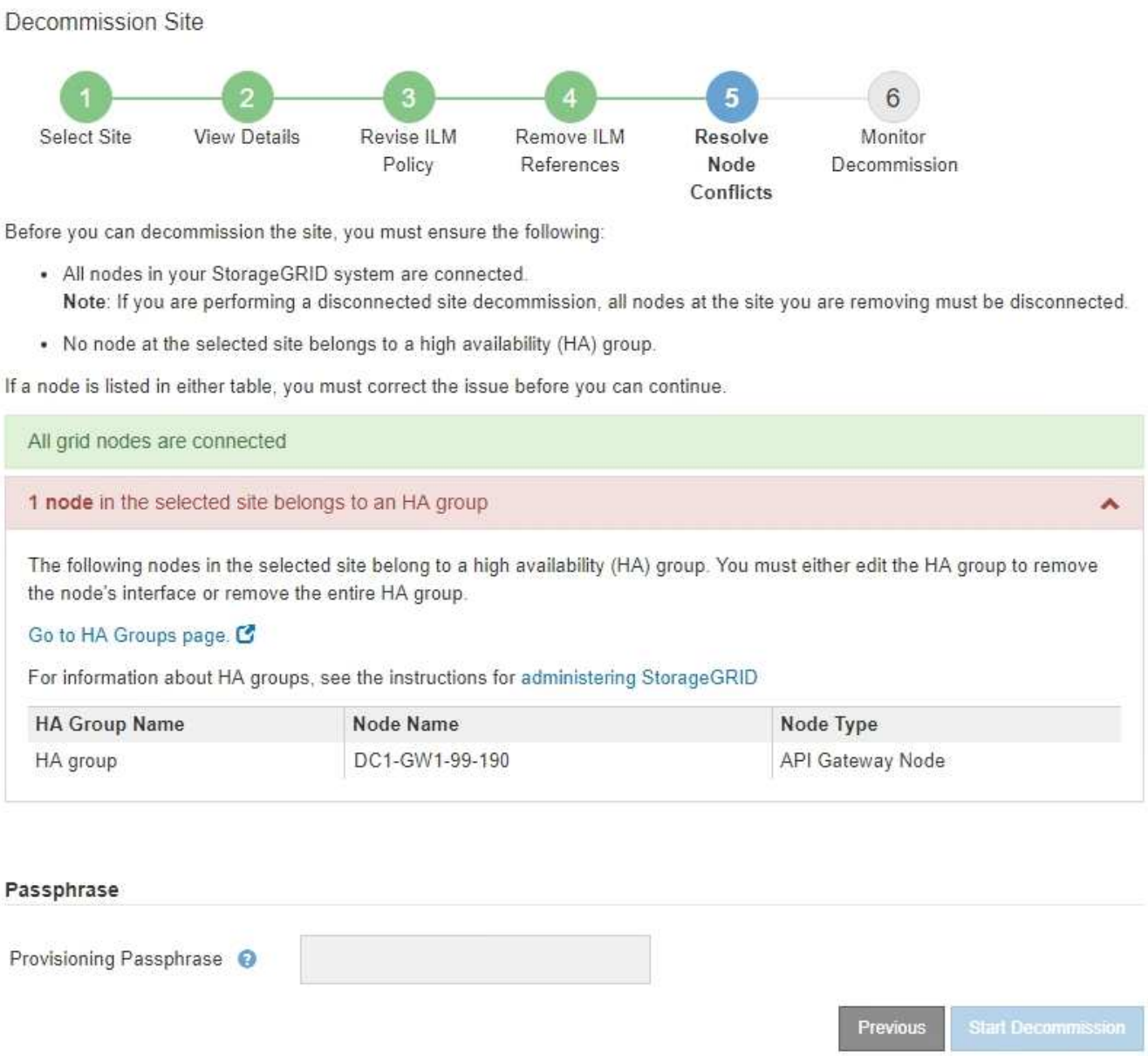


2. Se algum nó estiver desconetado, coloque-o novamente on-line.

   Consulte "Procedimentos do nó". 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).

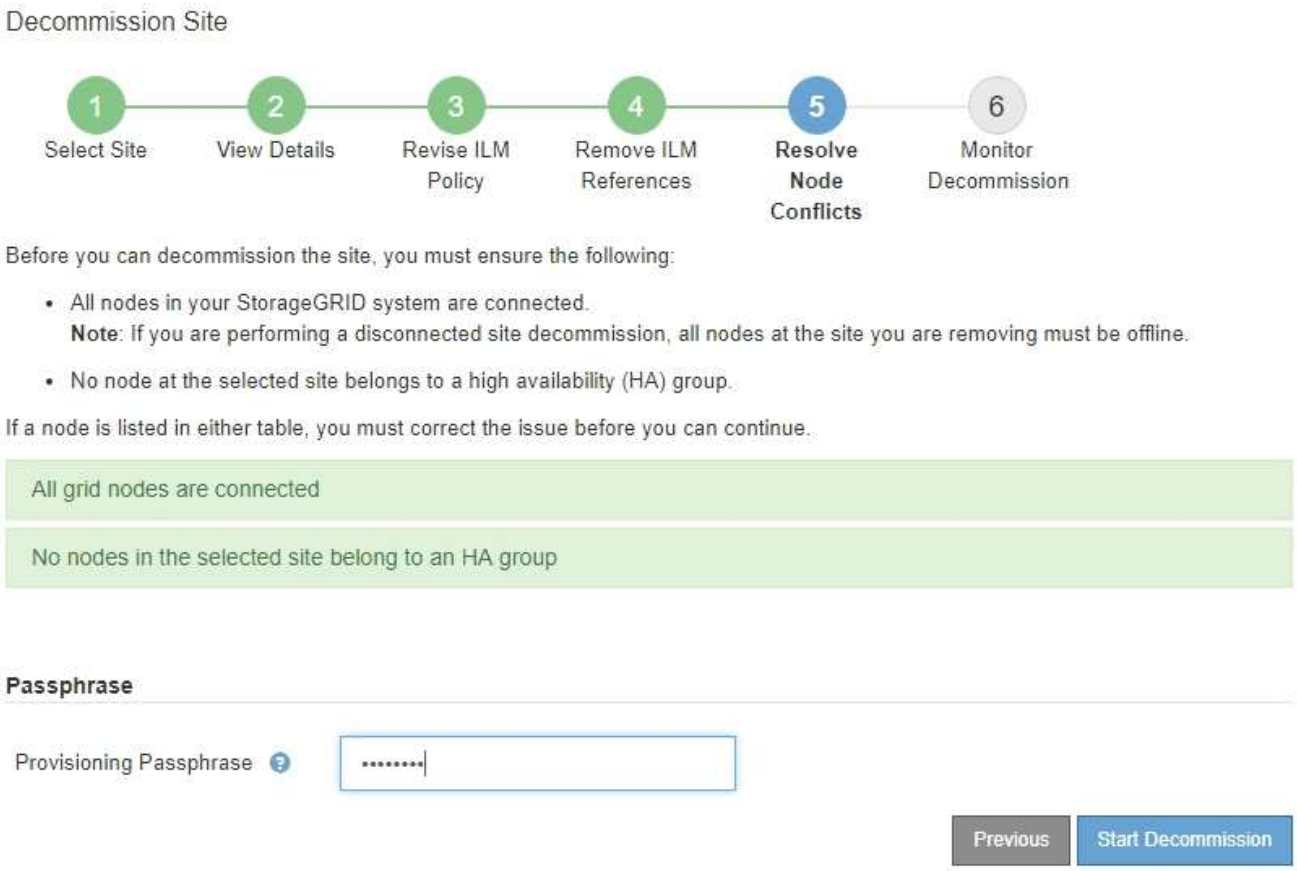


4. Se algum dos nós estiver listado, faça um dos seguintes procedimentos:
   - Edite cada grupo de HA afetado para remover a interface do nó.
   - Remover um grupo de HA que inclua somente nós deste local. Consulte as instruções para administrar o StorageGRID.

   Se todos os nós estiverem conetados e nenhum nó no local selecionado for usado em um grupo de HA, o campo **frase-passe de provisionamento** será ativado.

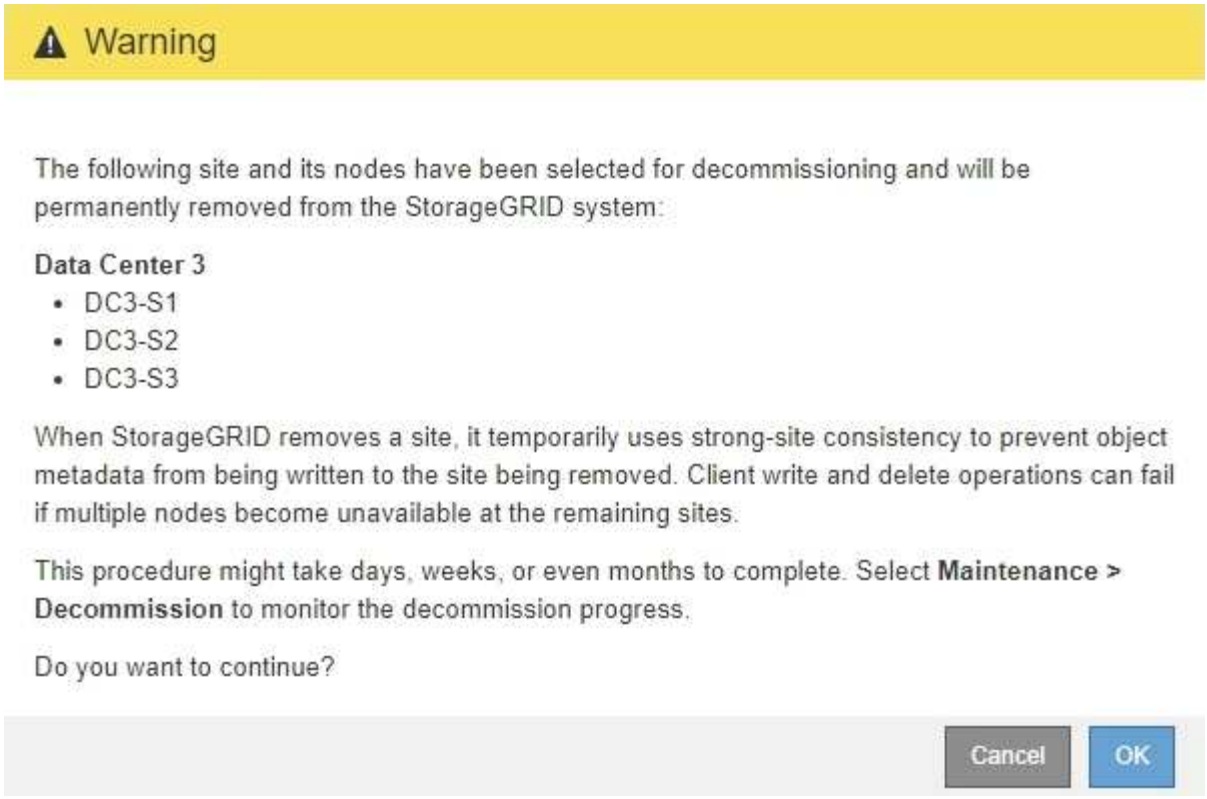
5. Introduza a frase-passe de aprovisionamento.

   O botão **Start Decommission** fica ativado.



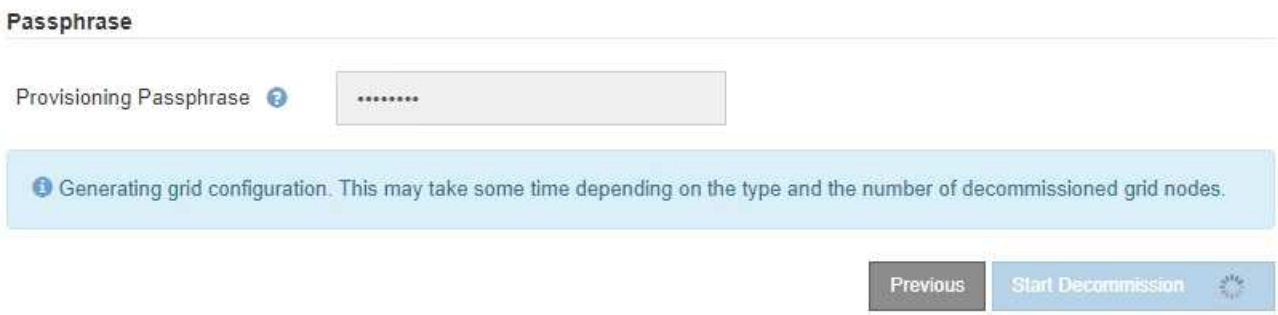
6. Se você estiver pronto para iniciar o procedimento de desativação do site, selecione **Start Decommission**.

   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.



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.



   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.

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 conetado, ele remove nós nessa ordem:

1. Nós de gateway

2. Nós de administração
3. Nós de storage

Quando o StorageGRID remove um site desconetado, 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.

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.

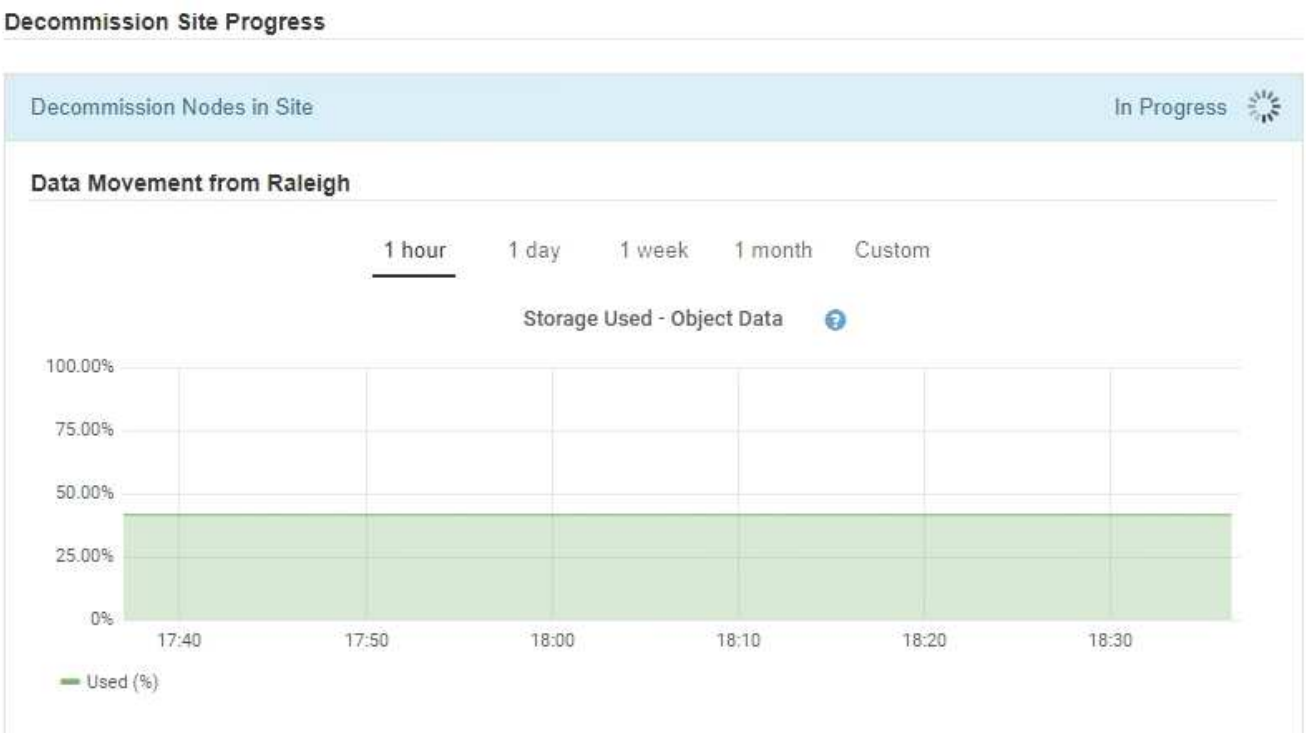
a. Selecione o link na mensagem ou selecione **MAINTENANCE** > **System** > **Recovery package**.
b. Transfira o `.zip` ficheiro.

   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.

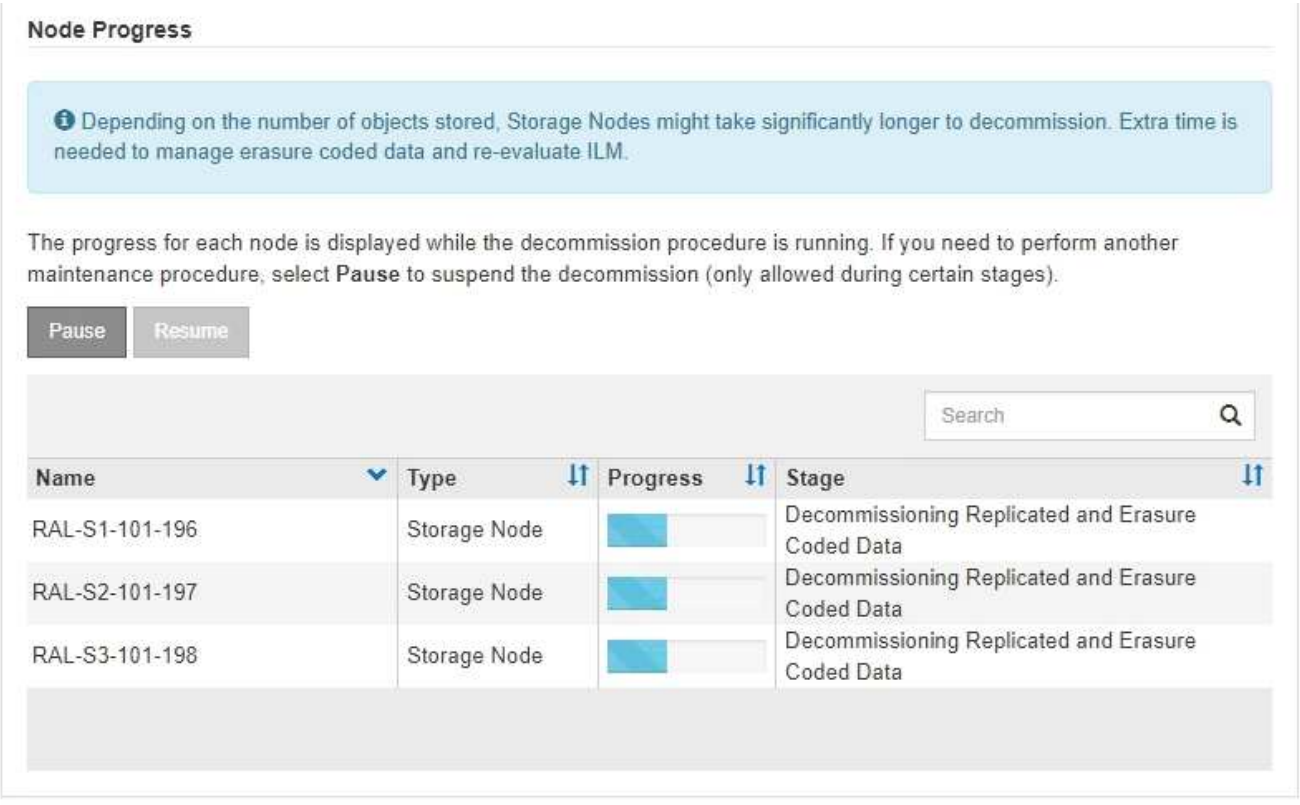
2. Usando o gráfico de movimentação de dados, monitore a movimentação de dados de objetos deste site para outros sites.

   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.



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.



Se você estiver monitorando o progresso de uma desativação de um site conetado, consulte esta tabela para entender os estágios de desativação de um nó de armazenamento:

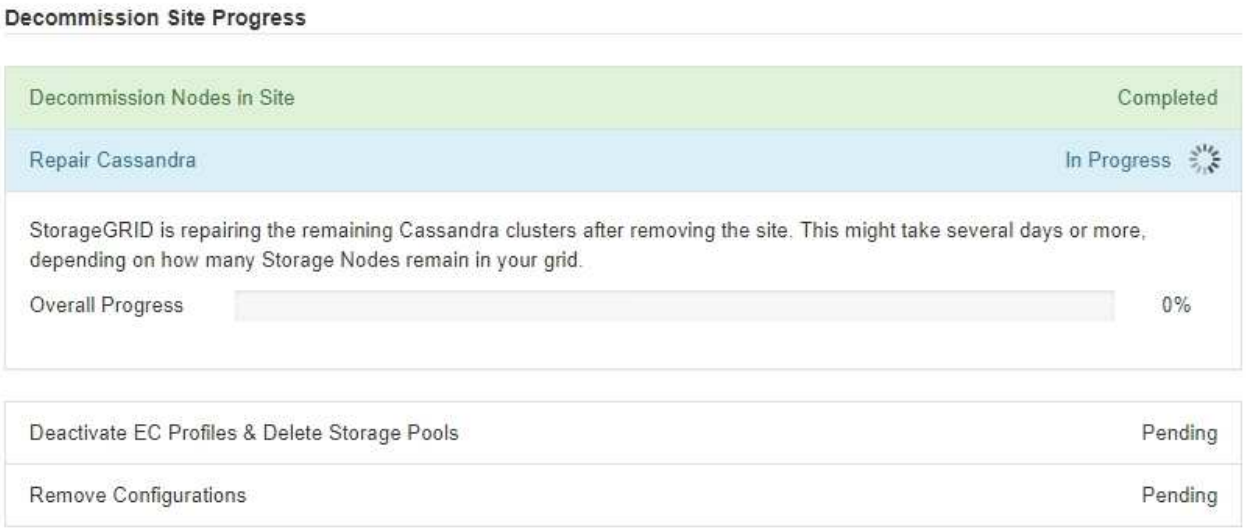
Fase	Duração estimada
Pendente	Minuto ou menos
Aguarde bloqueios	Minutos
Preparar tarefa	Minuto ou menos
Marcação LDR desativada	Minutos
Desativação de dados replicados e codificados por apagamento	Horas, dias ou semanas com base na quantidade de dados **Nota**: Se você precisar executar outras atividades 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 desconetado, 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

Fase	Duração estimada
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.

