Documentação do StorageGRID 11,5

StorageGRID 11.5

NetApp
November 07, 2024

Índice

Documentação do StorageGRID 11,5

Notas de lançamento

Obtenha informações específicas sobre novos recursos, recursos removidos e obsoletos, problemas corrigidos e problemas conhecidos.

Notas de versão estão disponíveis fora deste site de documentação. Você será solicitado a fazer login usando suas credenciais do site de suporte da NetApp.

- "HTML"
- "PDF"

Comece agora

Primário de grelha

Aprenda os conceitos básicos de um sistema NetApp StorageGRID.