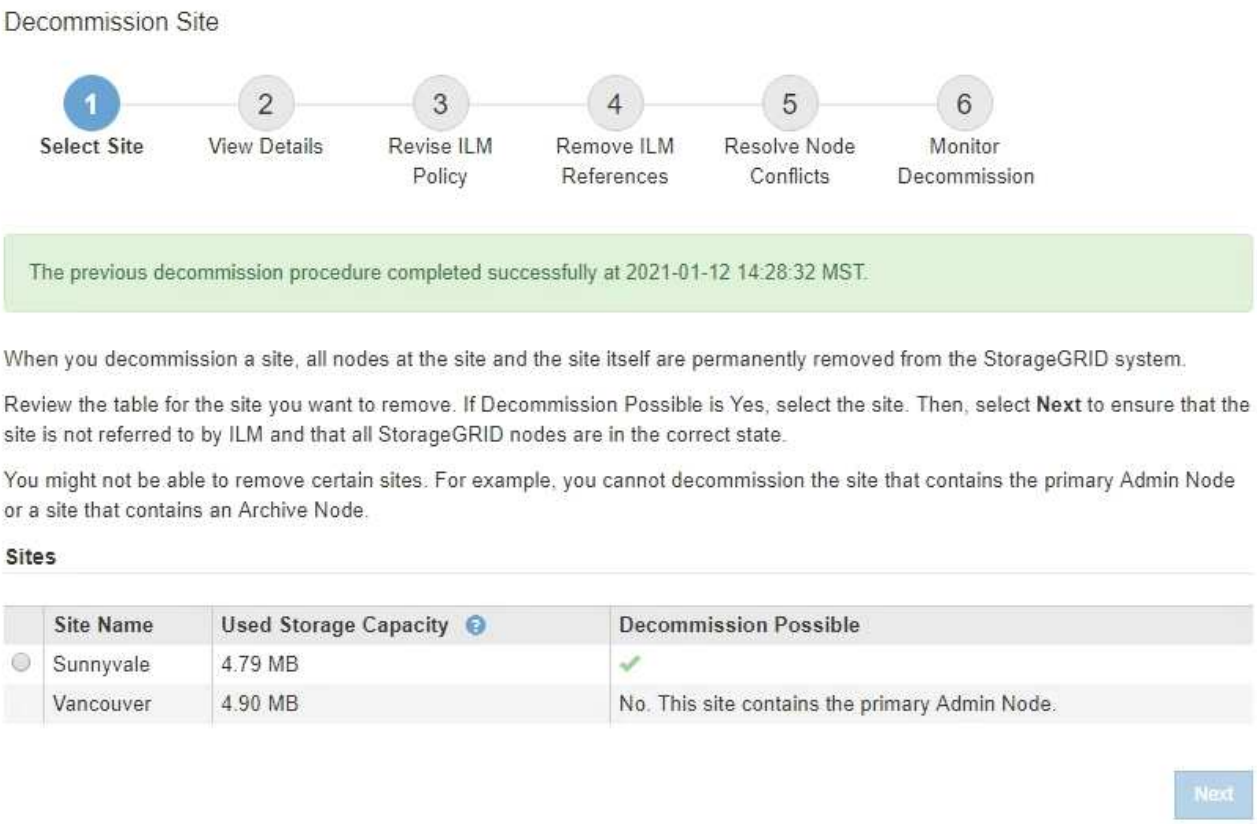


   - Durante a etapa **Deactivate EC Profiles & Delete Storage Pools**, as seguintes alterações de ILM são feitas:
     - Todos os perfis de codificação de apagamento que se referem ao site são desativados.
     - Todos os pools de armazenamento que se referem ao site são excluídos.

> O pool de storage de todos os nós de storage (StorageGRID 11,6 e anterior) também é removido porque 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.

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.



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 ative Directory (AD FS).
- Depois que os nós tiverem sido desligados automaticamente como parte do procedimento de desativação do site conetado, remova as máquinas virtuais associadas.

Renomeie grade, site ou nó

Use o procedimento de renomeação

Conforme necessário, você pode alterar os nomes de exibição exibidos no Gerenciador de Grade para toda a grade, cada site e cada nó. Você pode atualizar nomes de exibição com segurança e sempre que precisar.

Qual é o procedimento de mudança de nome?

Quando você instala o StorageGRID inicialmente, você especifica um nome para a grade, cada local e cada nó. Esses nomes iniciais são conhecidos como *nomes de sistema*, e eles são os nomes inicialmente exibidos em todo o StorageGRID.

Os nomes de sistema são necessários para operações internas do StorageGRID e não podem ser alterados. No entanto, você pode usar o procedimento de renomeação para definir novos *nomes de exibição* para a grade, cada site e cada nó. Esses nomes de exibição aparecem em vários locais do StorageGRID em vez de (ou, em alguns casos, além de) os nomes de sistema subjacentes.

Use o procedimento de renomeação para corrigir erros de digitação, implementar uma convenção de nomenclatura diferente ou para indicar que um site e todos os seus nós foram transferidos. Ao contrário dos nomes do sistema, os nomes de exibição podem ser atualizados sempre que necessário e sem afetar as operações do StorageGRID.

Onde aparecem os nomes do sistema e do visor?

A tabela a seguir resume onde nomes de sistema e nomes de exibição são exibidos na interface de usuário do StorageGRID e em arquivos StorageGRID.

Localização	Nome do sistema	Nome do visor
Páginas do Grid Manager	Mostrado a menos que o item seja renomeado	Se um item for renomeado, mostrado em vez do nome do sistema nessas localizações: • Painel de instrumentos • Página de nós • Páginas de configuração para grupos de alta disponibilidade, pontos de extremidade do balanceador de carga, interfaces VLAN, servidores de gerenciamento de chaves, senhas de grade e controle de firewall • Alertas • Definições do conjunto de armazenamento • Página de pesquisa de metadados de objetos • Páginas relacionadas a procedimentos de manutenção, incluindo atualização, hotfix, atualização do SANtricity os, desativação, expansão, recuperação e verificação de existência de objetos • Páginas de suporte (logs e diagnósticos) • Página de logon único, ao lado do nome de host do nó de administrador na tabela para detalhes do nó de administrador

Localização	Nome do sistema	Nome do visor
NÓS > **Visão geral** guia para um nó	Sempre apresentado	Mostrado apenas se o item for renomeado
Páginas legadas no Gerenciador de Grade (por exemplo, **SUPORTE** > **topologia de Grade**)	Mostrado	Não apresentado
Node-health API	Sempre devolvido	Retornado somente se o item for renomeado

Avisar ao usar SSH para acessar um nó	Mostrado como o nome principal, a menos que o item tenha sido renomeado:
	
	`admin@SYSTEM-NAME: ~ $`
	
	Incluído entre parênteses quando o item é renomeado:
	
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		Mostrado como o nome principal quando o item é renomeado:
		
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt` Arquivo no Pacote de recuperação	Mostrado como `Server Name`	Mostrado como `Display Name`
`/etc/hosts` arquivo em todos os nós Por exemplo: `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	Sempre mostrado na segunda coluna	Quando o item é renomeado, mostrado na quarta coluna
`topology-display-names.json`, Incluído com dados AutoSupport	Não incluído	Vazio a menos que os itens tenham sido renomeados; caso contrário, mapeia as IDs de grade, local e nó para seus nomes de exibição.

Requisitos de nome de exibição

Antes de utilizar este procedimento, reveja os requisitos para nomes de visualização.

Nomes de exibição para nós

Os nomes de exibição dos nós devem seguir estas regras:

- Deve ser único em todo o seu sistema StorageGRID.
- Não pode ser o mesmo que o nome do sistema para qualquer outro item no seu sistema StorageGRID.
- Deve conter pelo menos 1 e não mais de 32 carateres.
- Pode conter números, hífens (-) e letras maiúsculas e minúsculas.
- Pode começar ou terminar com uma letra ou número, mas não pode iniciar ou terminar com um hífen.
- Não pode ser todos os números.
- São sensíveis a maiúsculas e minúsculas. Por exemplo, `DC1-ADM` e `dc1-adm` são considerados duplicados.

Você pode renomear um nó com um nome de exibição que foi usado anteriormente por um nó diferente, desde que o nome não resulte em um nome de exibição duplicado ou nome de sistema.

Exibir nomes para grade e sites

Os nomes de exibição para a grade e sites seguem as mesmas regras com estas exceções:

- Pode incluir espaços.
- Pode incluir estes carateres especiais: `= - _ : , . @ !`
- Pode começar e terminar com os carateres especiais, incluindo hífens.
- Pode ser todos os números ou carateres especiais.

Apresentar as melhores práticas de nomes

Se você pretende renomear vários itens, documente seu esquema de nomenclatura geral antes de usar este procedimento. Crie um sistema que garanta que os nomes sejam únicos, consistentes e fáceis de entender rapidamente.

Você pode usar qualquer convenção de nomenclatura que atenda aos seus requisitos organizacionais. Considere estas sugestões básicas sobre o que incluir:

- **Indicador de local**: Se você tiver vários sites, adicione um código de site a cada nome de nó.
- * Tipo de nó*: Os nomes de nó normalmente indicam o tipo do nó. Você pode usar abreviações como `s`, `adm` e `gw` (nó de storage, nó de administrador e nó de gateway).
- **Número do nó**: Se um site contiver mais de um tipo específico de nó, adicione um número exclusivo ao nome de cada nó.

Pense duas vezes antes de adicionar detalhes específicos aos nomes que provavelmente mudarão ao longo do tempo. Por exemplo, não inclua endereços IP em nomes de nós porque esses endereços podem ser alterados. Da mesma forma, as localizações de rack ou os números de modelo de dispositivo podem mudar se você mover o equipamento ou atualizar o hardware.

Exemplos de nomes de exibição

Suponha que seu sistema StorageGRID tenha três data centers e tenha nós de diferentes tipos em cada data center. Seus nomes de exibição podem ser tão simples quanto estes:

- * Grade*: `StorageGRID Deployment`
- **Primeiro site**: `Data Center 1`
  - `dc1-adm1`
  - `dc1-s1`
  - `dc1-s2`
  - `dc1-s3`
  - `dc1-gw1`
- **Segundo site**: `Data Center 2`
  - `dc2-adm2`
  - `dc2-s1`
  - `dc2-s2`
  - `dc2-s3`
- * Terceiro site*: `Data Center 3`
  - `dc3-s1`
  - `dc3-s2`
  - `dc3-s3`

Adicionar ou atualizar nomes de exibição

Você pode usar este procedimento para adicionar ou atualizar os nomes de exibição usados para sua grade, sites e nós. Você pode renomear um único item, vários itens ou até mesmo todos os itens ao mesmo tempo. Definir ou atualizar um nome de exibição não afeta as operações do StorageGRID de forma alguma.

Antes de começar

- No **nó Admin principal**, você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

> Você pode adicionar ou atualizar nomes de exibição de um nó de administração não primário, mas você deve estar conetado ao nó de administração principal para baixar um pacote de recuperação.

- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento.
- Você entende os requisitos e as práticas recomendadas para nomes de exibição. "Renomeie grade, sites e nós"Consulte .

Como renomear grade, sites ou nós

Você pode renomear seu sistema StorageGRID, um ou mais sites ou um ou mais nós.

Você pode usar um nome de exibição que foi usado anteriormente por um nó diferente, desde que o nome

não resulte em um nome de exibição duplicado ou nome de sistema.

Selecione itens para mudar o nome

Para iniciar, selecione os itens que deseja renomear.

Passos

1. Selecione **MAINTENANCE** > **Tasks** > **Renomear grade, sites e nós**.
2. Para a etapa **Selecionar nomes**, selecione os itens que deseja renomear.

Item a alterar	Instrução
Nomes de tudo (ou quase tudo) em seu sistema	a. Selecione **Selecionar tudo**. b. Opcionalmente, limpe todos os itens que você não deseja renomear.
Nome da grelha	Selecione a caixa de verificação para a grelha.
Nome de um site e alguns ou todos os seus nós	a. Marque a caixa de seleção no cabeçalho da tabela para o site. b. Opcionalmente, limpe todos os nós que você não deseja renomear.
Nome de um site	Selecione a caixa de verificação para o site.
Nome de um nó	Selecione a caixa de verificação para o nó.

3. Selecione **continuar**.
4. Reveja a tabela, que inclui os itens selecionados.
   - A coluna **Nome de exibição** mostra o nome atual de cada item. Se o item nunca tiver sido renomeado, seu nome de exibição será o mesmo que seu nome de sistema.
   - A coluna **Nome do sistema** mostra o nome digitado para cada item durante a instalação. Os nomes do sistema são usados para operações internas do StorageGRID e não podem ser alterados. Por exemplo, o nome do sistema para um nó pode ser o nome do host.
   - A coluna **tipo** indica o tipo do item: Grade, local ou o tipo específico de nó.

Propor novos nomes

Para a etapa **propor novos nomes**, você pode inserir um nome de exibição para cada item individualmente ou renomear itens em massa.

Renomeie itens individualmente

Siga estas etapas para inserir um nome de exibição para cada item que você deseja renomear.

Passos

1. No campo **Nome de exibição**, insira um nome de exibição proposto para cada item na lista.

   "Renomeie grade, sites e nós"Consulte para saber os requisitos de nomenclatura.

2. Para remover quaisquer itens que você não deseja renomear, selecione ✕ na coluna **Remover da lista**.

   Se você não vai propor um novo nome para um item, você deve removê-lo da tabela.

3. Quando tiver proposto novos nomes para todos os itens da tabela, selecione **Renomear**.

   É apresentada uma mensagem de sucesso. Os novos nomes de exibição agora são usados em todo o Gerenciador de Grade.

Renomeie itens em massa

Use a ferramenta de renomeação em massa se os nomes de itens compartilharem uma cadeia de carateres comum que você deseja substituir por uma cadeia de carateres diferente.

Passos

1. Para a etapa **propor novos nomes**, selecione **usar a ferramenta de renomeação em massa**.

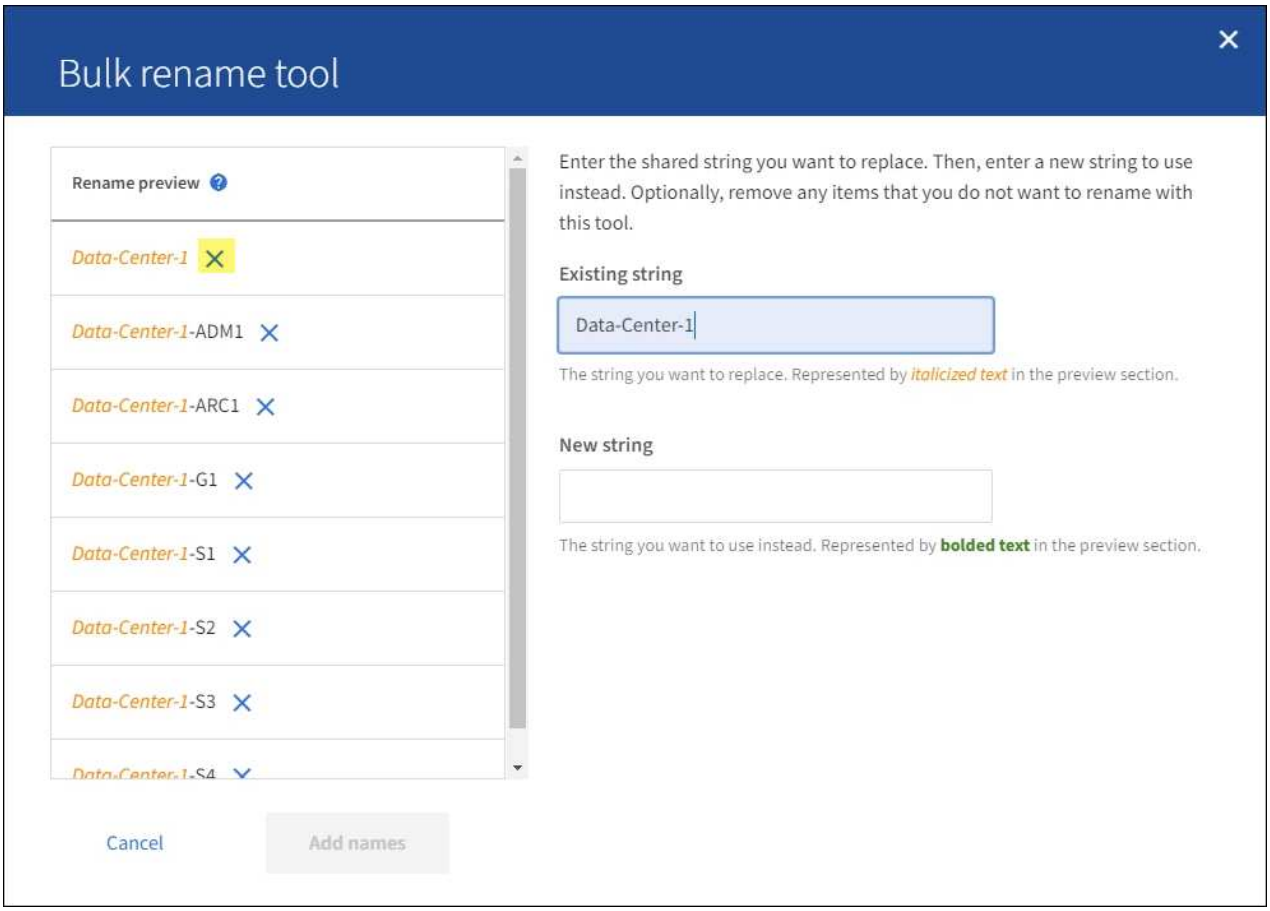
   A visualização **Renomear** inclui todos os itens que foram mostrados para a etapa **propor novos nomes**. Você pode usar a visualização para ver como os nomes de exibição ficarão depois de substituir uma string compartilhada.

2. No campo **string existente**, insira a string compartilhada que você deseja substituir. Por exemplo, se a cadeia de carateres que você deseja substituir for `Data-Center-1`, digite **Data-Center-1**.

   À medida que você digita, seu texto é realçado onde quer que seja encontrado nos nomes à esquerda.

3. ✕Selecione para remover quaisquer itens que você não deseja renomear com esta ferramenta.

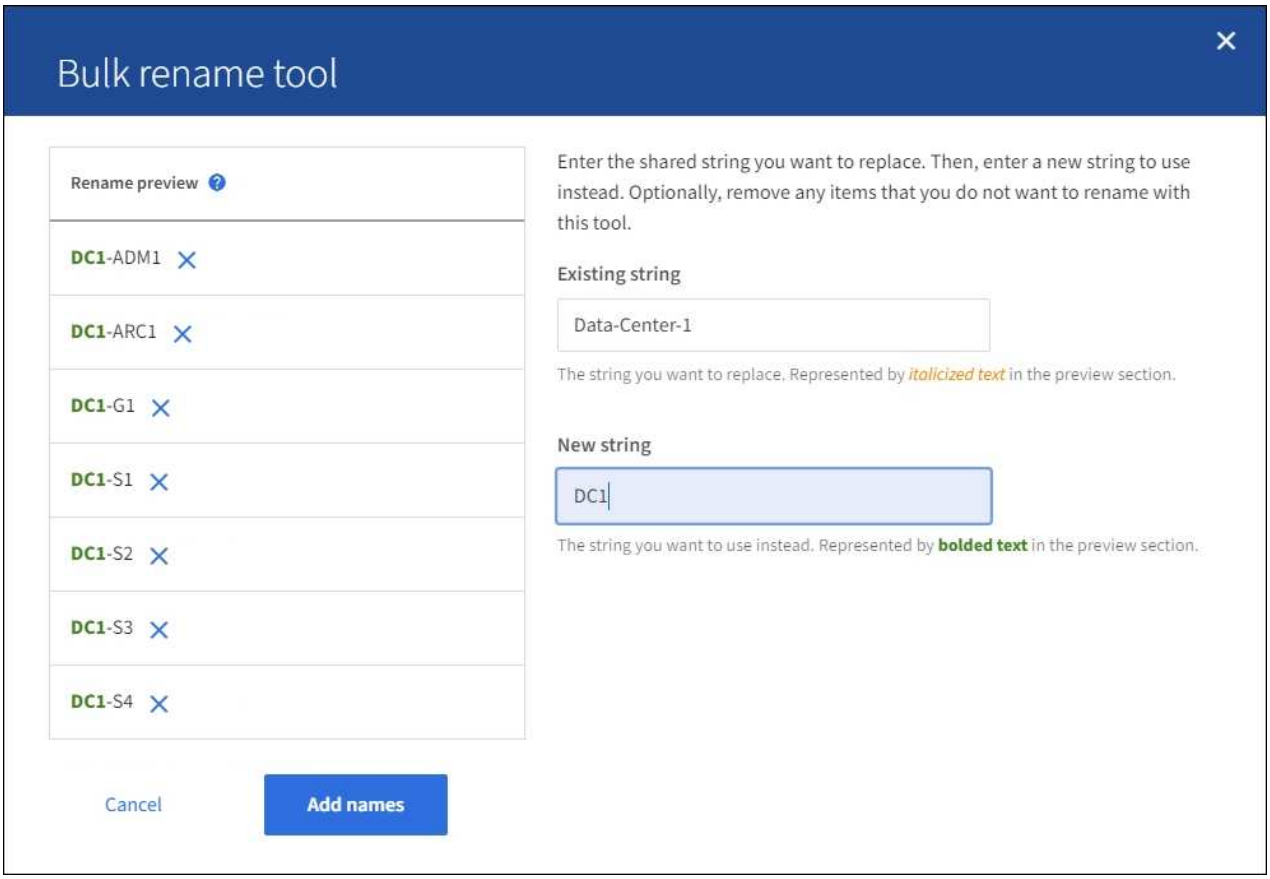
   Por exemplo, suponha que você queira renomear todos os nós que contêm a cadeia de carateres `Data-Center-1`, mas você não quer renomear o `Data-Center-1` próprio site. ✕Selecione para remover o site da pré-visualização de renomeação.



4. No campo **New string**, insira a string de substituição que deseja usar. Por exemplo, digite **DC1**.

   "Renomeie grade, sites e nós"Consulte para saber os requisitos de nomenclatura.

   À medida que você digita a string de substituição, os nomes à esquerda são atualizados, para que você possa verificar se os novos nomes estarão corretos.



5. Quando estiver satisfeito com os nomes mostrados na pré-visualização, selecione **Adicionar nomes** para adicionar os nomes à tabela para a etapa **propor novos nomes**.
6. Faça quaisquer alterações adicionais necessárias ou selecione para remover quaisquer itens que você não deseja renomear.
7. Quando estiver pronto para renomear todos os itens da tabela, selecione **Renomear**.

   É apresentada uma mensagem de sucesso. Os novos nomes de exibição agora são usados em todo o Gerenciador de Grade.

Baixe o pacote de recuperação

Quando terminar de renomear itens, baixe e salve um novo Pacote de recuperação. Os novos nomes de exibição para os itens que você renomeou são incluídos no `Passwords.txt` arquivo.

Passos

1. Introduza a frase-passe de aprovisionamento.
2. Selecione **Download Recovery Package**.

   O download começa imediatamente.

3. Quando o download for concluído, abra o `Passwords.txt` arquivo para ver o nome do servidor de todos os nós e os nomes de exibição de todos os nós renomeados.
4. Copie o `sgws-recovery-package-id-revision.zip` arquivo 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.

5. Selecione **Finish** para retornar ao primeiro passo.

Reverter nomes de exibição de volta para nomes de sistema

Você pode reverter uma grade renomeada, site ou nó de volta para o nome original do sistema. Quando você reverte um item de volta ao nome do sistema, as páginas do Gerenciador de Grade e outros locais do StorageGRID não mostram mais um **Nome de exibição** para esse item. Apenas o nome do sistema do item é mostrado.

Passos

1. Selecione **MAINTENANCE** > **Tasks** > **Renomear grade, sites e nós**.
2. Para a etapa **Selecionar nomes**, selecione todos os itens que você deseja reverter para os nomes do sistema.
3. Selecione **continuar**.
4. Para a etapa **propor novos nomes**, reverta os nomes de exibição de volta aos nomes de sistema individualmente ou em massa.

Reverta para nomes de sistema individualmente

a. Copie o nome de sistema original de cada item e cole-o no campo **Nome de exibição** ou selecione ✕ para remover quaisquer itens que você não deseja reverter.

   Para reverter um nome de exibição, o nome do sistema deve aparecer no campo **Nome de exibição**, mas o nome não diferencia maiúsculas de minúsculas.

b. Selecione **Renomear**.

   É apresentada uma mensagem de sucesso. Os nomes de exibição desses itens não são mais usados.

Reverter para nomes de sistema em massa

a. Para a etapa **propor novos nomes**, selecione **usar a ferramenta de renomeação em massa**.

b. No campo **string existente**, insira a string de nome de exibição que deseja substituir.

c. No campo **Nova cadeia**, insira a cadeia de nomes de sistema que deseja usar.

d. Selecione **Adicionar nomes** para adicionar os nomes à tabela para a etapa **propor novos nomes**.

e. Confirme se cada entrada no campo **Nome de exibição** corresponde ao nome no campo **Nome do sistema**. Faça quaisquer alterações ou selecione ✕ para remover quaisquer itens que você não deseja reverter.

   Para reverter um nome de exibição, o nome do sistema deve aparecer no campo **Nome de exibição**, mas o nome não diferencia maiúsculas de minúsculas.

f. Selecione **Renomear**.

   É apresentada uma mensagem de sucesso. Os nomes de exibição desses itens não são mais usados.

5. Baixe e salve um novo pacote de recuperação.

   Os nomes de exibição dos itens que você reverteu não estão mais incluídos no `Passwords.txt` arquivo.

Procedimentos do nó

Procedimentos de manutenção do nó

Talvez seja necessário executar procedimentos de manutenção relacionados a nós de grade ou serviços de nós específicos.

Procedimentos do Server Manager

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.

Para executar os procedimentos do Gerenciador de servidores, você geralmente precisa acessar a linha de

comando do nó.

> 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`

Procedimentos de reinicialização, desligamento e energia do nó

Use esses procedimentos para reinicializar um ou mais nós, desligar e reiniciar nós ou desligar nós e ligá-los novamente.

Procedimentos de remapeamento de portas

Você pode usar os procedimentos de remapeamento de portas para remover os remapas de portas de um nó, por exemplo, se quiser configurar um ponto de extremidade do balanceador de carga usando uma porta que foi anteriormente remapeada.

Procedimentos do Server Manager

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

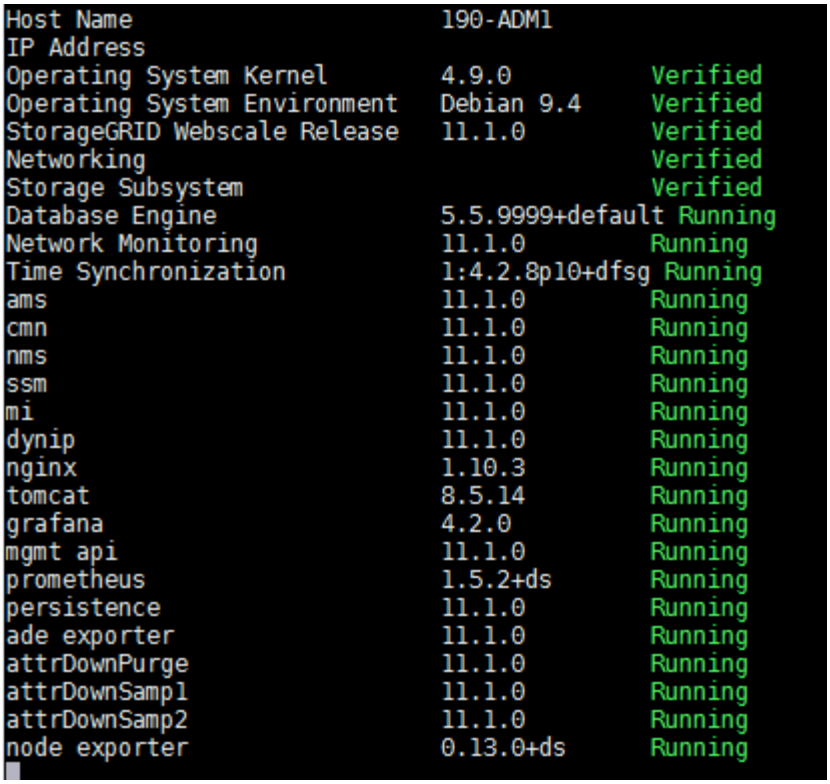
Passos

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.



3. Volte para a linha de comando, pressione **Ctrl** * C*.
4. 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.

5. 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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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

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. 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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Quando você usa estas etapas para "parar administrativamente" um serviço, o Gerenciador de servidores 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"

Forçar o serviço a terminar

Se você precisar parar um serviço imediatamente, você pode usar o `force-stop` comando.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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`

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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

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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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`

Procedimentos de reinicialização, desligamento e energia

Execute uma reinicialização contínua

Você pode executar uma reinicialização contínua para reinicializar vários nós de grade sem causar uma interrupção do serviço.

Antes de começar

- Você está conetado ao Gerenciador de Grade no nó Admin principal e está usando um "navegador da web suportado".

  Você deve estar conetado ao nó de administração principal para executar este procedimento.

- Você tem o "Permissão de manutenção ou acesso root".

Sobre esta tarefa

Use este procedimento se você precisar reinicializar vários nós ao mesmo tempo. Por exemplo, você pode usar este procedimento depois de alterar o modo FIPS para a grade "Política de segurança TLS e SSH". Quando o modo FIPS muda, você deve reinicializar todos os nós para colocar a alteração em vigor.

Se você só precisa reiniciar um nó, você pode "Reinicie o nó a partir do separador tarefas".

Quando o StorageGRID reinicializa os nós de grade, ele emite o `reboot` comando em cada nó, o que faz com que o nó desligue e reinicie. Todos os serviços são reiniciados automaticamente.

- Reiniciar um nó VMware reinicializa a máquina virtual.
- Reiniciar um nó Linux reinicializa o contentor.
- Reiniciar um nó de dispositivo StorageGRID reinicializa o controlador de computação.

O procedimento de reinicialização contínua pode reinicializar vários nós ao mesmo tempo, com estas exceções:

- Dois nós do mesmo tipo não serão reinicializados ao mesmo tempo.
- Os nós de Gateway e os nós de administrador não serão reiniciados ao mesmo tempo.

Em vez disso, esses nós são reinicializados sequencialmente para garantir que grupos de HA, dados de objetos e serviços de nós críticos permaneçam sempre disponíveis.

Quando você reinicia o nó Admin principal, seu navegador perde temporariamente o acesso ao Gerenciador de Grade, para que você não possa mais monitorar o procedimento. Por este motivo, o nó de administração principal é reiniciado por último.

Execute uma reinicialização contínua

Selecione os nós que pretende reiniciar, reveja as suas seleções, inicie o procedimento de reinício e monitorize o progresso.

Selecione nós

Como primeiro passo, acesse a página de reinicialização contínua e selecione os nós que deseja reinicializar.

Passos

1. Selecione **MAINTENANCE** > **Tasks** > **Rolling reboot**.
2. Revise o estado da conexão e os ícones de alerta na coluna **Nome do nó**.

   Não é possível reiniciar um nó se ele estiver desconetado da grade. As caixas de verificação estão desativadas para nós com estes ícones: Ou .

3. Se algum nó tiver alertas ativos, revise a lista de alertas na coluna **Resumo de alertas**.

   Para ver todos os alertas atuais de um nó, você também pode selecionar o "Separador Descrição geral dos nós >".

4. Opcionalmente, execute as ações recomendadas para resolver quaisquer alertas atuais.
5. Opcionalmente, se todos os nós estiverem conetados e você quiser reinicializar todos eles, marque a caixa de seleção no cabeçalho da tabela e selecione **Selecionar tudo**. Caso contrário, selecione cada nó que você deseja reinicializar.

   Você pode usar as opções de filtro da tabela para exibir subconjuntos de nós. Por exemplo, você pode exibir e selecionar somente nós de storage ou todos os nós em um determinado local.

6. Selecione **seleção de revisão**.

Seleção de revisão

Nesta etapa, você pode determinar quanto tempo o procedimento de reinicialização total pode demorar e confirmar se selecionou os nós corretos.

1. Na página de seleção Revisão, revise o Resumo, que indica quantos nós serão reinicializados e o tempo total estimado para que todos os nós sejam reiniciados.
2. Opcionalmente, para remover um nó específico da lista de reinicialização, selecione **Remover**.
3. Opcionalmente, para adicionar mais nós, selecione **passo anterior**, selecione os nós adicionais e selecione **seleção de revisão**.
4. Quando estiver pronto para iniciar o procedimento de reinicialização contínua para todos os nós selecionados, selecione **Reboot Nodes**.
5. Se você selecionou para reinicializar o nó de administração principal, leia a mensagem de informações e selecione **Yes**.

   O nó Admin principal será o último nó a reiniciar. Enquanto este nó estiver reiniciando, a conexão do seu navegador será perdida. Quando o nó Admin principal estiver disponível novamente, você deve recarregar a página de reinicialização contínua.

Monitore uma reinicialização contínua

Enquanto o procedimento de reinicialização contínua estiver em execução, você pode monitorá-lo a partir do nó de administração principal.

Passos

1. Reveja o progresso geral da operação, que inclui as seguintes informações:

- Número de nós reiniciados
- Número de nós em processo de reinicialização
- Número de nós que ainda precisam ser reiniciados

2. Revise a tabela para cada tipo de nó.

   As tabelas fornecem uma barra de progresso da operação em cada nó e mostram a etapa de reinicialização para esse nó, que pode ser um destes:

   - A aguardar para reiniciar
   - Parar serviços
   - Reiniciar o sistema
   - Iniciar serviços
   - Reinicialização concluída

Pare o procedimento de reinicialização contínua

Você pode parar o procedimento de reinicialização contínua do nó de administração principal. Quando você parar o procedimento, todos os nós que têm o status "parando serviços", "reinicializando o sistema" ou "iniciando serviços" concluirão a operação de reinicialização. No entanto, esses nós não serão mais rastreados como parte do procedimento.

Passos

1. Selecione **MAINTENANCE** > **Tasks** > **Rolling reboot**.
2. Na etapa **Monitor Reboot**, selecione **Stop Reboot Procedure**.

Reinicie o nó da grade a partir da guia tarefas

Você pode reinicializar um nó de grade individual a partir da guia tarefas na página nós.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento.
- Se você estiver reinicializando o nó Admin principal ou qualquer nó de armazenamento, você revisou as seguintes considerações:
  - Quando você reinicia o nó Admin principal, seu navegador perde temporariamente o acesso ao Gerenciador de Grade.
  - Se você reinicializar dois ou mais nós de storage em um determinado local, talvez não consiga acessar certos objetos durante a reinicialização. Esse problema pode ocorrer se qualquer regra ILM usar a opção de ingestão **Dual commit** (ou uma regra especifica **Balanced** e não é possível criar imediatamente todas as cópias necessárias). Nesse caso, o StorageGRID comprometerá objetos recém-ingeridos a dois nós de storage no mesmo local e avaliará o ILM posteriormente.
  - 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.

Sobre esta tarefa

Quando o StorageGRID reinicializa um nó de grade, ele emite o `reboot` comando no nó, o que faz com que o

nó desligue e reinicie. Todos os serviços são reiniciados automaticamente.

- Reiniciar um nó VMware reinicializa a máquina virtual.
- Reiniciar um nó Linux reinicializa o contentor.
- Reiniciar um nó de dispositivo StorageGRID reinicializa o controlador de computação.

> Se for necessário reiniciar mais de um nó, pode utilizar o "procedimento de reinicialização a rolar".

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. Introduza a frase-passe de aprovisionamento e selecione **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 para o nó na página nós. Quando todos os serviços tiverem sido iniciados novamente e o nó for conetado com êxito à grade, a página de nós deve exibir o status normal (sem ícones à esquerda do nome do nó), indicando que nenhum alerta está ativo e o nó está conetado 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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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. 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.

Antes de começar

- Você tem o `Passwords.txt` arquivo.

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. "Gerenciar objetos com ILM"Consulte .

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 estiver a desligar um nó de dispositivo, siga os passos para o seu aparelho.

SG6160

a. Desligue a alimentação do controlador de armazenamento SG6100-CN.

b. Aguarde até que o LED azul de alimentação no controlador de armazenamento SG6100-CN se desligue.

SGF6112

a. Desligue a alimentação do aparelho.

b. Aguarde até que o LED azul de alimentação se desligue.

SG6000

a. 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.

b. Desligue o aparelho e aguarde até que o LED azul de alimentação se desligue.

SG5800

a. 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.

b. Na página inicial do Gerenciador do sistema do SANtricity, selecione **Exibir operações em andamento**.

c. Confirme se todas as operações foram concluídas antes de continuar com a próxima etapa.

d. Desligue ambos os interruptores de energia no compartimento do controlador e aguarde que todos os LEDs no compartimento do controlador se desliguem.

SG5700

a. 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.

b. Desligue a alimentação do aparelho e aguarde que todas as atividades de exibição de LED e de sete segmentos parem.

SG100 ou SG1000

a. Desligue a alimentação do aparelho.

b. Aguarde até que o LED azul de alimentação se desligue.

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 estiver a desligar um nó de dispositivo, siga os passos para o seu aparelho.

SG6160

a. Desligue a alimentação do controlador de armazenamento SG6100-CN.
b. Aguarde até que o LED azul de alimentação no controlador de armazenamento SG6100-CN se desligue.

SGF6112

a. Desligue a alimentação do aparelho.
b. Aguarde até que o LED azul de alimentação se desligue.

SG6000

a. 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.

b. Desligue o aparelho e aguarde até que o LED azul de alimentação se desligue.

SG5800

a. 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.

b. Na página inicial do Gerenciador do sistema do SANtricity, selecione **Exibir operações em andamento**.
c. Confirme se todas as operações foram concluídas antes de continuar com a próxima etapa.
d. Desligue ambos os interruptores de energia no compartimento do controlador e aguarde que todos os LEDs no compartimento do controlador se desliguem.

SG5700

a. 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.

b. Desligue a alimentação do aparelho e aguarde que todas as atividades de exibição de LED e de sete segmentos parem.

SG110 ou SG1100

a. Desligue a alimentação do aparelho.
b. Aguarde até que o LED azul de alimentação se desligue.

SG100 ou SG1000

a. Desligue a alimentação do aparelho.
b. Aguarde até que o LED azul de alimentação se desligue.

7. Faça logout do shell de comando: `exit`

Informações relacionadas

- "Aparelhos de armazenamento SGF6112 e SG6160"
- "SG6000 dispositivos de armazenamento"
- "SG5700 dispositivos de armazenamento"
- "SG5800 dispositivos de armazenamento"
- "Aparelhos de serviços SG110 e SG1100"
- "Aparelhos de serviços SG100 e SG1000"

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 em nós de administração e nós de gateway e, em seguida, pare os serviços em 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 acedam 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 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 de dispositivo, siga as etapas para o seu dispositivo.

SG110 ou SG1100

a. Desligue a alimentação do aparelho.
b. Aguarde até que o LED azul de alimentação se desligue.

SG100 ou SG1000

a. Desligue a alimentação do aparelho.
b. Aguarde até que o LED azul de alimentação se desligue.

SG6160

a. Desligue a alimentação do controlador de armazenamento SG6100-CN.
b. Aguarde até que o LED azul de alimentação no controlador de armazenamento SG6100-CN se desligue.

SGF6112

a. Desligue a alimentação do aparelho.
b. Aguarde até que o LED azul de alimentação se desligue.

SG6000

a. 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.

b. Desligue o aparelho e aguarde até que o LED azul de alimentação se desligue.

SG5800

a. 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.

b. Na página inicial do Gerenciador do sistema do SANtricity, selecione **Exibir operações em andamento**.
c. Confirme se todas as operações foram concluídas antes de continuar com a próxima etapa.
d. Desligue ambos os interruptores de energia no compartimento do controlador e aguarde que todos os LEDs no compartimento do controlador se desliguem.

SG5700

a. 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.

b. 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.

Inicie os nós de grade

> 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 reconstroem dados do Cassandra. Isso pode resultar em perda de dados.

Se possível, ligue 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 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.

Informações relacionadas

- "Aparelhos de armazenamento SGF6112 e SG6160"
- "Aparelhos de serviços SG110 e SG1100"
- "Aparelhos de serviços SG100 e SG1000"
- "SG6000 dispositivos de armazenamento"
- "SG5800 dispositivos de armazenamento"
- "SG5700 dispositivos de armazenamento"

Procedimentos de remapeamento de portas

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, "Configuração dos pontos de extremidade do balanceador de carga"consulte .

> Se o remapeamento da porta fornecer acesso ao cliente, reconfigure o cliente para usar uma porta diferente como um endpoint do balanceador de carga para evitar a perda de serviço. Caso contrário, a remoção do mapeamento de portas resultará na perda de acesso do cliente e deve ser agendada 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: `reboot`
4. Faça logout do shell de comando: `exit`
5. Repita estas etapas em cada nó de administração e nó de gateway que tenha portas remapeadas conflitantes.

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.

Sobre esta tarefa

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.

> 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 remapas 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 remapas 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.

Procedimentos de 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 para 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.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento.
- Você tem 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 uma nova sub-rede à lista de sub-rede da rede de Grade antes de iniciar o procedimento de expansão. Caso contrário, você terá que cancelar a expansão, adicionar a nova sub-rede e iniciar a expansão novamente.

Adicione uma sub-rede

Passos

1. Selecione **MAINTENANCE** > **Network** > **Grid Network**.
2. Selecione **Adicionar outra sub-rede** para adicionar uma nova sub-rede na notação CIDR.

   Por exemplo, introduza `10.96.104.0/22`.

3. Insira a senha de provisionamento e selecione **Salvar**.
4. Aguarde até que as alterações sejam aplicadas e, em seguida, faça o download de um novo pacote de recuperação.
   a. Selecione **MAINTENANCE** > **System** > **Recovery package**.
   b. Introduza a **frase-passe de aprovisionamento**.

> 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. Ele também é usado para recuperar o nó de administração principal.

As sub-redes especificadas são configuradas automaticamente para o sistema StorageGRID.

Edite uma sub-rede

Passos

1. Selecione **MAINTENANCE** > **Network** > **Grid Network**.
2. Selecione a sub-rede que deseja editar e faça as alterações necessárias.
3. Introduza a frase-passe do aprovisionamento e selecione **Guardar**.
4. Selecione **Sim** na caixa de diálogo de confirmação.
5. Aguarde até que as alterações sejam aplicadas e, em seguida, faça o download de um novo pacote de recuperação.
   a. Selecione **MAINTENANCE** > **System** > **Recovery package**.
   b. Introduza a **frase-passe de aprovisionamento**.

Eliminar uma sub-rede

Passos

1. Selecione **MAINTENANCE** > **Network** > **Grid Network**.
2. Selecione o ícone de exclusão ao lado da sub-rede.
3. Introduza a frase-passe do aprovisionamento e selecione **Guardar**.
4. Selecione **Sim** na caixa de diálogo de confirmação.
5. Aguarde até que as alterações sejam aplicadas e, em seguida, faça o download de um novo pacote de recuperação.
   a. Selecione **MAINTENANCE** > **System** > **Recovery package**.
   b. Introduza a **frase-passe de aprovisionamento**.

Configurar endereços IP

Diretrizes de endereço 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.

O procedimento de mudança de IP pode ser um procedimento disruptivo. Partes da grade podem estar indisponíveis até que a nova configuração seja aplicada.

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.

Se pretender alterar o endereço IP da rede de grelha para todos os nós da grelha, utilize o "procedimento especial para mudanças em toda a grade".

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 de cliente estiver contida em um grupo HA, você não poderá alterar o endereço IP da rede de 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.

Antes de começar

Você tem o `Passwords.txt` arquivo.

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:

- "Instale o StorageGRID no Red Hat Enterprise Linux"
- "Instale o StorageGRID no Ubuntu ou Debian"

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 "procedimento para configurar links de rede" .

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 "Configurando o SSO".

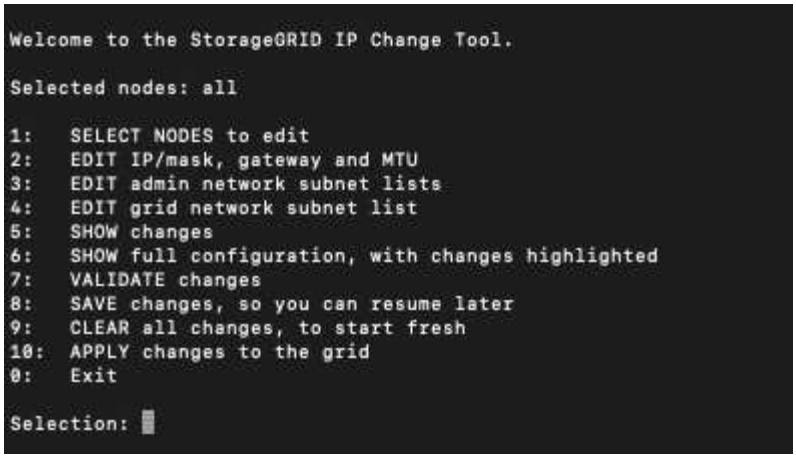
> Todas as alterações feitas na rede usando a ferramenta Change IP são propagadas para o firmware do instalador dos dispositivos StorageGRID. Dessa forma, se o software StorageGRID for reinstalado em um dispositivo ou se um dispositivo for colocado no modo de manutenção, a configuração de rede estará 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.



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 fazer a seleção, 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.

      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 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   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 sequências 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.

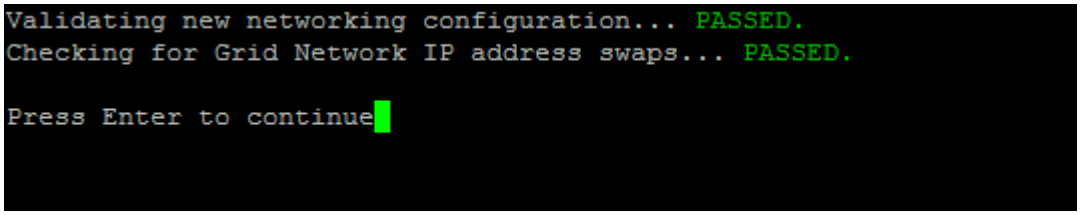
```
Validating new networking configuration... FAILED.

  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.



8. Após a aprovação da validação, 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.

   - **Cancel**: 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.

     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 alterar o estágio, um novo pacote de recuperação é gerado como resultado da

alteração de 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 Cliente pela primeira vez, certifique-se de que adicionou a interface conforme descrito em "Linux: Adicione interfaces ao nó existente".

    a. 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 aprovisionamento.

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.

Antes de começar

- Você tem o `Passwords.txt` arquivo.

Você pode adicionar, excluir ou alterar sub-redes para todos os nós na Lista de sub-redes de rede Admin.

Passos

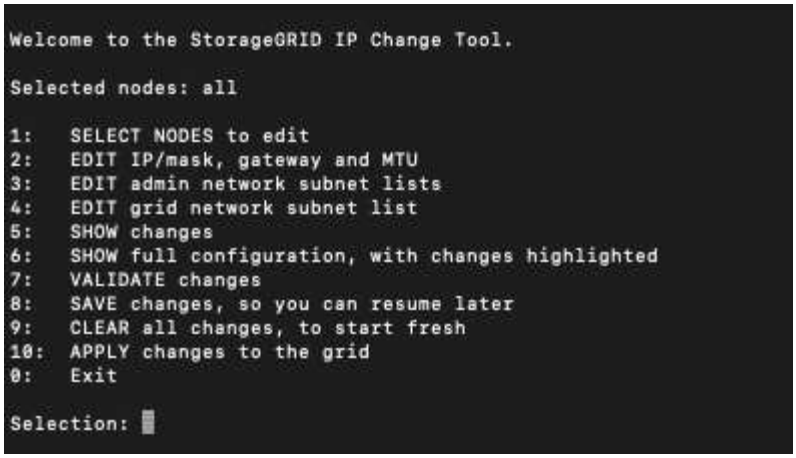
1. Faça login no nó de administração principal:

    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.



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" (todos) 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, pressione **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 aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't 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 don't 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 conetividade.

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 saída de exemplo a seguir:

      ```
      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 aprovisionamento.

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.

Antes de começar

- Você tem o `Passwords.txt` arquivo.

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 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. 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:

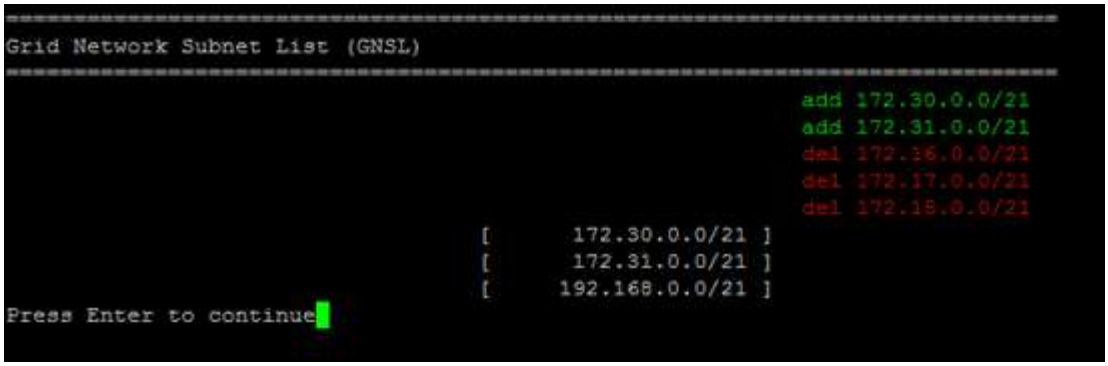
```
Editing: Grid Network Subnet List

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:



- 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 saída de exemplo a seguir:

      ```
      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**, reinicie o nó o mais rápido possível após o preparo para minimizar interrupções.

- **Cancel**: 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 alterar o estágio, um novo pacote de recuperação é gerado como resultado da alteração de configuração da grade.

12. Se a configuração for interrompida devido a erros, as seguintes opções estarão disponíveis:
    - Para terminar 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 aprovisionamento.

    > 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.

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.

Antes de começar

- Você tem o `Passwords.txt` arquivo.

Para garantir que a grade seja iniciada com sucesso, você deve fazer todas as alterações ao mesmo tempo.

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 ative Directory (AD FS) imediatamente após você alterar endereços IP. "Configurar o logon único"Consulte .

   Se necessário, adicione a nova sub-rede para os novos endereços IP.

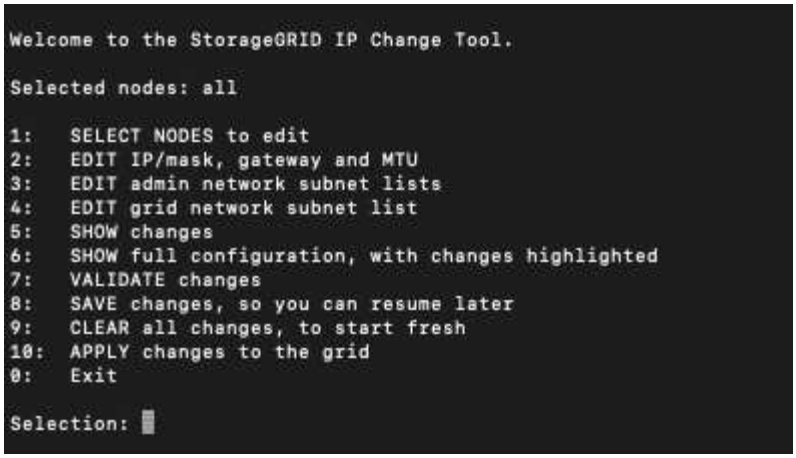
2. Faça login no nó de administração principal:

   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`.



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.

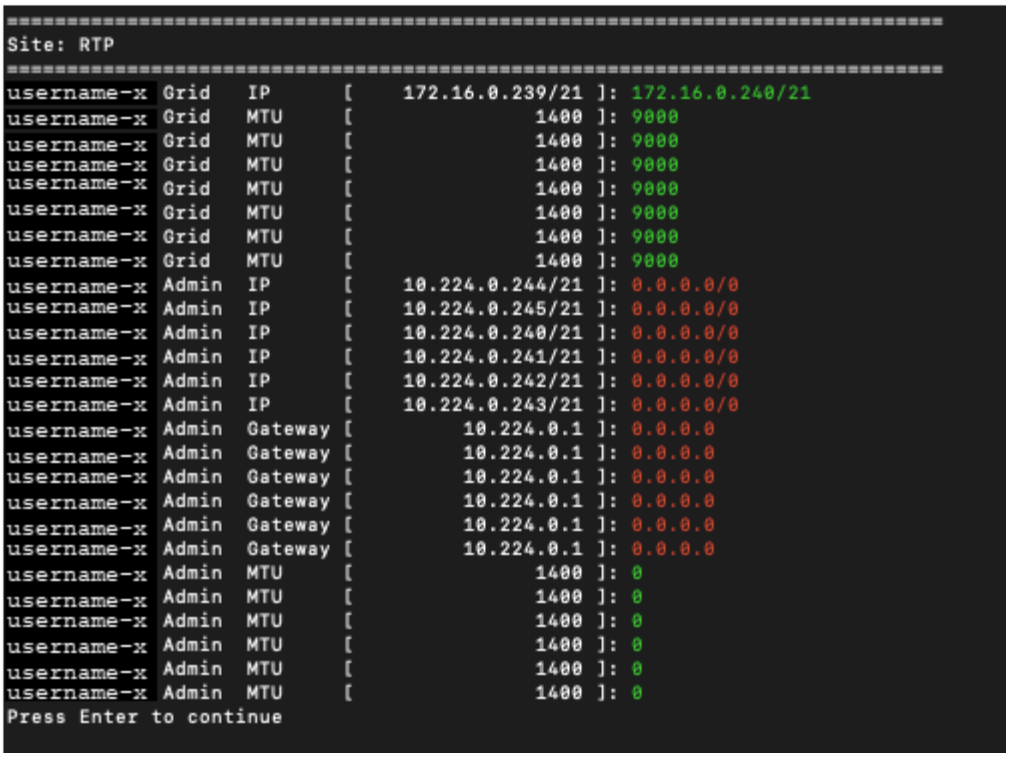
      Editar o endereço IP, o comprimento do prefixo, o gateway ou MTU de uma interface configurada por DHCP alterará a interface para estática. É apresentado um aviso antes de cada interface configurada pelo DHCP.

   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:



- **6**: Mostra edições na saída que exibe a configuração completa. As alterações são realçadas em verde (adições) ou vermelho (exclusões).

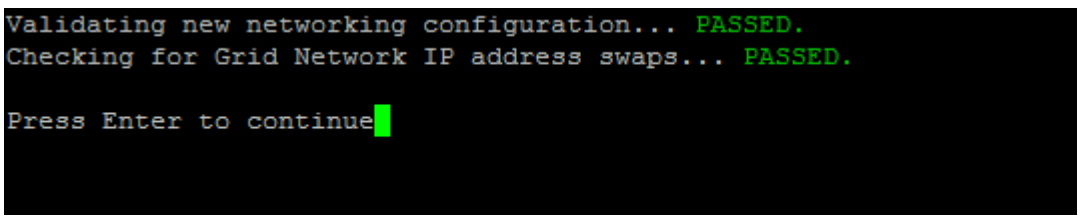
> Certas interfaces de linha de comando podem mostrar adições e exclusões usando a formatação strikethrough. A exibição adequada depende do cliente terminal que suporta as sequências de escape VT100 necessárias.

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.

   Neste exemplo, a validação passou.



8. Após a aprovação da validação, selecione **10** para aplicar a nova configuração de rede.
9. Selecione **stage** para aplicar as alterações na próxima vez que os nós forem reiniciados.

> Você deve selecionar **stage**. Não execute uma reinicialização contínua, manualmente ou selecionando **Apply** em vez de **stage**; a grade não será iniciada com êxito.

10. Depois que as alterações estiverem concluídas, selecione **0** para sair da ferramenta Change IP (alterar IP).
11. Encerre todos os nós simultaneamente.

> Toda a grade deve ser desligada, de modo que todos os nós estejam inativos ao mesmo tempo.

12. Faça as alterações de rede física ou virtual necessárias.
13. Verifique se todos os nós da grade estão inativos.
14. Potência em todos os nós.
15. Depois que a grelha for iniciada com sucesso:
    a. Se você adicionou novos servidores NTP, exclua os valores antigos do servidor NTP.
    b. Se você adicionou novos servidores DNS, exclua os valores antigos do servidor DNS.
16. Faça o download do novo Pacote de recuperação do Gerenciador de Grade.
    a. Selecione **MAINTENANCE** > **System** > **Recovery package**.
    b. Introduza a frase-passe de aprovisionamento.

Informações relacionadas

- "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 StorageGRID no Red Hat Enterprise Linux"
- "Instale o StorageGRID no 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 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.

Antes de começar

- Você tem acesso às instruções para instalar o StorageGRID em sua plataforma Linux.
  - "Instale o StorageGRID no Red Hat Enterprise Linux"
  - "Instale o StorageGRID no Ubuntu ou Debian"
- Você tem o `Passwords.txt` arquivo.
- Você "permissões de acesso específicas"tem .

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 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.

   `INTERFACE_TARGET_nnnn=value`

   Para *nnnn*, especifique um número exclusivo para cada `INTERFACE_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:

   `INTERFACE_TARGET_0001=ens256, Trunk`

   > Não especifique 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"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.

Antes de começar

- Tem acesso às instruções para "Instalando o StorageGRID em sua plataforma VMware".

- Você tem máquinas virtuais Admin Node e Gateway Node VMware.
- Você tem uma sub-rede de rede que não está sendo usada como rede de Grade, Admin ou rede de Cliente.
- Você tem o `Passwords.txt` arquivo.
- Você "permissões de acesso específicas"tem .

> Não tente adicionar interfaces a um nó enquanto uma atualização de software, procedimento de recuperação ou procedimento de expansão estiver ativo.

Sobre esta tarefa

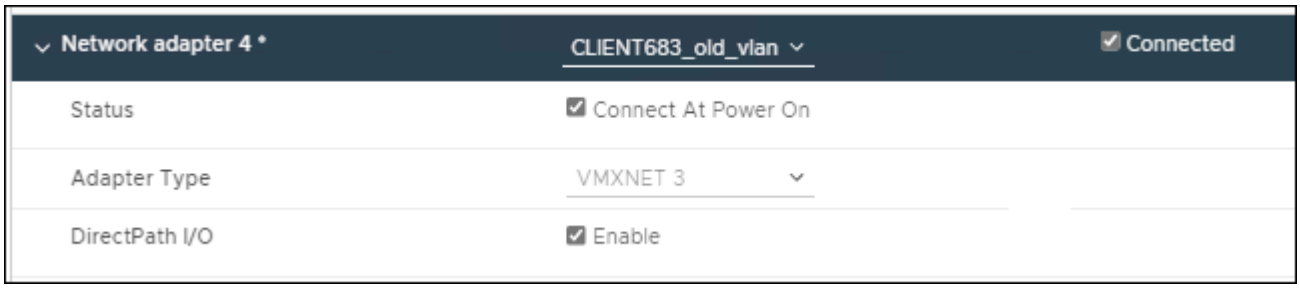
Siga estas etapas para adicionar uma ou mais interfaces extras a um nó VMware depois que o nó tiver sido instalado. Por exemplo, você pode querer adicionar uma interface de tronco a um Admin ou Gateway Node, para que você possa usar interfaces VLAN para segregar o tráfego que pertence a diferentes aplicativos 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**.



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"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, atualizar e remover servidores DNS, para que você possa usar nomes de host de nome de domínio totalmente qualificado (FQDN) em vez de endereços IP.

Para usar nomes de domínio totalmente qualificados (FQDNs) em vez de endereços IP ao especificar nomes de host para destinos externos, especifique o endereço IP de cada servidor DNS que você usará. Essas entradas são usadas para AutoSupport, e-mails de alerta, notificações SNMP, endpoints de serviços de plataforma, pools de armazenamento em nuvem e muito mais.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem os endereços IP dos servidores DNS para configurar.

Sobre esta tarefa

Para garantir o funcionamento correto, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três serão usados por causa das limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, pode "Personalize a lista de servidores DNS"usar um conjunto diferente de até três servidores DNS para nós individuais (normalmente todos os nós em um site).

Se possível, use servidores DNS que cada site pode acessar localmente para garantir que um site islanded

possa resolver os FQDNs para destinos externos.

Adicione um servidor DNS

Siga estas etapas para adicionar um servidor DNS.

Passos

1. Selecione **MAINTENANCE** > **Network** > **DNS Servers**.
2. Selecione **Adicionar outro servidor** para adicionar um servidor DNS.
3. Selecione **Guardar**.

Modifique um servidor DNS

Siga estas etapas para modificar um servidor DNS.

Passos

1. Selecione **MAINTENANCE** > **Network** > **DNS Servers**.
2. Selecione o endereço IP do nome do servidor que deseja editar e faça as alterações necessárias.
3. Selecione **Guardar**.

Eliminar um servidor DNS

Siga estas etapas para excluir um endereço IP de um servidor DNS.

Passos

1. Selecione **MAINTENANCE** > **Network** > **DNS Servers**.
2. Selecione o ícone de eliminação junto ao endereço IP.
3. Selecione **Guardar**.

Modifique a configuração DNS para um nó de grade único

Em vez de configurar o DNS 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 Grid Manager para configurar servidores DNS. Use o script a seguir somente se você precisar usar servidores DNS diferentes para diferentes nós de grade.

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 `#`.

   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`

Gerenciar 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.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento.
- Você tem os endereços IPv4 dos servidores NTP para configurar.

Como o StorageGRID usa o NTP

O sistema StorageGRID utiliza 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 conetam-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.

Diretrizes do servidor NTP

Siga estas diretrizes para proteger contra problemas de tempo:

- Os servidores NTP externos conetam-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, incluindo o StorageGRID. Para obter detalhes, "Limite de suporte para configurar o serviço de tempo do Windows para ambientes de alta precisão" consulte .

Configurar servidores NTP

Siga estas etapas para adicionar, atualizar ou remover servidores NTP.

Passos

1. Selecione **MAINTENANCE** > **Network** > **NTP Servers**.
2. Na seção servidores, adicione, atualize ou remova entradas do servidor NTP, conforme necessário.

   Você deve incluir pelo menos quatro servidores NTP e pode especificar até seis servidores.

3. Introduza a frase-passe de aprovisionamento do seu sistema StorageGRID e, em seguida, selecione **Guardar**.

   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.

Resolver problemas do servidor NTP

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.

Restaure a conetividade de rede para nós isolados

Em certas circunstâncias, um ou mais grupos de nós podem não ser capazes de entrar em Contato com o resto da grade. Por exemplo, alterações de endereço IP em todo o local ou grade podem resultar em nós isolados.

Sobre esta tarefa

O isolamento do nó é indicado por:

- Alertas, como **não é possível se comunicar com o nó** (**Alertas** > **atual**)
- Diagnósticos relacionados à conetividade (**SUPORTE** > **Ferramentas** > **Diagnóstico**)

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 painel do Gerenciador do locatário podem estar desatualizados. Os totais serão atualizados quando a conetividade 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, talvez seja necessário executar o utilitário de linha de comando em cada nó isolado.

Passos

Este procedimento não se aplica quando apenas alguns serviços estão offline ou a comunicar erros de comunicação.

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 might 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 estado do serviço IP dinâmico é "em execução" depois de executar o `storagegrid-status` comando.
   - Na página nós, 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 host e middleware

Linux: Migrar o nó de grade para o novo host

Você pode migrar um ou mais nós de StorageGRID de um host Linux (o *host de origem*) para outro host Linux (o *host de destino*) para executar a manutenção do host sem afetar a funcionalidade ou a disponibilidade da sua grade.

Por exemplo, você pode querer migrar um nó para executar patches de SO e reinicializar.

Antes de começar

- Você planejou a implantação do StorageGRID para incluir suporte à migração.
  - "Requisitos de migração de contêineres de nós para o Red Hat Enterprise Linux"
  - "Requisitos de migração de contentor de nó para Ubuntu ou Debian"
- O host de destino já está preparado para uso no StorageGRID.
- 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.

Exportar nó do host de origem

Como primeira etapa, encerre o nó de grade e exporte-o do host Linux de origem.

Execute os seguintes comandos no *source host*.

Passos

1. Obtenha o status de todos os nós atualmente em execução no host de origem.

   ```
   sudo storagegrid node status all
   ```

   Exemplo de saída:

```
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 estiver em execução.

   `sudo storagegrid node stop DC1-S3`

   Exemplo de saída:

```
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`

   Exemplo de saída:

```
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. Anote o `import` comando sugerido na saída.

   Você executará esse comando no host de destino na próxima etapa.

Importar nó no host de destino

Depois de exportar o nó do host de origem, importe e valide o nó no host 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 os seguintes comandos no *host de destino*.

Passos

1. Importe o nó no host de destino.

   `sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local`

   Exemplo de saída:

```
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
   ```

   Exemplo de saída:

   ```
   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.

   - "Instale o StorageGRID no Red Hat Enterprise Linux"
   - "Instale o StorageGRID no Ubuntu ou Debian"

Inicie o nó migrado

Depois de validar o nó migrado, você inicia o nó executando um comando no *host de destino*.

Passos

1. Inicie o nó no novo host.

   ```
   sudo storagegrid node start DC1-S3
   ```

2. Faça login no Gerenciador de Grade e verifique se o status do nó está verde sem alerta.

   > 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.

3. 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.

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.

Recuperar ou substituir nós

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.

> 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. "Como o suporte técnico recupera um site"Consulte .

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 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 "Verifique e atualize a versão do instalador do StorageGRID Appliance".
- Se você estiver recuperando um nó de grade diferente do nó Admin principal, há conetividade entre o nó de grade sendo recuperado e o nó Admin principal.
- Se você estiver recuperando um nó de armazenamento de dispositivo, especifique o mesmo tipo de armazenamento que o dispositivo original (combinado, somente metadados ou somente dados) durante a instalação do dispositivo. Se especificar um tipo de armazenamento diferente, a recuperação falhará e exigirá a reinstalação do dispositivo com o tipo de armazenamento correto especificado.

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	Se você precisa recuperar um nó de grade, você precisa Transfira os ficheiros de instalação do StorageGRID fazer isso para sua plataforma. **Observação:** você não precisa baixar arquivos se estiver recuperando volumes de armazenamento com falha em um nó de armazenamento.
Serviço de laptop	O computador portátil de serviço tem de ter o seguinte: • Porta de rede • Cliente SSH (por exemplo, PuTTY) • "Navegador da Web suportado"

Item	Notas
Arquivo do pacote de recuperação `.zip`	Obtenha uma cópia do arquivo mais recente do Pacote de recuperação `.zip`: `sgws-recovery-package-id-revision.zip` 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. Se o nó Admin principal estiver operando normalmente, você poderá fazer o download do Pacote de recuperação do Gerenciador de Grade. Selecione **MAINTENANCE** > **System** > **Recovery package**. 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: `/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg` Use o pacote de recuperação com o número de revisão mais alto.
`Passwords.txt` ficheiro	Contém as senhas necessárias para acessar os nós de grade na linha de comando. 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 `Passwords.txt` arquivo.
Documentação atual para a sua plataforma	Vá para o site do fornecedor da plataforma para obter documentação. Para obter as versões suportadas atuais da sua plataforma, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

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 Utilizador final, selecione a caixa de verificação e, em seguida, selecione **Accept & continue**.
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	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu ou Debian ou appliances	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.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 "Sistema Red Hat Enterprise Linux", 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.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL.
Ferramenta de script de implantação	Descrição

Caminho e nome do arquivo	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 `configure-storagegrid.py` 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. Você também pode usar este script para integração Ping federate.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.
	Exemplo de função do Ansible e manual de estratégia para configurar hosts do RHEL para implantação de contêineres do StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.
	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 `/debs/storagegrid-webscale-images-version-SHA.deb`.
	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. Você também pode usar este script para integração Ping federate.
	Um exemplo de arquivo de configuração para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` 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.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.

Caminho e nome do arquivo	Descrição
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.
	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.
	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 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.

Caminho e nome do arquivo	Descrição
	Um exemplo de arquivo de configuração para uso com o `deploy-vsphere-ovftool.sh` 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 entrar na API de Gerenciamento de Grade quando o logon único (SSO) está ativado. Você também pode usar este script para integração Ping federate.
	Um exemplo de arquivo de configuração para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único (SSO) está habilitado usando o ative Directory ou Ping federate.
	Um script auxiliar chamado pelo script Python complementar `storagegrid-ssoauth-azure.py` para executar interações SSO com o Azure.
	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.

Caminho e nome do arquivo	Descrição
	MD5 checksum para o arquivo `/debs/storagegridwebscale-images-version-SHA.deb`.

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 o suporte técnico recupera um site"
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 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 de nó de arquivo (StorageGRID 11,8 doc site)"

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

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
• 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. Isso inclui o caso em que um nó de storage falha enquanto a recuperação de outro nó de storage ainda está em andamento.	Entre em Contato com o suporte técnico.	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. O suporte técnico pode determinar quando é seguro iniciar a recuperação de um segundo nó de armazenamento. **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.
Mais de um nó de storage em um local falhou ou um local inteiro falhou.	Entre em Contato com o suporte técnico. Pode ser necessário executar um procedimento de recuperação do local.	O suporte técnico avaliará sua situação e desenvolverá um plano de recuperação. "Como o suporte técnico recupera um site"Consulte .
Um nó de storage de dispositivo falhou.	"Recupere o nó de storage do dispositivo"	O procedimento de recuperação para nós de storage do dispositivo é o mesmo para todas as falhas.
Um ou mais volumes de armazenamento falharam, mas a unidade do sistema está intacta	"Recuperar de uma falha no volume de armazenamento em que a unidade do sistema está intacta"	Este procedimento é usado para nós de storage baseados em software.
A unidade do sistema falhou.	"Recuperar de falha na unidade do sistema"	O procedimento de substituição do nó depende da plataforma de implantação e se algum volume de storage também falhou.

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 aparecer uma mensagem de erro indicando que a reparação falhou, execute o comando indicado na mensagem de erro.

Recupere o nó de storage do dispositivo

Avisos para recuperar os nós 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.

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. "Como o suporte técnico recupera um site"Consulte .

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.

Para procedimentos de manutenção de hardware, como instruções para substituir um controlador ou reinstalar o sistema operacional SANtricity, consulte "instruções de manutenção para o seu aparelho 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.

Passos

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.

   > Não tente acelerar a reinicialização desligando a alimentação ou reiniciando o aparelho. Você pode interromper atualizações automáticas de BIOS, BMC ou outras atualizações de firmware.

   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.

Antes de começar

- O dispositivo foi instalado em um rack, conetado 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 do seu dispositivo de armazenamento. "Início rápido para instalação de hardware"Consulte .
- 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 host (nome do sistema) do nó.
- Inicie a instalação e aguarde à medida que os volumes estão configurados e o software está instalado.

> Ao recuperar um nó de armazenamento de dispositivo, reinstale-o com o mesmo tipo de armazenamento que o dispositivo original (combinado, somente metadados ou somente dados). Se especificar um tipo de armazenamento diferente, a recuperação falhará e exigirá a reinstalação do dispositivo com o tipo de armazenamento correto especificado.

- 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.

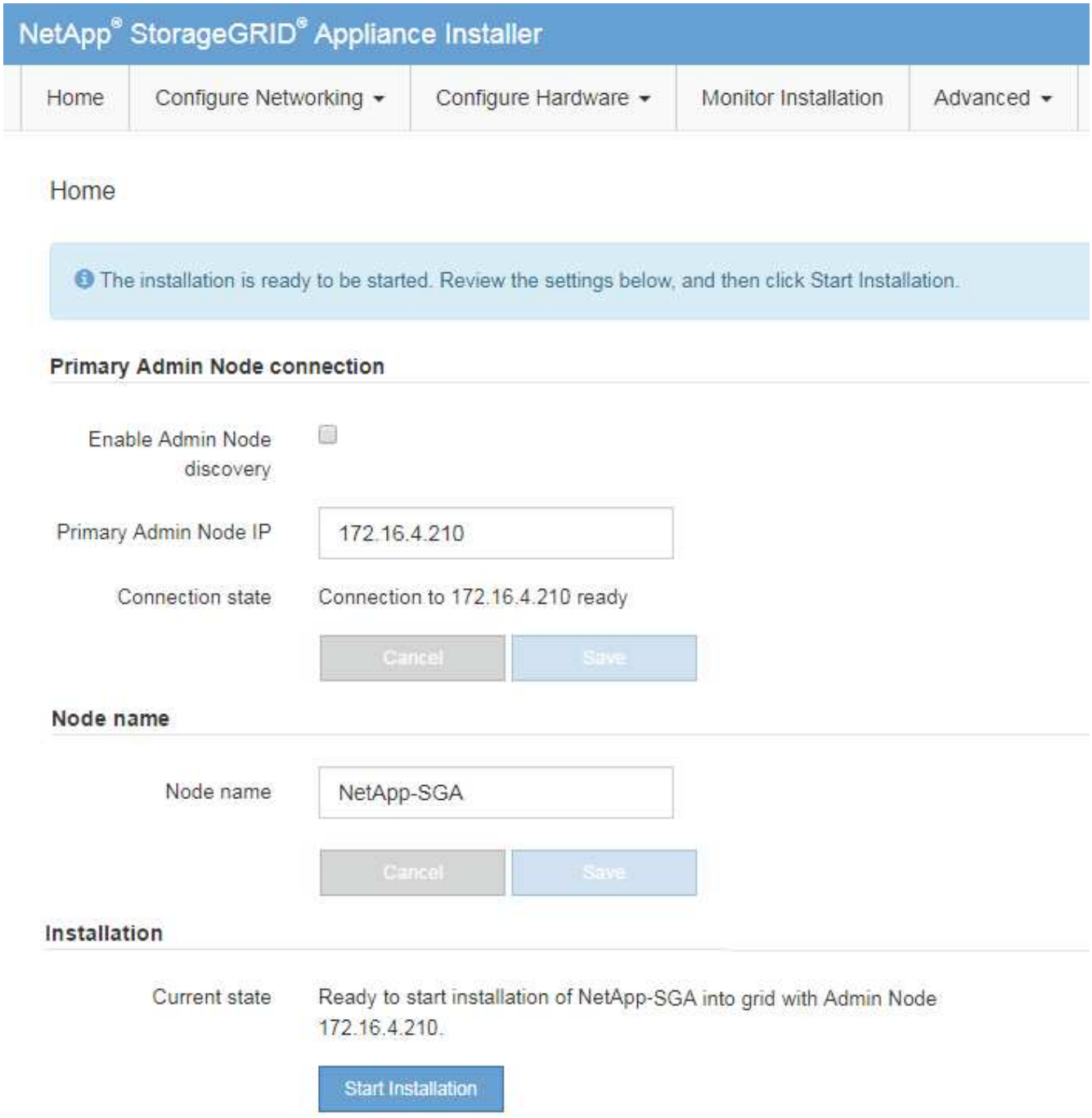
3. Se este endereço IP não for exibido ou você precisar alterá-lo, especifique o endereço:

Opção	Passos
Entrada de IP manual	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 conetados	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 de host (nome do sistema) 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 `node name` no grid com o nó Admin principal "*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 manutenção do seu aparelho.

6. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.



O estado atual muda para "a 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. "Monitore a instalação do dispositivo"Consulte .

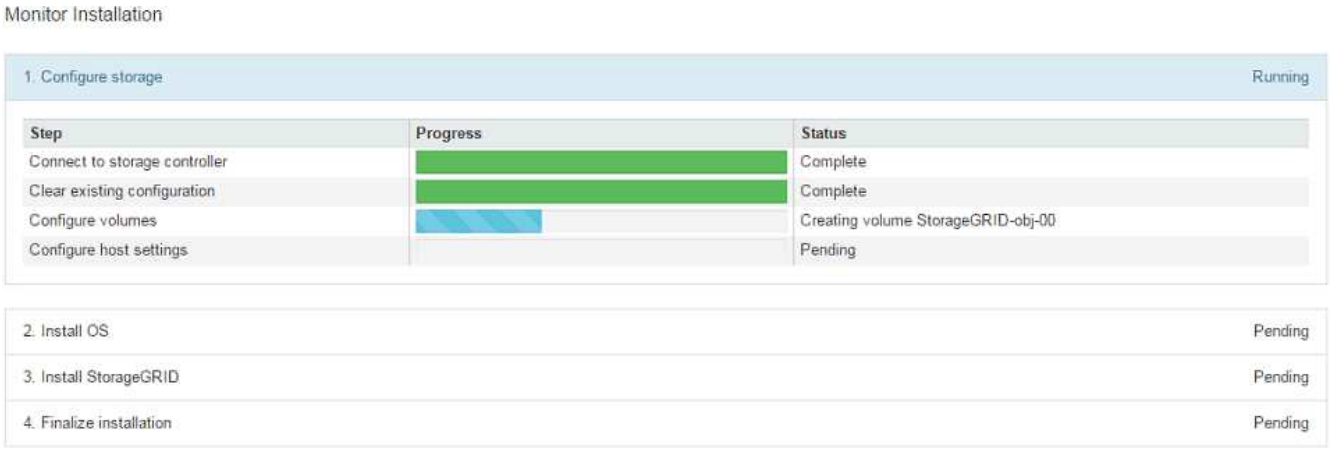
Monitore a instalação do dispositivo StorageGRID

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.

Passos

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.



   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 são mostradas com uma barra de status verde e um status de "ignorado".

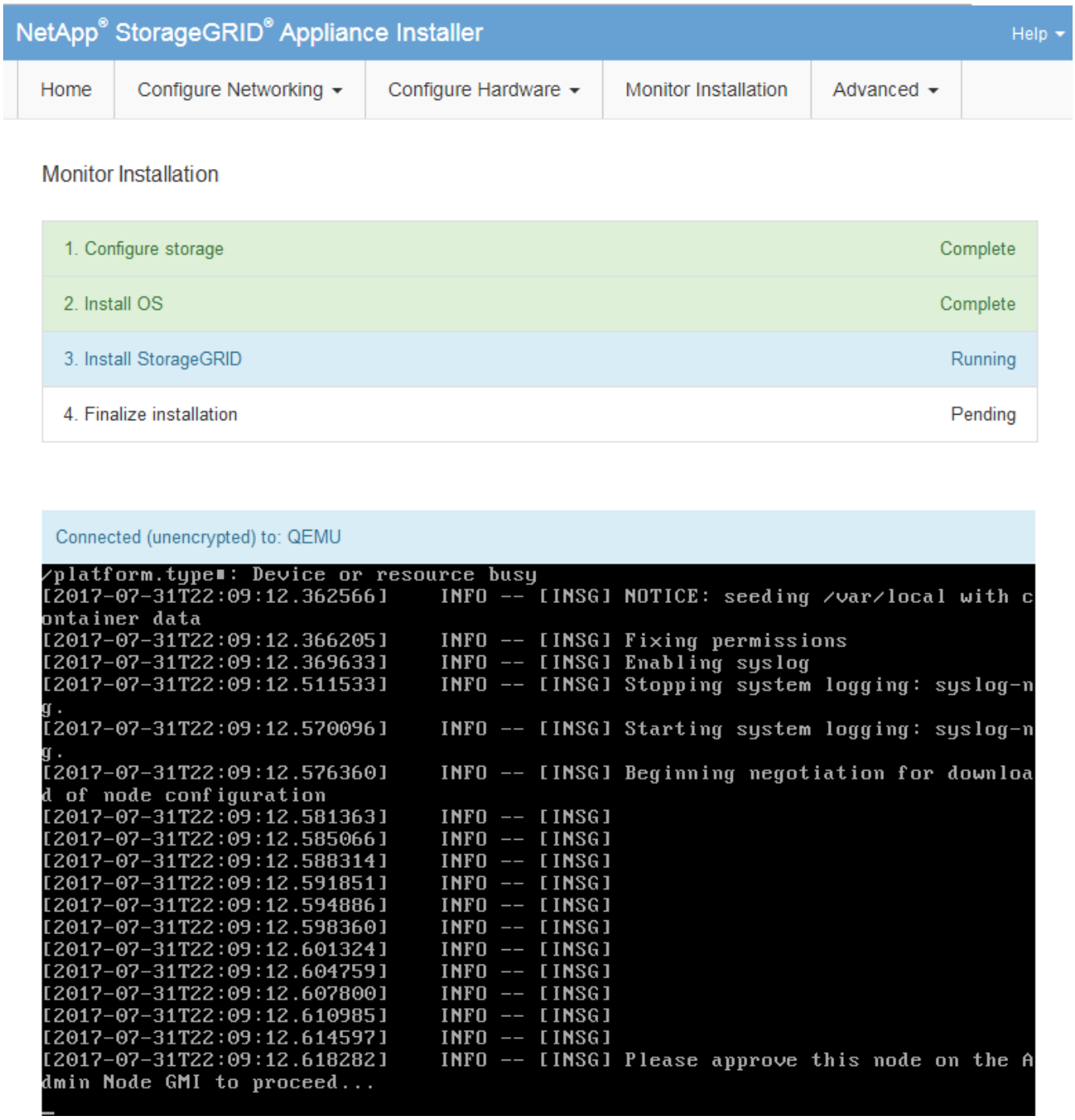
2. Reveja o progresso das duas primeiras fases de instalação.
   - **1. Configurar armazenamento**

     Durante essa etapa, o instalador se coneta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o SANtricity os 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.



4. Vá para "Selecione Iniciar recuperação 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.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento.

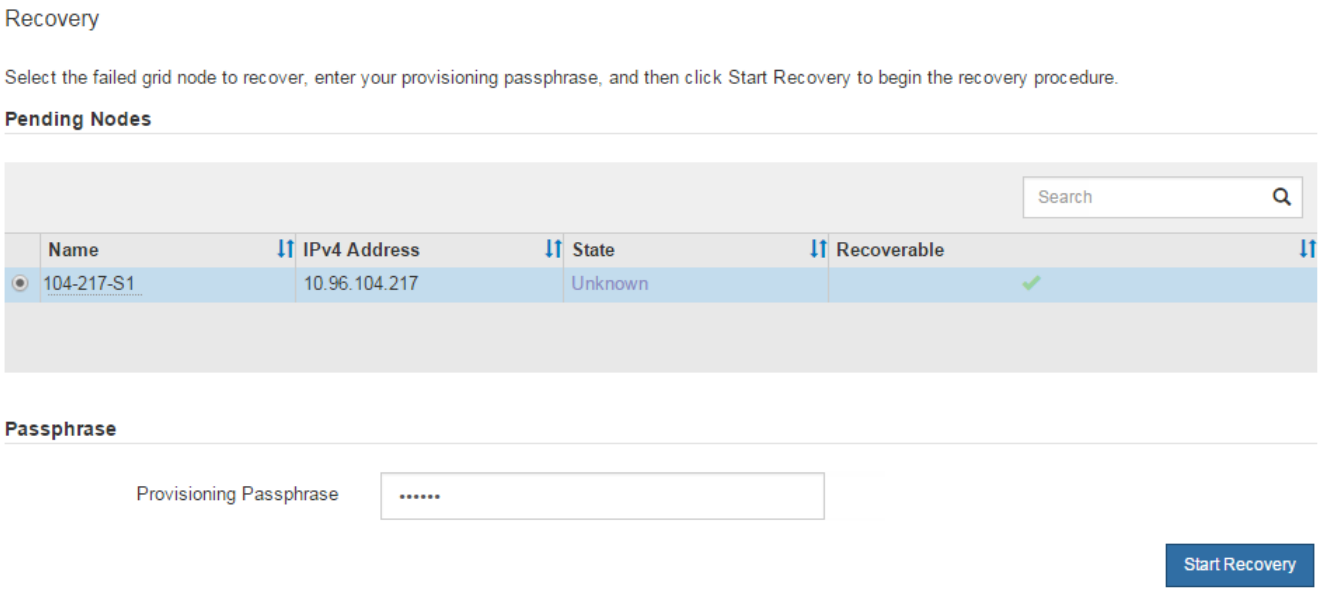
- Você implantou um nó de storage do dispositivo de recuperação.
- Tem a data de início de quaisquer trabalhos de reparação para dados codificados por apagamento.
- Você verificou que o nó de storage não foi reconstruído nos últimos 15 dias.

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.

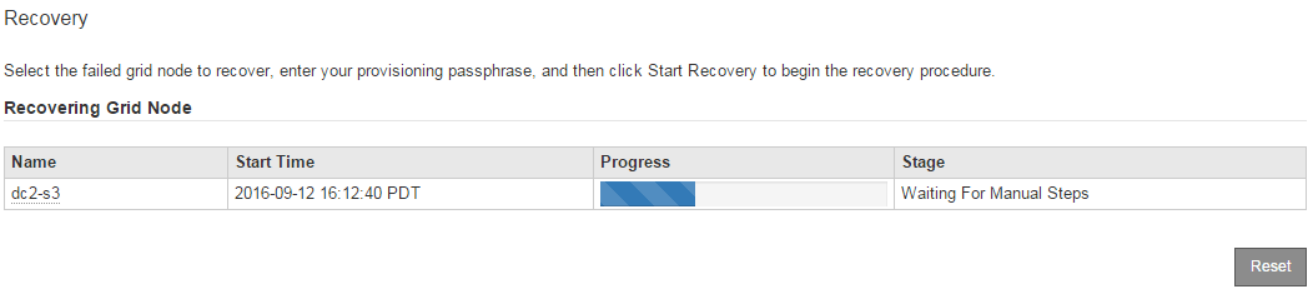
   Os nós aparecem na lista depois que eles falham, mas você não pode selecionar um nó até que ele seja reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de aprovisionamento**.
4. Clique em **Iniciar recuperação**.

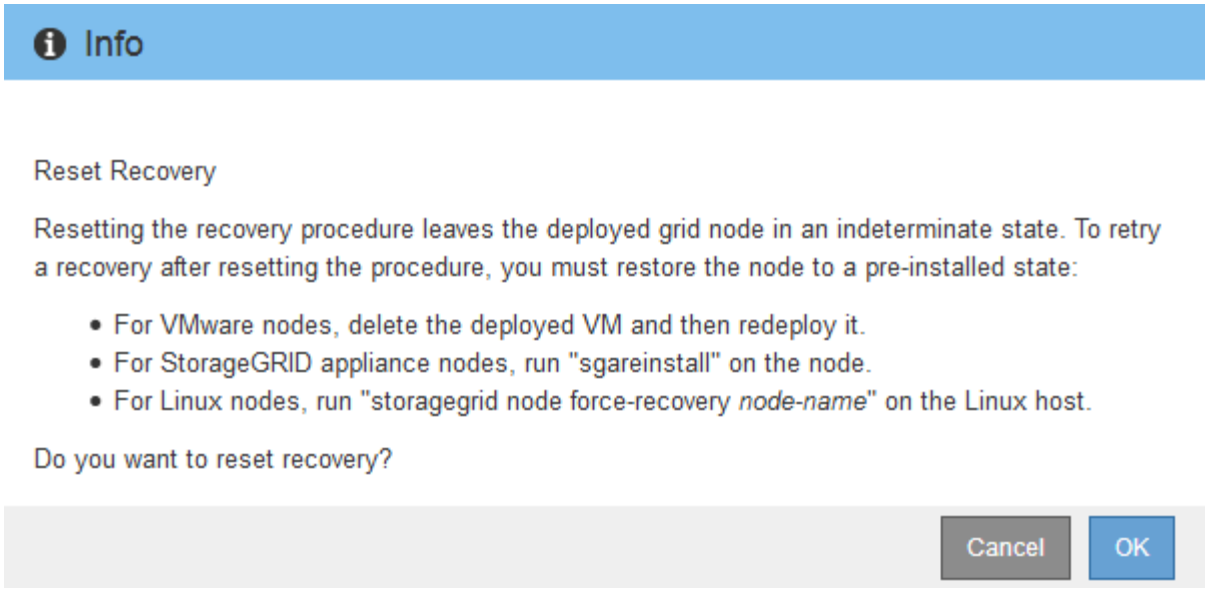


5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).

   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 storage do dispositivo.



A qualquer momento durante a recuperação, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.



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 reformatação 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.

Antes de começar

- 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 executar `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:
   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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't 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 conetado 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 conetado 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.

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:

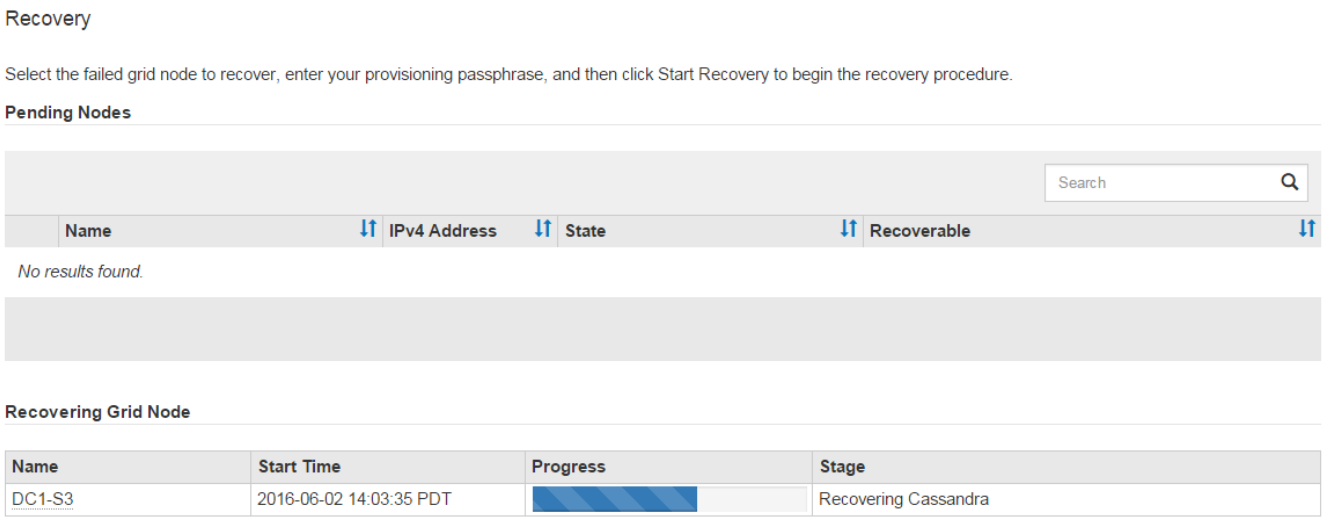
   - O script pode levar horas para ser executado.
   - Em geral, você deve deixar a sessão SSH sozinha enquanto o script estiver sendo executado.
   - Não pressione **Ctrl C** enquanto a sessão SSH estiver ativa.
   - O script será executado em segundo plano se ocorrer uma interrupção da rede e terminar 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 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 aparecer uma mensagem de erro indicando que a reparação 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.



6. Depois que o `sn-recovery-postinstall.sh` script iniciar os serviços no nó, você pode restaurar os dados do objeto para qualquer volume de armazenamento formatado pelo script.

   O script pergunta se você deseja usar o processo de restauração de volume do Gerenciador de Grade.

   - Na maioria dos casos, você deve "Restaure dados de objetos usando o Gerenciador de Grade". Resposta `y` para usar o Gerenciador de Grade.
   - Em casos raros, como quando instruído pelo suporte técnico ou quando você souber que o nó de substituição tem menos volumes disponíveis para storage de objetos do que o nó original, você deve "restaure os dados do objeto manualmente" usar o `repair-data` script. Se um desses casos se aplicar, responda `n`.

   > Se você responder `n` ao uso do processo de restauração de volume do Gerenciador de Grade (restaurar dados de objeto manualmente):
   >
   > - Não é possível restaurar dados de objetos usando o Gerenciador de Grade.
   > - Você pode monitorar o progresso dos trabalhos de restauração manual usando o Gerenciador de Grade.

   Depois de fazer sua seleção, o script é concluído e os próximos passos para recuperar dados de objeto são mostrados. Depois de rever estes passos, prima qualquer tecla para regressar à linha de comando.

Restaure os dados de objeto para o volume de storage do dispositivo

Depois de recuperar volumes de storage para o nó de storage do dispositivo, você pode restaurar os dados de objeto replicados ou codificados por apagamento que foram perdidos quando o nó de storage falhou.

Que procedimento devo utilizar?

Sempre que possível, restaure os dados do objeto usando a página **Restauração de volume** no Gerenciador de Grade.

- Se os volumes estiverem listados em **MAINTENANCE** > **volume restoration** > **nodes to restore**, restaure os dados do objeto usando o "Página de restauração de volume no Gerenciador de Grade".

- Se os volumes não estiverem listados em **MAINTENANCE** > **volume restoration** > **nodes to restore**, siga as etapas abaixo para usar o `repair-data` script para restaurar os dados do objeto.

  Se o nó de armazenamento recuperado contiver menos volumes do que o nó que está substituindo, você deve usar o `repair-data` script.

> O script repair-data está obsoleto e será removido em uma versão futura. Sempre que possível, utilize o "Procedimento de restauração de volume no Gerenciador de Grade".

Use o `repair-data` script para restaurar dados de objeto

Antes de começar

- Você confirmou 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 ou de um Cloud Storage Pool, supondo que as regras de ILM da grade tenham sido configuradas de modo que 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.

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.

> O script repair-data está obsoleto e será removido em uma versão futura. Sempre que possível, utilize o "Procedimento de restauração de volume no Gerenciador de Grade".

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
```

Dados codificados por 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
```

Você pode rastrear reparos de dados codificados por apagamento com este comando:

```
repair-data show-ec-repair-status
```

> As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. No entanto, se todos os dados codificados por apagamento não puderem ser contabilizados, o reparo não poderá ser concluído. O reparo será concluído depois que todos os nós estiverem disponíveis.

> 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 conetado 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, onde `--nodes` está o nome do host (nome do sistema), 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 do 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. "Investigue objetos perdidos"Consulte .

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção, onde `--nodes` está o nome do host (nome do sistema), para reparar todo o nó de armazenamento.

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 sua grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó (onde `--nodes` está o nome do host do 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 do 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. Observe a descrição do alerta e as ações recomendadas para determinar a causa da perda e se a recuperação é possível.

Dados codificados por 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 (onde `--nodes` está o nome do host do 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.

Também pode monitorizar o estado dos trabalhos de restauro de volume em processo e ver um histórico dos trabalhos de restauro concluídos no "Gerenciador de grade".

Dados replicados

- 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
  ```

- Para determinar se as reparações estão concluídas:
  a. Selecione **NODES** > ***Storage Node a ser reparado*** > **ILM**.
  b. Reveja os atributos na secção 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.

Dados codificados por 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.

Antes de começar

- Você está conetado 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

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.

> 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, utilize o procedimento do dispositivo: "Recupere o nó de storage do dispositivo".

Este procedimento de recuperação inclui as seguintes tarefas:

- "Reveja os avisos de recuperação do volume de armazenamento"
- "Identificar e desmontar volumes de storage com falha"
- "Recupere os volumes e reconstrua o banco de dados Cassandra"
- "Restaurar dados de objeto"
- "Verifique o estado de armazenamento"

Avisos para recuperação do volume de armazenamento

Antes de recuperar volumes de armazenamento com falha para um nó de armazenamento, reveja 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. "Como o suporte técnico recupera um site"Consulte .

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.

Informações relacionadas

"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.

Antes de começar

Você está conetado 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 detetar 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 detetar 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 conete 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. Depois de um volume ter 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 UUUID 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

1. Execute as etapas a seguir para gravar os volumes de armazenamento com falha e os nomes de seus dispositivos:

   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.

   b. 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

   c. 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
/	croot	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

2. 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 seguinte script para desmontar um volume de armazenamento 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 o serviço Cassandra dependendo do volume de armazenamento 0.

   > Se o serviço Cassandra já estiver parado, você não será solicitado. O serviço Cassandra é interrompido apenas para o volume 0.

   ```
   root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
   Services depending on storage volume 0 (cassandra) aren't down.
   Services depending on storage volume 0 must be stopped before running
   this script.
   Stop services that require storage volume 0 [y/N]? y
   Shutting down services that require storage volume 0.
   Services requiring storage volume 0 stopped.
   Unmounting /var/local/rangedb/0
   /var/local/rangedb/0 is unmounted.
   ```

   Em alguns segundos, o volume é desmontado. As mensagens são exibidas indicando cada etapa do processo. A mensagem final indica que o volume está desmontado.

5. Se a desmontagem falhar porque o volume está ocupado, você pode forçar uma desmontagem usando a `--use-umountof` opção:

Forçar uma desmontagem usando a `--use-umountof` opção pode fazer com que processos ou serviços que usam o volume se comportem inesperadamente ou travem.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

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.

Antes de começar

- Você tem o `Passwords.txt` arquivo.
- As unidades de sistema no servidor estão intactas.
- A causa da falha foi identificada e, se necessário, o hardware de armazenamento de substituição já foi adquirido.
- O tamanho total do armazenamento de substituição é 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 .

Passos

1. Conforme necessário, substitua o armazenamento físico ou virtual com falha associado aos volumes de armazenamento com falha identificados e desmontados anteriormente.

   Não remonte os volumes nesta etapa. O armazenamento é remontado e adicionado em `/etc/fstab` um passo posterior.

2. No Gerenciador de Grade, vá para **NÓS `appliance Storage Node`** > **hardware**. Na seção StorageGRID Appliance da página, verifique se o modo RAID de armazenamento está funcionando.
3. 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 `#`.

4. 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.

5. Reformate quaisquer volumes de armazenamento com falha e reconstrua o banco de dados Cassandra, se necessário. Introduza: `reformat_storage_block_devices.rb`

   - Quando o volume de armazenamento 0 estiver desmontado, os prompts e as mensagens indicarão que o serviço Cassandra está sendo interrompido.
   - 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 aparecer uma mensagem de erro indicando que a reparação 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
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 b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

Depois que os volumes de armazenamento forem reformatados e remontados e as operações necessárias do Cassandra estiverem concluídas, você poderá "Restaure dados de objetos usando o Gerenciador de Grade".

Restaure os dados de objetos para o volume de storage em que a unidade do sistema esteja intacta

Depois de recuperar um volume de storage em um nó de storage em que a unidade do sistema está intacta, você pode restaurar os dados de objetos replicados ou codificados por apagamento que foram perdidos quando o volume de storage falhou.

Que procedimento devo utilizar?

Sempre que possível, restaure os dados do objeto usando a página **Restauração de volume** no Gerenciador de Grade.

- Se os volumes estiverem listados em **MAINTENANCE** > **volume restoration** > **nodes to restore**, restaure os dados do objeto usando o "Página de restauração de volume no Gerenciador de Grade".
- Se os volumes não estiverem listados em **MAINTENANCE** > **volume restoration** > **nodes to restore**, siga as etapas abaixo para usar o `repair-data` script para restaurar os dados do objeto.

  Se o nó de armazenamento recuperado contiver menos volumes do que o nó que está substituindo, você deve usar o `repair-data` script.

> ⓘ O script repair-data está obsoleto e será removido em uma versão futura. Sempre que possível, utilize o "Procedimento de restauração de volume no Gerenciador de Grade".

Use o `repair-data` script para restaurar dados de objeto

Antes de começar

- Você confirmou 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 ou de um Cloud Storage Pool, supondo que as regras de ILM da grade tenham sido configuradas de modo que 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.

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.

O script repair-data está obsoleto e será removido em uma versão futura. Sempre que possível, utilize o "Procedimento de restauração de volume no Gerenciador de Grade".

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
```

Dados codificados por 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
```

Você pode rastrear reparos de dados codificados por apagamento com este comando:

```
repair-data show-ec-repair-status
```

> As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. No entanto, se todos os dados codificados por apagamento não puderem ser contabilizados, o reparo não poderá ser concluído. O reparo será concluído depois que todos os nós estiverem disponíveis.

> 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 conetado 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, onde `--nodes` está o nome do host (nome do sistema), 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 do 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. "Investigue objetos perdidos"Consulte .

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção, onde `--nodes` está o nome do host (nome do sistema), para reparar todo o nó de armazenamento.

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 sua grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó (onde `--nodes` está o nome do host do 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 do 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. Observe a descrição do alerta e as ações recomendadas para determinar a causa da perda e se a recuperação é possível.

Dados codificados por 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 (onde `--nodes` está o nome do host do 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.

Também pode monitorizar o estado dos trabalhos de restauro de volume em processo e ver um histórico dos trabalhos de restauro concluídos no "Gerenciador de grade".

Dados replicados

- 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
  ```

- Para determinar se as reparações estão concluídas:
  a. Selecione **NODES** > ***Storage Node a ser reparado*** > **ILM**.
  b. Reveja os atributos na secção 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.

Dados codificados por 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.

Antes de começar

- Você está conetado 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

Avisos para recuperação da unidade do sistema Storage Node

Antes de recuperar uma unidade de sistema com falha de um nó de armazenamento, reveja os avisos gerais "avisos e considerações para a recuperação do nó da grade" e específicos a seguir.

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. "Como o suporte técnico recupera um site"Consulte .

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 de uma falha no volume 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.

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. Deve seguir um procedimento diferente para "Recupere um 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 "Substituindo 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.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento.
- Você implantou e configurou o nó de substituição.
- Tem a data de início de quaisquer trabalhos de reparação para dados codificados por apagamento.
- Você verificou que 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:

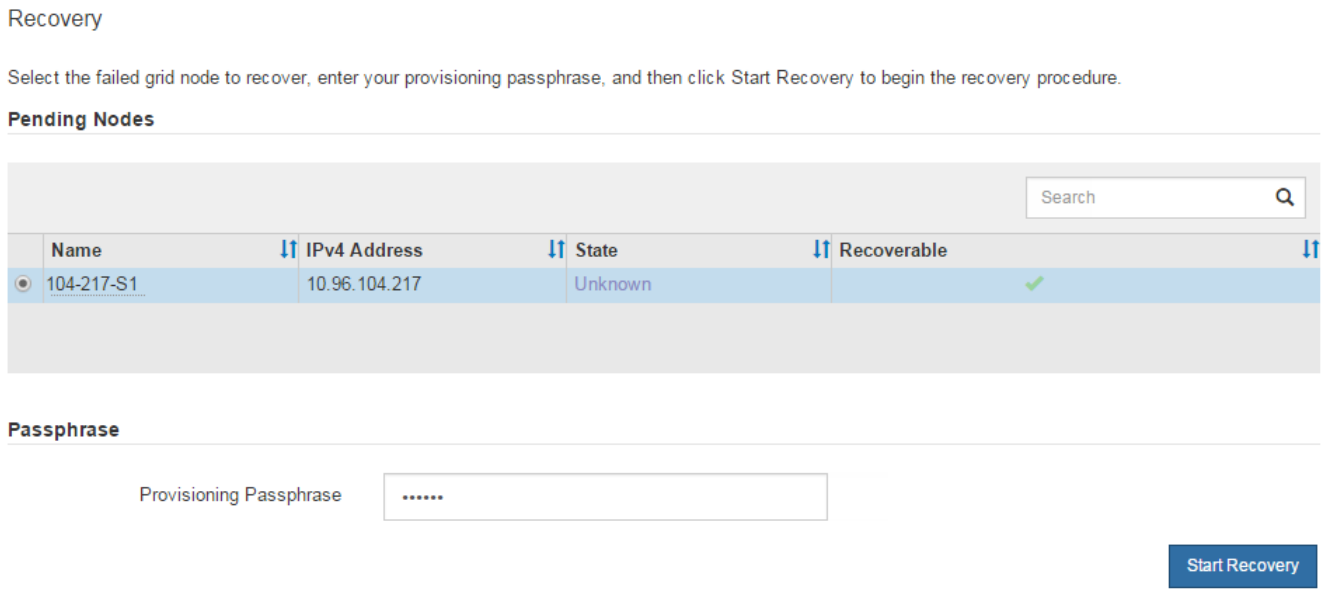
- Você teve que usar o `--force` sinalizador para importar o nó, ou você emitiu `storagegrid node force-recovery` *`node-name`*
- Você teve que fazer uma reinstalação completa do nó, ou você precisava restaurar /var/local.

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.

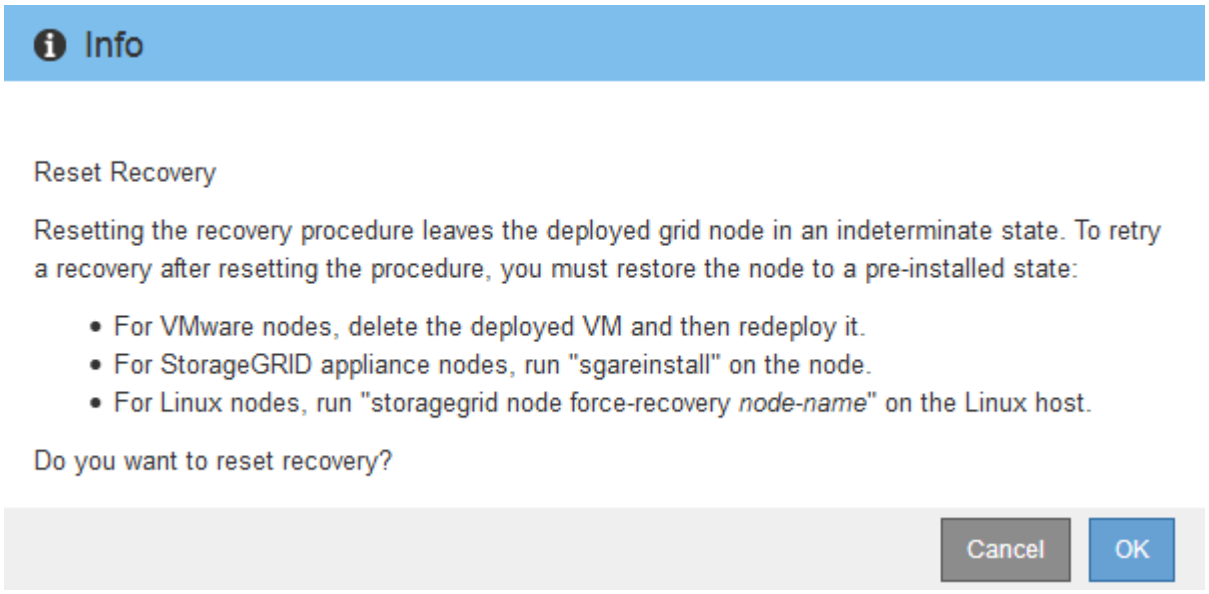
   Os nós aparecem na lista depois que eles falham, mas você não pode selecionar um nó até que ele seja reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de aprovisionamento**.
4. Clique em **Iniciar recuperação**.



5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).

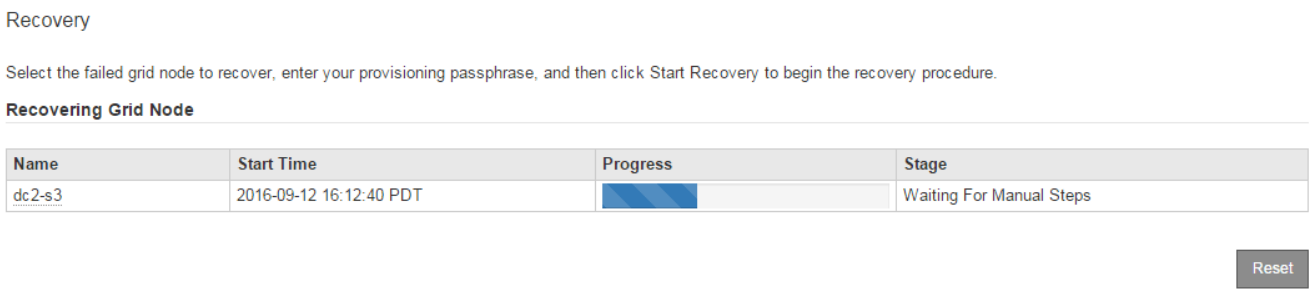
> Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.



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 "Remontagem e reformatação de volumes de storage (etapas manuais)".



Remontagem e reformatação de 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.

Antes de começar

- 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 armazenamento 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't 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 conetado 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 conetado 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 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:

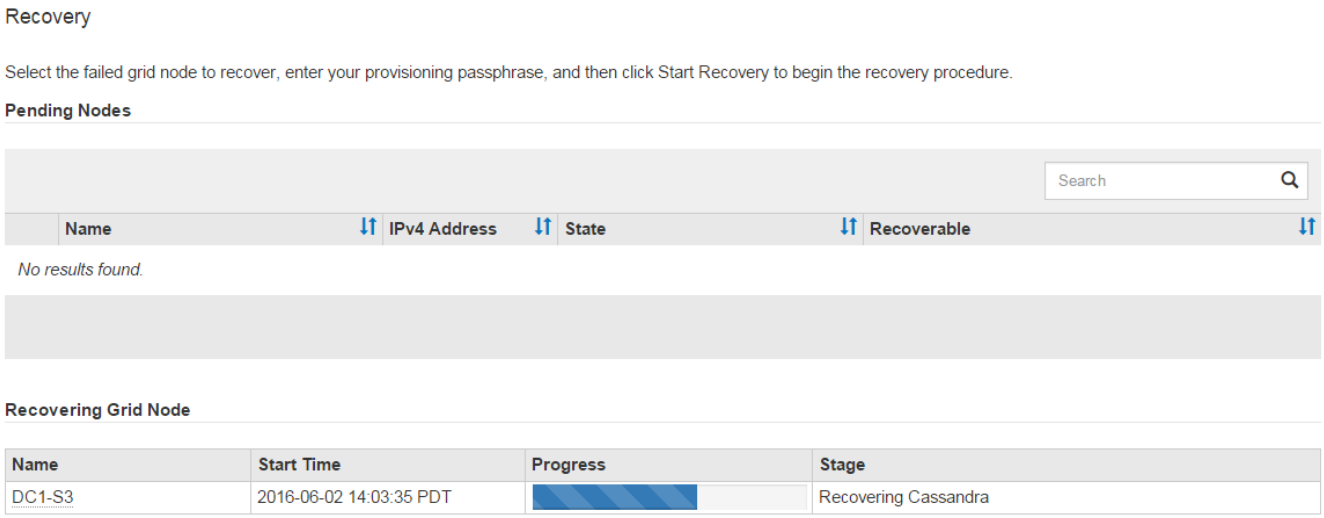
   - O script pode levar horas para ser executado.
   - Em geral, você deve deixar a sessão SSH sozinha enquanto o script estiver sendo executado.
   - Não pressione **Ctrl C** enquanto a sessão SSH estiver ativa.
   - O script será executado em segundo plano se ocorrer uma interrupção da rede e terminar 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 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 aparecer uma mensagem de erro indicando que a reparação 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.



6. Depois que o `sn-recovery-postinstall.sh` script iniciar os serviços no nó, você pode restaurar os dados do objeto para qualquer volume de armazenamento formatado pelo script.

   O script pergunta se você deseja usar o processo de restauração de volume do Gerenciador de Grade.

   - Na maioria dos casos, você deve "Restaure dados de objetos usando o Gerenciador de Grade". Resposta `y` para usar o Gerenciador de Grade.
   - Em casos raros, como quando instruído pelo suporte técnico ou quando você souber que o nó de substituição tem menos volumes disponíveis para storage de objetos do que o nó original, você deve "restaure os dados do objeto manualmente" usar o `repair-data` script. Se um desses casos se aplicar, responda `n`.

   > Se você responder `n` ao uso do processo de restauração de volume do Gerenciador de Grade (restaurar dados de objeto manualmente):
   >
   > - Não é possível restaurar dados de objetos usando o Gerenciador de Grade.
   > - Você pode monitorar o progresso dos trabalhos de restauração manual usando o Gerenciador de Grade.

   Depois de fazer sua seleção, o script é concluído e os próximos passos para recuperar dados de objeto são mostrados. Depois de rever estes passos, prima qualquer tecla para regressar à linha de comando.

Restaurar dados de objetos para o volume de storage (falha na unidade do sistema)

Depois de recuperar volumes de storage para um nó de storage que não seja do dispositivo, você pode restaurar os dados de objeto replicados ou codificados por apagamento que foram perdidos quando o nó de storage falhou.

Que procedimento devo utilizar?

Sempre que possível, restaure os dados do objeto usando a página **Restauração de volume** no Gerenciador de Grade.

- Se os volumes estiverem listados em **MAINTENANCE** > **volume restoration** > **nodes to restore**, restaure os dados do objeto usando o "Página de restauração de volume no Gerenciador de Grade".

- Se os volumes não estiverem listados em **MAINTENANCE** > **volume restoration** > **nodes to restore**, siga as etapas abaixo para usar o `repair-data` script para restaurar os dados do objeto.

  Se o nó de armazenamento recuperado contiver menos volumes do que o nó que está substituindo, você deve usar o `repair-data` script.

> O script repair-data está obsoleto e será removido em uma versão futura. Sempre que possível, utilize o "Procedimento de restauração de volume no Gerenciador de Grade".

Use o `repair-data` script para restaurar dados de objeto

Antes de começar

- Você confirmou 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 ou de um Cloud Storage Pool, supondo que as regras de ILM da grade tenham sido configuradas de modo que 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.

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.

> O script repair-data está obsoleto e será removido em uma versão futura. Sempre que possível, utilize o "Procedimento de restauração de volume no Gerenciador de Grade".

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
```

Dados codificados por 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
```

Você pode rastrear reparos de dados codificados por apagamento com este comando:

```
repair-data show-ec-repair-status
```

> As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. No entanto, se todos os dados codificados por apagamento não puderem ser contabilizados, o reparo não poderá ser concluído. O reparo será concluído depois que todos os nós estiverem disponíveis.

> 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 conetado 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, onde `--nodes` está o nome do host (nome do sistema), 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 do 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. "Investigue objetos perdidos"Consulte .

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção, onde `--nodes` está o nome do host (nome do sistema), para reparar todo o nó de armazenamento.

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 sua grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó (onde `--nodes` está o nome do host do 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 do 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. Observe a descrição do alerta e as ações recomendadas para determinar a causa da perda e se a recuperação é possível.

Dados codificados por 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 (onde `--nodes` está o nome do host do 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.

Também pode monitorizar o estado dos trabalhos de restauro de volume em processo e ver um histórico dos trabalhos de restauro concluídos no "Gerenciador de grade".

Dados replicados

- 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
  ```

- Para determinar se as reparações estão concluídas:
  a. Selecione **NODES** > ***Storage Node a ser reparado*** > **ILM**.
  b. Reveja os atributos na secção 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.

Dados codificados por 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.

Antes de começar

- Você está conetado 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.

Restaure dados de objetos usando o Gerenciador de Grade

Você pode restaurar dados de objeto para um volume de armazenamento ou nó de armazenamento com falha usando o Grid Manager. Você também pode usar o Gerenciador de Grade para monitorar os processos de restauração em andamento e exibir um histórico de restauração.

Antes de começar

- Você concluiu um destes procedimentos para formatar volumes com falha:
  - "Remontagem e reformatação dos volumes de storage do dispositivo (etapas manuais)"
  - "Remontagem e reformatação de volumes de storage (etapas manuais)"
- Você confirmou que o nó de armazenamento onde você está restaurando objetos tem um estado de conexão de **Connected** na guia **NODES** > **Overview** no Gerenciador de Grade.
- Você confirmou o seguinte:
  - Uma expansão de grade para adicionar um nó de storage não está em processo.
  - A desativação de um nó de storage não está em processo ou falhou.
  - A recuperação de um volume de armazenamento com falha não está em processo.
  - Uma recuperação de um nó de armazenamento com uma unidade de sistema com falha não está em processo.
  - Um trabalho de reequilíbrio EC não está em processo.
  - A clonagem do nó do dispositivo não está em processo.

Sobre esta tarefa

Depois de substituir as unidades e executar as etapas manuais para formatar os volumes, o Gerenciador de Grade exibe os volumes como candidatos para restauração na guia **MAINTENANCE** > **volume restoration** > **Nodes to restore**.

Sempre que possível, restaure os dados do objeto usando a página de restauração de volume no Gerenciador de Grade. Você pode ativar o modo de restauração automáticainiciar automaticamente a restauração de volume quando os volumes estiverem prontos para serem restaurados ou realize manualmente a restauração do volume. Siga estas diretrizes:

- Se os volumes estiverem listados em **MAINTENANCE** > **volume restoration** > **nodes to restore**, restaure os dados do objeto conforme descrito nas etapas abaixo. Os volumes serão listados se:
  - Alguns, mas não todos, volumes de armazenamento em um nó falharam
  - Todos os volumes de storage em um nó falharam e estão sendo substituídos pelo mesmo número de volumes ou mais volumes

  A página de restauração de volume no Gerenciador de Grade também permite que monitorize o processo de restauro do volumevocê e veja o histórico de restauração.
- Se os volumes não estiverem listados no Gerenciador de Grade como candidatos à restauração, siga as etapas apropriadas para usar o `repair-data` script para restaurar dados de objeto:
  - "Restauração de dados de objetos para o volume de armazenamento (falha na unidade do sistema)"
  - "Restaure os dados de objetos para o volume de storage em que a unidade do sistema esteja intacta"

- "Restaure os dados de objeto para o volume de storage do dispositivo"

  > O script repair-data está obsoleto e será removido em uma versão futura.

  Se o nó de armazenamento recuperado contiver menos volumes do que o nó que está substituindo, você deve usar o `repair-data` script.

Você pode restaurar dois tipos de dados de objeto:

- Os objetos de dados replicados são restaurados de outros locais, supondo que as regras de ILM da grade foram configuradas para disponibilizar cópias de objetos.
  - 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.
- Os objetos de dados codificados por apagamento (EC) são restaurados pela remontagem dos fragmentos armazenados. Fragmentos corrompidos ou perdidos são recriados pelo algoritmo de codificação de apagamento a partir dos dados restantes e fragmentos de paridade.

  As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. No entanto, se todos os dados codificados por apagamento não puderem ser contabilizados, a reparação não poderá ser concluída. O reparo será concluído depois que todos os nós estiverem disponíveis.

> A restauração de volume depende da disponibilidade de recursos onde as cópias de objetos são armazenadas. O progresso da restauração de volume é não linear e pode levar dias ou semanas para ser concluído.

ative o modo de restauração automática

Quando ativa o modo de restauro automático, a restauração do volume é iniciada automaticamente quando os volumes estão prontos para serem restaurados.

Passos

1. No Grid Manager, vá para **MAINTENANCE** > **volume restoration**.
2. Selecione a guia **nós a restaurar** e deslize a alternância para **modo de restauração automática** para a posição ativada.
3. Quando a caixa de diálogo de confirmação for exibida, revise os detalhes.

> - Você não poderá iniciar trabalhos de restauração de volume manualmente em nenhum nó.
> - As restaurações por volume só começarão automaticamente quando não houver outros procedimentos de manutenção em andamento.
> - Pode monitorizar o estado do trabalho a partir da página de monitorização do progresso.
> - O StorageGRID tenta novamente restaurações de volume automaticamente que não são iniciadas.

4. Quando entender os resultados da ativação do modo de restauração automática, selecione **Sim** na caixa de diálogo de confirmação.

   Você pode desativar o modo de restauração automática a qualquer momento.

restaure manualmente o volume ou nó com falha

Siga estas etapas para restaurar um volume ou nó com falha.

Passos

1. No Grid Manager, vá para **MAINTENANCE** > **volume restoration**.
2. Selecione a guia **nós a restaurar** e deslize a alternância para **modo de restauração automática** para a posição desativada.

   O número na guia indica o número de nós com volumes que exigem restauração.

3. Expanda cada nó para ver os volumes de TI que precisam de restauração e seu status.
4. Corrija quaisquer problemas que impeçam a restauração de cada volume. Os problemas serão indicados quando selecionar **aguardando etapas manuais**, se for exibido como o status do volume.
5. Selecione um nó para restaurar onde todos os volumes indicam um status Pronto para restaurar.

   Você só pode restaurar os volumes para um nó de cada vez.

   Cada volume no nó deve indicar que está pronto para ser restaurado.

6. Selecione **Iniciar restauração**.
7. Aborde quaisquer avisos que possam aparecer ou selecione **Iniciar de qualquer maneira** para ignorar os avisos e iniciar a restauração.

Os nós são movidos da guia **nós para restaurar** para a guia **progresso da restauração** quando a restauração é iniciada.

Se uma restauração de volume não puder ser iniciada, o nó retornará à guia **nós para restaurar**.

Ver o progresso da restauração

A guia **progresso da Restauração** mostra o status do processo de restauração de volume e informações sobre os volumes de um nó que está sendo restaurado.

As taxas de reparo de dados para objetos replicados e codificados por apagamento em todos os volumes são médias que resumem todas as restaurações em processo, incluindo as restaurações iniciadas com `repair-data` o script. A porcentagem de objetos nesses volumes que estão intactos e não requerem restauração também é indicada.

> ⓘ A restauração de dados replicados depende da disponibilidade de recursos onde as cópias replicadas são armazenadas. O progresso da restauração de dados replicados é não linear e pode levar dias ou semanas para ser concluído.

A seção Restoration Jobs (tarefas de restauração) exibe informações sobre restaurações de volume iniciadas no Grid Manager.

- O número no cabeçalho da seção trabalhos de restauração indica o número de volumes que estão sendo

restaurados ou enfileirados para restauração.

- A tabela exibe informações sobre cada volume em um nó que está sendo restaurado e seu progresso.
  - O progresso de cada nó exibe a porcentagem de cada trabalho.
  - Expanda a coluna Detalhes para exibir a hora de início da restauração e o ID do trabalho.
- Se uma restauração de volume falhar:
  - A coluna Status indica `failed (attempting retry)`, e será tentada novamente automaticamente.
  - Se vários trabalhos de restauro falharem, o trabalho mais recente será novamente tentado automaticamente primeiro.
  - O alerta **EC repair failure** é acionado se as tentativas continuarem falhando. Siga as etapas no alerta para resolver o problema.

Ver histórico de restauro

A guia **Histórico de Restauração** mostra informações sobre todas as restaurações de volume concluídas com êxito.

> Os tamanhos não são aplicáveis a objetos replicados e são exibidos apenas para restaurações que contêm objetos de dados codificados por apagamento (EC).

Monitorizar trabalhos de reparação de dados

Você pode monitorar o status dos trabalhos de reparo usando o `repair-data` script da linha de comando.

Estas incluem tarefas iniciadas manualmente ou trabalhos iniciados automaticamente pelo StorageGRID como parte de um procedimento de desativação.

> Em vez disso, se estiver a executar trabalhos de restauro de volume"Monitore o progresso e visualize um histórico desses trabalhos no Gerenciador de Grade".

Monitore o status das `repair-data` tarefas com base se você usa **dados replicados**, **dados codificados por apagamento (EC)** ou ambos.

Dados replicados

- 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
  ```

- Para determinar se as reparações estão concluídas:
  a. Selecione **NODES** > ***Storage Node a ser reparado*** > **ILM**.
  b. Reveja os atributos na secção 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.

Dados codificados por 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
   ```

Recuperar de falhas no Admin Node

Recuperação do nó de administração primário ou não primário

O processo de recuperação para um nó Admin depende se é o nó Admin primário ou um nó Admin não primário.

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.

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

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.

Você deve reparar ou substituir imediatamente um nó de administração principal com falha 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.

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.

Siga estas etapas de alto nível para recuperar um nó de administração principal:

1. "Copiar registos de auditoria do nó de administração principal avariado"
2. "Substitua o nó de administração principal"
3. "Configure o nó de administração principal de substituição"
4. "Determine se há um requisito de hotfix para o nó de administração primário recuperado"
5. "Restaure o log de auditoria no nó de administração primário recuperado"
6. "Restaure o banco de dados Admin Node ao recuperar um Admin Node primário"
7. "Restaure as métricas do Prometheus ao recuperar um nó de administração principal"

Copiar registos 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.

Sobre esta tarefa

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.

Passos

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. Navegue até o diretório de exportação de auditoria:

   ```
   cd /var/local/log
   ```

4. Renomeie o arquivo de origem `audit.log` para um nome de arquivo numerado exclusivo. Por exemplo, renomeie o arquivo audit.log para `2023-10-25.txt.1`.

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```

5. Reinicie o serviço AMS: `service ams start`
6. 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.

7. Copie todos os arquivos de log de auditoria para o local temporário: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Quando solicitado, insira a senha para admin.

8. 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"

Plataforma de substituição	Procedimento
Aparelhos de serviços	"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 "Substituindo um nó Linux".

Configure o nó de administração principal de substituição

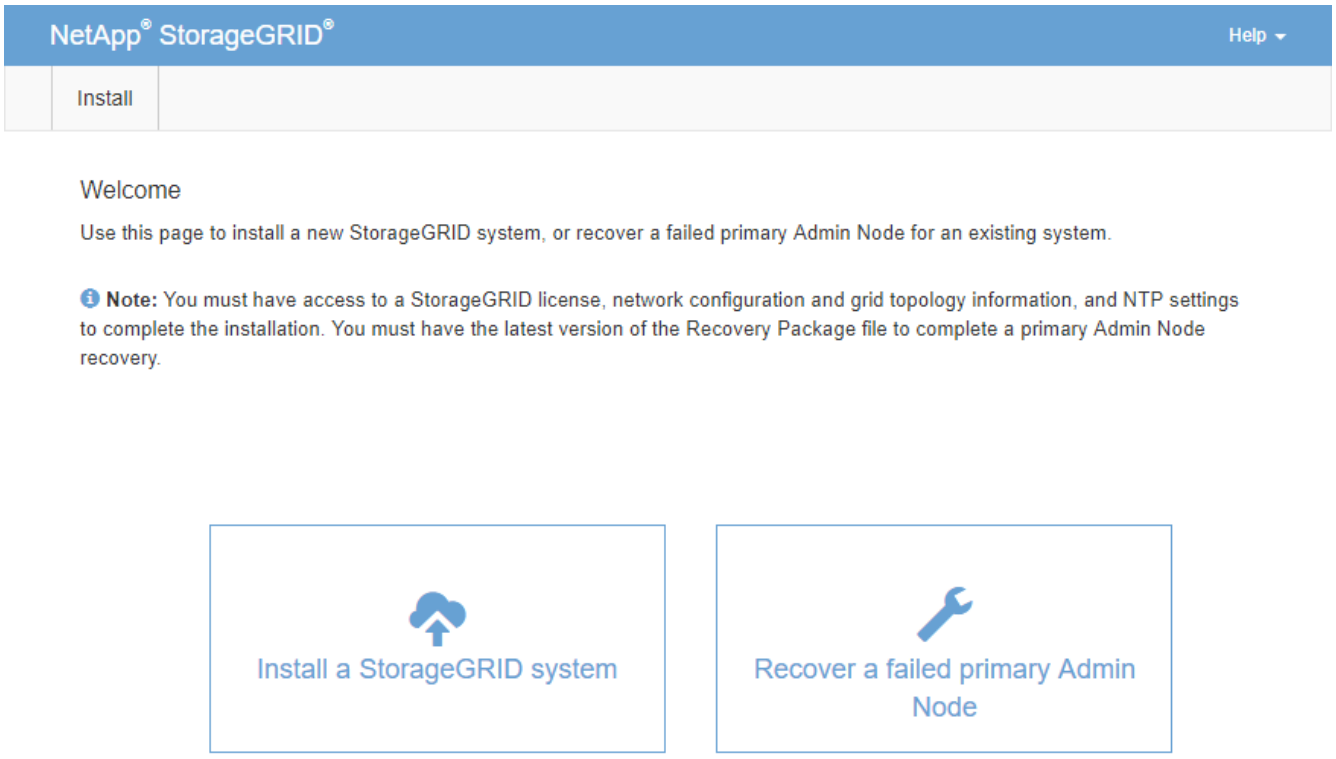
O nó de substituição deve ser configurado como nó de administração principal para o seu sistema StorageGRID.

Antes de começar

- Para nós de administração primários hospedados em máquinas virtuais, a máquina virtual foi implantada, ativada e inicializada.
- Para nós de administração primários hospedados em um dispositivo de serviços, você substituiu o dispositivo e instalou o software. Consulte "instruções de instalação para o seu aparelho" .
- Tem a cópia de segurança mais recente do ficheiro do pacote de recuperação (`sgws-recovery-package-id-revision.zip`).
- Você tem a senha de provisionamento.

Passos

1. Abra o navegador da Web e navegue até `https://primary_admin_node_ip`.
2. Gerencie uma senha temporária do instalador conforme necessário:
   - Se já tiver sido definida uma palavra-passe utilizando um destes métodos, introduza a palavra-passe para prosseguir.
     - Um usuário define a senha ao acessar o instalador anteriormente
     - Para sistemas bare metal, a senha foi importada automaticamente do arquivo de configuração do nó em `/etc/storagegrid/nodes/<node_name>.conf`
     - Para VMs, a senha SSH/console foi importada automaticamente das propriedades OVF
   - Se não tiver sido definida uma palavra-passe, defina opcionalmente uma palavra-passe para proteger o instalador do StorageGRID.
3. Clique em **Recover a failed Primary Admin Node** (recuperar um nó de administrador principal principal)



4. 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**.
5. Introduza a frase-passe de aprovisionamento.
6. 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.

7. 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, "Configurar o logon único"consulte . 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.

Depois de recuperar um nó de administrador principal, "determine se você precisa aplicar um hotfix".

Determine o requisito de hotfix para o nó de administração principal

Depois de recuperar um nó de administrador principal, determine se você precisa aplicar um hotfix.

Antes de começar

A recuperação do nó de administrador principal está concluída.

Passos

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Selecione **NODES**.
3. Na lista à esquerda, selecione o nó de administração principal.
4. Na guia Visão geral, observe a versão exibida no campo **versão do software**.
5. Selecione qualquer outro nó de grade.
6. 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 deverá "aplique um hotfix"atualizar o nó de administração principal recuperado para a mesma versão.

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.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- Você copiou os logs de auditoria para outro local depois que o nó Admin original falhou.

Sobre esta tarefa

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/log`
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`

Restaure o banco de dados do nó de administração ao recuperar o nó de administração primário

Se você quiser manter as informações históricas sobre atributos 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.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

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
- Dados de atributos históricos, que são usados em gráficos de estilo legado na página de nós

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 Admin Node.

> 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.

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 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`

Restaure 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.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

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 de administração principal, não será possível restaurar o banco 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.

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. 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

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.

Siga estas etapas de alto nível para recuperar um nó de administração não primário:

1. "Copiar registos de auditoria do nó de administração não primário com falha"
2. "Substitua o nó de administração não primário"
3. "Selecione Iniciar recuperação para configurar o nó de administração não primário"
4. "Restaure o log de auditoria em um nó de administração não primário recuperado"
5. "Restaure o banco de dados Admin Node ao recuperar um Admin Node não primário"
6. "Restaure as métricas do Prometheus ao recuperar um nó de administração não primário"

Copiar registos 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. Navegue até o diretório de exportação de auditoria:

   ```
   cd /var/local/log
   ```
4. Renomeie o arquivo audit.log de origem para um nome de arquivo numerado exclusivo. Por exemplo, renomeie o arquivo audit.log para `2023-10-25.txt.1`.

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```
5. Reinicie o serviço AMS: `service ams start`
6. 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.
7. Copie todos os arquivos de log de auditoria para o local temporário: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Quando solicitado, insira a senha para admin.
8. 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	"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 "Substituindo 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.

Antes de começar

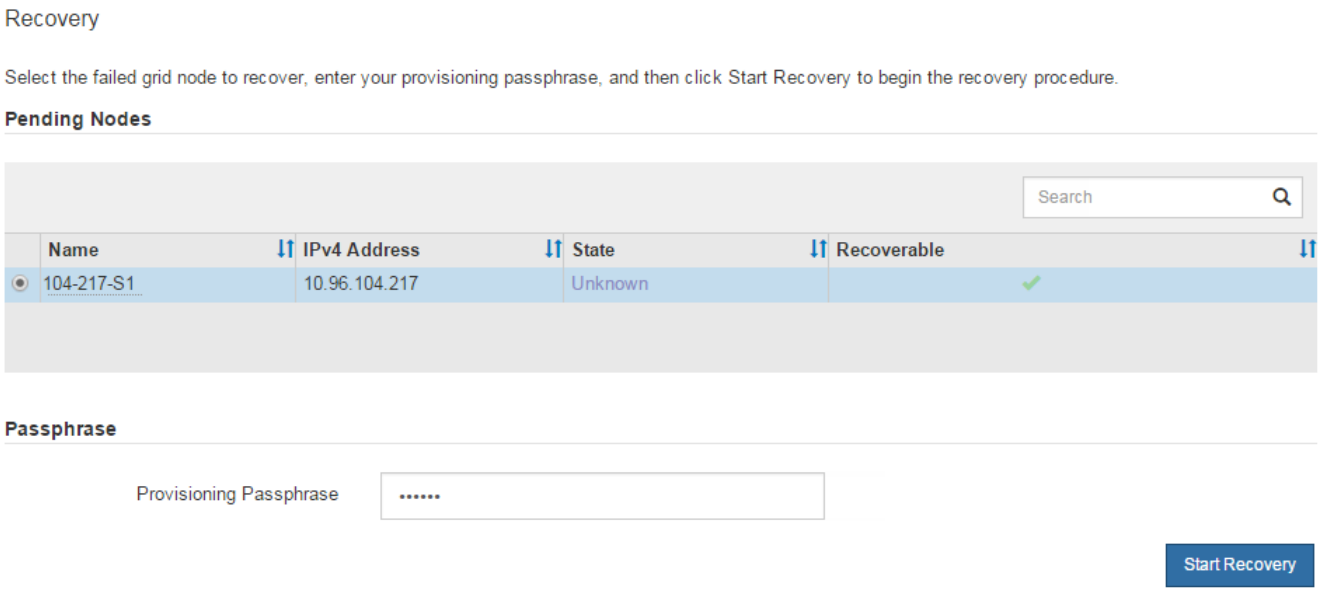
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento.
- Você implantou e configurou o nó de substituição.

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.

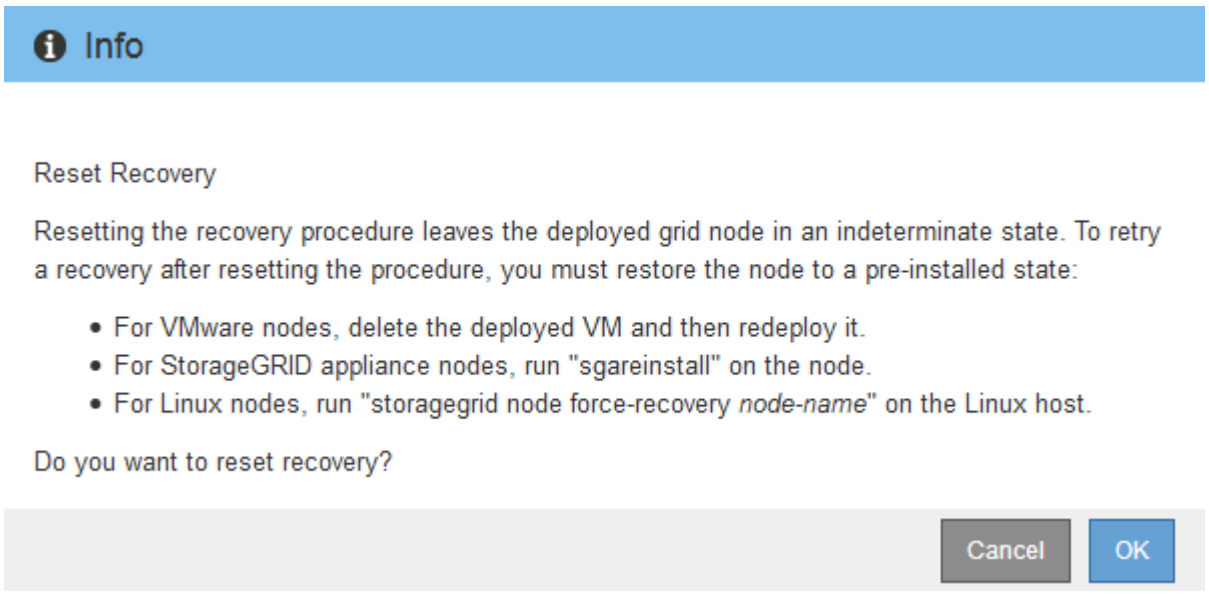
   Os nós aparecem na lista depois que eles falham, mas você não pode selecionar um nó até que ele seja reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de aprovisionamento**.
4. Clique em **Iniciar recuperação**.



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 é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.



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. "Prepare o aparelho para reinstalação (apenas substituição da plataforma)"Consulte .

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, "Configurar o logon único"consulte . 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.

Restaure 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.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- Você copiou os logs de auditoria para outro local depois que o nó Admin original falhou.

Sobre esta tarefa

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/log
```

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`

Restaure o banco de dados Admin Node ao recuperar o nó Admin não primário

Se você quiser manter as informações históricas sobre atributos 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.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

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
- Dados de atributos históricos, que são usados em gráficos de estilo legado na página de nós

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.

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. 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`

Restaure 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.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

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.

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. 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

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"
Aparelhos de serviços	"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 "Substituindo 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.

Antes de começar

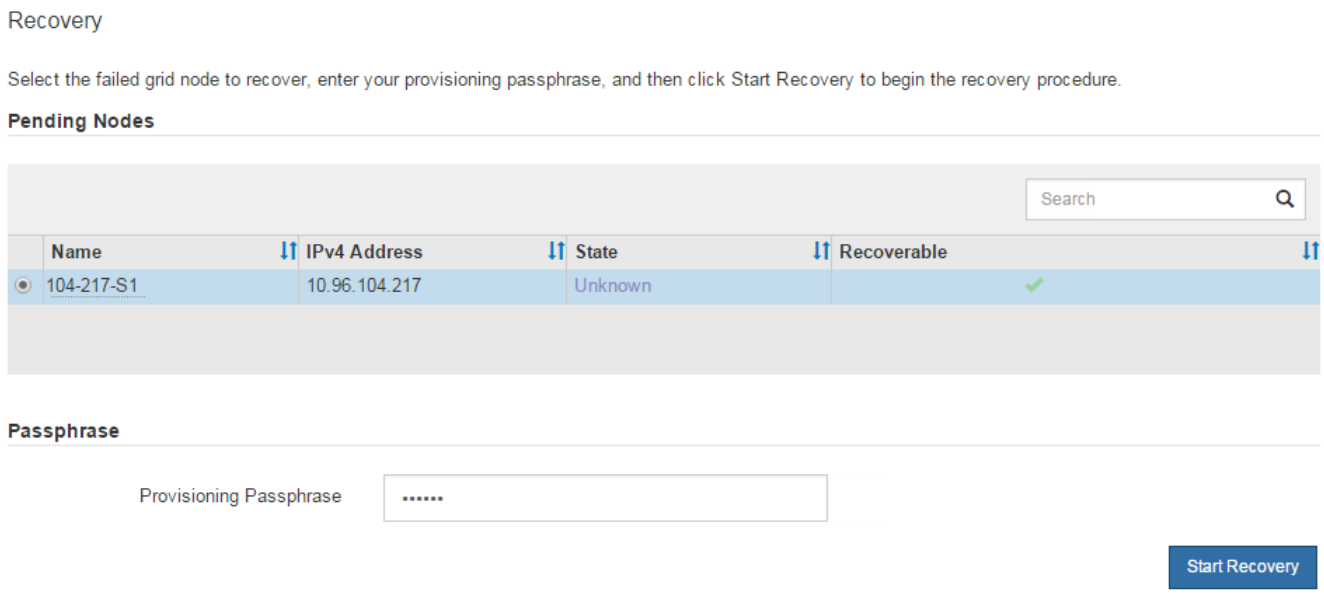
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você tem a senha de provisionamento.
- Você implantou e configurou o nó de substituição.

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.

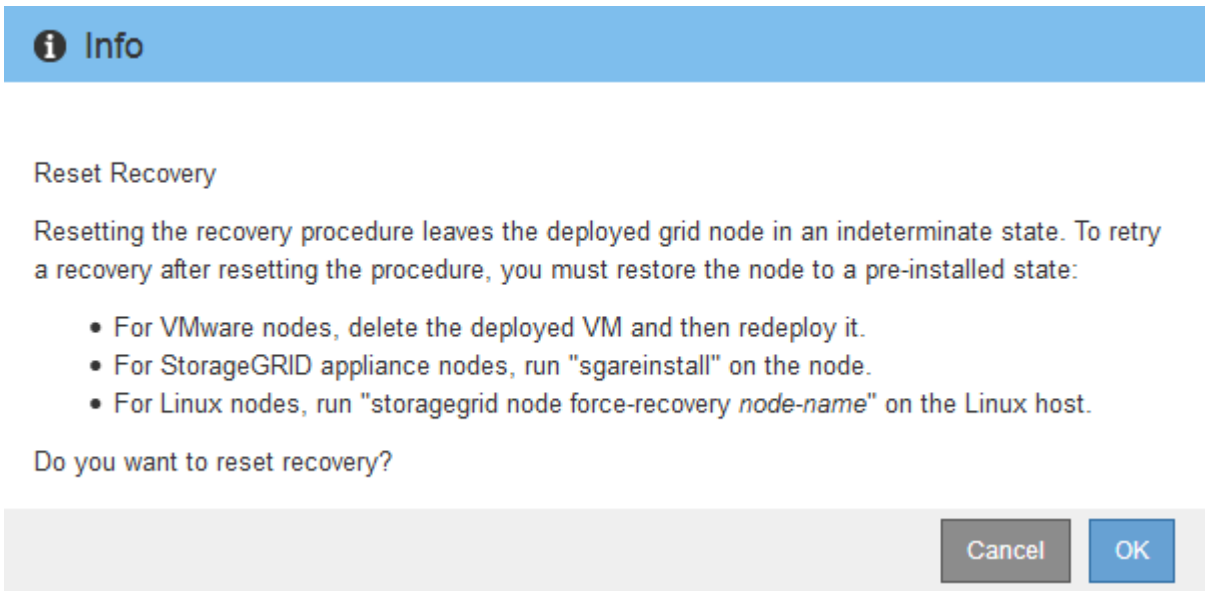
   Os nós aparecem na lista depois que eles falham, mas você não pode selecionar um nó até que ele seja reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de aprovisionamento**.
4. Clique em **Iniciar recuperação**.



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 é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.



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. "Prepare o aparelho para reinstalação (apenas substituição da plataforma)"Consulte .

Recuperação de falhas do nó de arquivo

Recuperação de falhas do nó de arquivo

O suporte para nós de arquivamento foi removido.

Para obter informações sobre como recuperar nós de arquivamento, "Recuperação de falhas de nó de arquivo (StorageGRID 11,8 doc site)" consulte .

Substitua o nó Linux

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, implante e configure o host de substituição antes que você possa 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 ou Debian. Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

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 ou nós de gateway. 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.

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:

- "Instalar o Linux (Red Hat Enterprise Linux)"

- "Instalar Linux (Ubuntu ou Debian)"

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 anfitrião 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 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.

Restaure nós de grade para o host

Para restaurar um nó de grade com falha para um novo host Linux, execute estas etapas para restaurar o arquivo de configuração do nó.

1. Restaure e valide o nó restaurando o arquivo de configuração do nó. Para 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.
2. Inicie o serviço de host do StorageGRID.
3. Conforme necessário, recupere todos os nós que não forem iniciados.

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.

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.

- "Instale o StorageGRID no Red Hat Enterprise Linux"
- "Instale o StorageGRID no Ubuntu ou Debian"

Passos

1. Na linha de comando do host recuperado, liste todos os nós 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-arc1           /dev/mapper/sgws-arc1-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, crie novamente o arquivo de configuração do nó para restaurá-lo para o host. Para obter instruções, consulte:

   - "Crie arquivos de configuração de nós para o Red Hat Enterprise Linux"
   - "Crie arquivos de configuração de nó para Ubuntu ou Debian"

> 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 as diretrizes em 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.

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 for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

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> does not exist
```

Isso significa que `/etc/storagegrid/nodes/node-name.conf` mapeia o dispositivo de bloco usado por *node-name* para `PURPOSE` 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 não conseguir restaurar ou recriar o ficheiro especial do dispositivo de bloco em falta, pode alocar um novo dispositivo de bloco com o tamanho e a categoria de armazenamento apropriados e editar o ficheiro de configuração do nó para alterar o valor de `BLOCK_DEVICE_PURPOSE` para apontar para o novo ficheiro especial do dispositivo de bloco.

Determine o tamanho e a categoria de armazenamento apropriados usando as tabelas do seu sistema operacional Linux:

- "Requisitos de armazenamento e desempenho para Red Hat Enterprise Linux"
- "Requisitos de armazenamento e desempenho para Ubuntu ou Debian"

Revise as recomendações para configurar o armazenamento de host antes de prosseguir com a substituição do dispositivo de bloco:

- "Configurar o armazenamento de host para Red Hat Enterprise Linux"
- "Configurar o armazenamento de host para Ubuntu ou Debian"

> 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.

> 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
> ```

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.

Passos

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
   ```

3. Se qualquer nó retornar um status de "não está em execução" ou "parado", execute o seguinte comando:

   ```
   sudo storagegrid node start node-name
   ```

4. 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.

Passos

1. Confirme se a configuração de rede do nó está correta.

   O nó pode ter falhado ao reingressar na grade devido a mapeamentos de interface de rede incorretos ou a um endereço IP ou gateway de rede de Grade incorreto.

2. Se a configuração da rede estiver correta, emita o `force-recovery` comando:

   `sudo storagegrid node force-recovery node-name`

3. Execute as etapas de recuperação adicionais para o nó. "O que vem a seguir: Execute etapas adicionais de recuperação, se necessário"Consulte .

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"

Tipo de recuperação	Próximo passo
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 (baseado em software): • Se você tivesse que usar o `--force` sinalizador para importar o nó, ou você emitiu `storagegrid node force-recovery node-name` • Se você teve que fazer uma reinstalação completa do nó ou você precisava restaurar /var/local	"Selecione Iniciar recuperação para configurar o nó de armazenamento"
Nó de storage (baseado em software): • Se você adicionou um novo dispositivo de bloco. • Se, para qualquer `<PURPOSE>`, o valor `BLOCK_DEVICE_<PURPOSE>` 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 VMware

Quando você recupera um nó StorageGRID com falha hospedado no VMware, você remove o nó com falha e implanta um nó de recuperação.

Antes de começar

Você determinou 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 e nós de gateway.

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 conete-a a uma ou mais redes StorageGRID. Para obter instruções, "Implantando um nó StorageGRID como uma máquina virtual"consulte .

   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.

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"

Substitua o nó com falha pelo dispositivo de serviços

Substitua o nó com falha pelo dispositivo de serviços

Você pode usar um utilitário de serviços 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.

Antes de começar

- Você determinou 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 confirmou que a versão do Instalador de dispositivos StorageGRID no utilitário de serviços corresponde à versão de software do seu sistema StorageGRID. "Verifique e atualize a versão do instalador do StorageGRID Appliance"Consulte .

> Não implante um dispositivo de serviços SG110 e SG1100 ou um dispositivo de serviços SG100 e SG1000 no mesmo site. Pode resultar em performance imprevisível.

Sobre esta tarefa

Você pode usar um dispositivo de serviços 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 em um host VMware ou Linux e estiver usando um utilitário de serviços para o nó de substituição, primeiro instale o novo hardware de dispositivo usando o mesmo nome de nó (nome do sistema) que o nó com falha.

Antes de começar

Você tem 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. O nome do nó é o nome do host (nome do sistema).
- **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.

Sobre esta tarefa

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.

Passos

1. Siga as instruções para instalar um novo dispositivo de serviços. "Início rápido para instalação de hardware"Consulte .
2. Quando for solicitado um nome de nó, use o nome do nó do nó com falha.

Prepare o aparelho 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.

Passos

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, use o Instalador de dispositivos StorageGRID, que está incluído no dispositivo.

Antes de começar

- O dispositivo é instalado em um rack, conetado às redes e ligado.
- Os links de rede e endereços IP são 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 são definidas na Lista de sub-redes de rede de grade no nó de administração principal.

  ```
  https://docs.netapp.com/us-en/storagegrid-
  appliances/installconfig/index.html["Início rápido para instalação de
  hardware"^]Consulte .
  ```

- Você está usando um "navegador da web suportado".
- Tem 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:

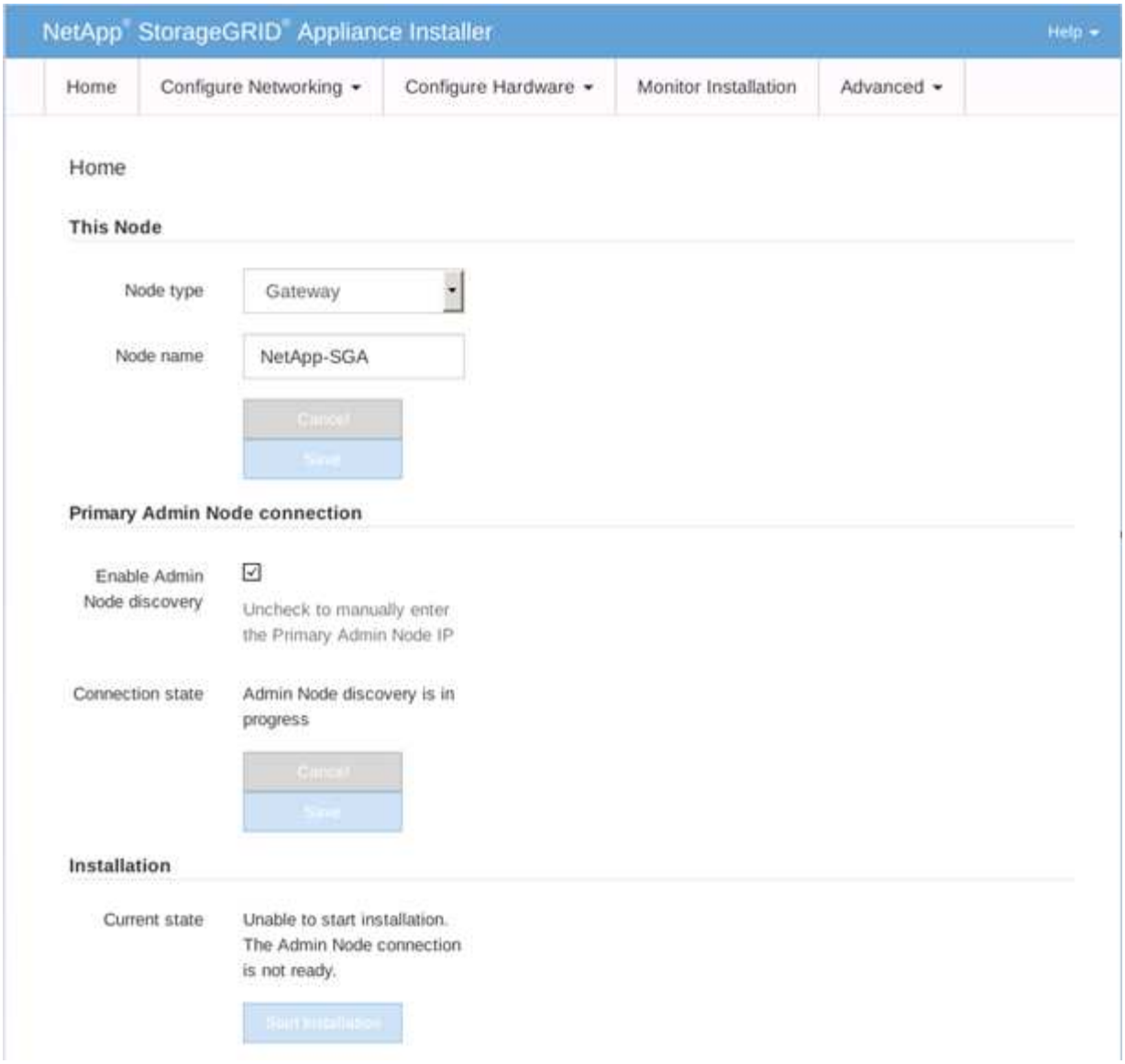
- Para um nó de administração principal, especifique o nome do nó e, em seguida, carregue os pacotes de software apropriados (se necessário).
- Para um nó de administração não primário ou um nó de gateway, especifique ou confirme o endereço IP do nó de administração principal e o nome do nó.
- Inicie 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 utilitário de serviços.

   `https://Controller_IP:8443`

   A página inicial do instalador do dispositivo StorageGRID é exibida.



2. Para instalar um nó de administração principal:

   a. Na seção este nó, para **tipo de nó**, selecione **Admin principal**.

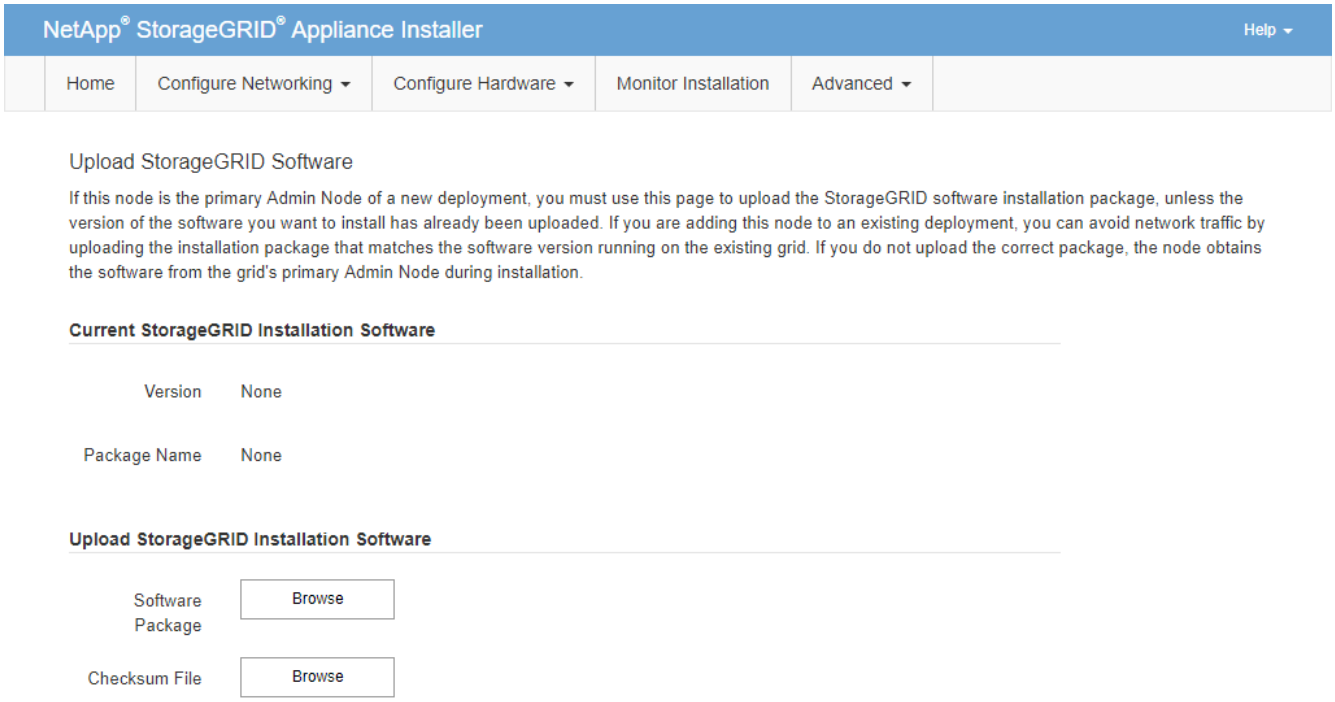
   b. No campo **Nome do nó**, insira o mesmo nome que foi usado para o nó que você está recuperando e clique em **Salvar**.

   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.



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	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 conetados	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 esse dispositivo de serviços será implantado. c. Clique em **Salvar**. d. Aguarde enquanto o estado de conexão para o novo endereço IP se torna "pronto".

4. 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 manutenção do seu aparelho.

5. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.

   O estado atual muda para "a 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.

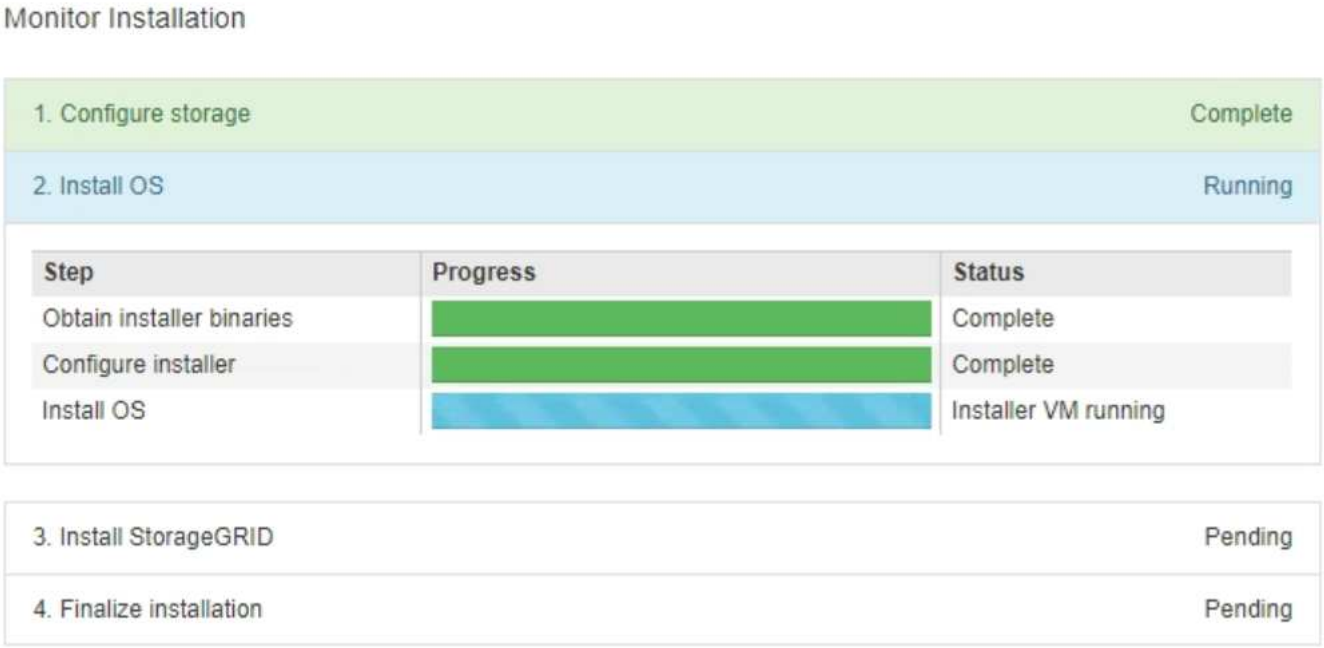
Monitorar a instalação do dispositivo de serviços

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.

Passos

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.



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 são mostradas com uma barra de status verde e um status de "ignorado".

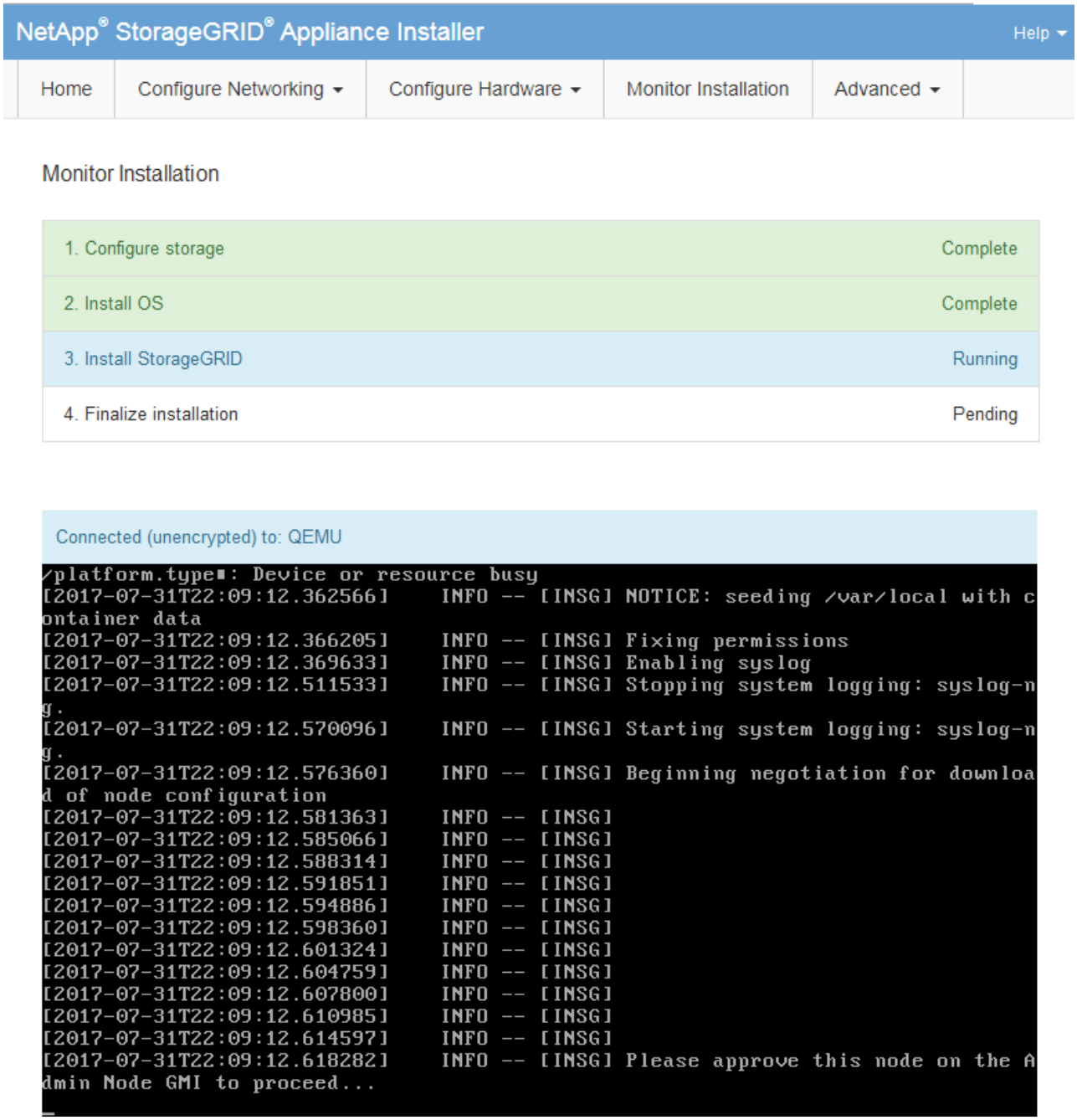
2. Reveja o progresso das duas primeiras fases de instalação.
   - **1. Configurar armazenamento**

     Durante este estágio, o instalador limpa qualquer configuração existente das unidades e configura as configurações do host.

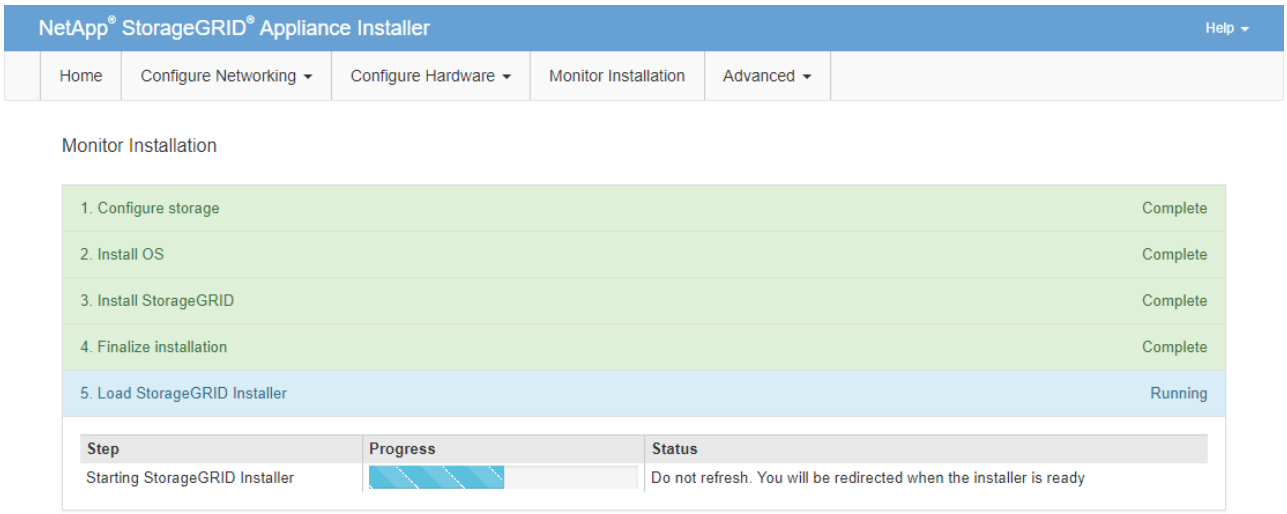
   - **2. Instale o os**

     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.



- 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.



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 o suporte técnico recupera um site

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, determine 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 Policies**: O número, tipo e localização das cópias de objetos em sua grade é controlado por suas políticas ativas de ILM. As especificidades de suas políticas 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)**: A consistência aplicada a um bucket (ou container) afeta 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. Se o valor de consistência permitir consistência eventual, alguns metadados de objeto 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 em suas políticas 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.

A recuperação do local só pode ser realizada por suporte técnico.

Esta é uma visão geral do processo que o suporte técnico usa para recuperar um site com falha:

1. Suporte técnico:
   a. Faz uma avaliação detalhada da falha.
   b. Trabalha com você para rever seus objetivos de negócios.
   c. Desenvolve um plano de recuperação adaptado à sua situação.
2. Se o nó de administração principal falhar, o suporte técnico o recupera.
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, o suporte técnico usa comandos especializados 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, o suporte técnico usa procedimentos padrão para recuperar nós de Gateway com falha ou nós de administração não primários.

Informações relacionadas

"Desativação do site"

Como ativar o StorageGRID no seu ambiente

https://docs.netapp.com/us-en/storagegrid-enable/index.html["Como ativar o StorageGRID"^]Acesse para saber como testar e ativar aplicativos em seu ambiente StorageGRID.

Como gerenciar o StorageGRID usando o BlueXP

https://docs.netapp.com/us-en/bluexp-storagegrid/index.html["Gerenciamento de StorageGRID usando o BlueXP"^]Acesse para saber como gerenciar seus sistemas StorageGRID do BlueXP usando o Gerenciador de Grade e usar os serviços de dados do BlueXP para backups, categorização de dados e muito mais.

Outras versões da documentação do NetApp StorageGRID

Você pode encontrar documentação para outras versões do software NetApp StorageGRID aqui:

- "Documentação do StorageGRID 11,8"
- "Documentação do StorageGRID 11,7"
- "Documentação do StorageGRID 11,6"
- "Documentação do StorageGRID 11,5"
- "Centro de Documentação do StorageGRID 11,4"
- "Centro de Documentação do StorageGRID 11,3"

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

https://library.netapp.com/ecm/ecm_download_file/ECMLP3330669

Informações sobre direitos autorais

Informações sobre marcas comerciais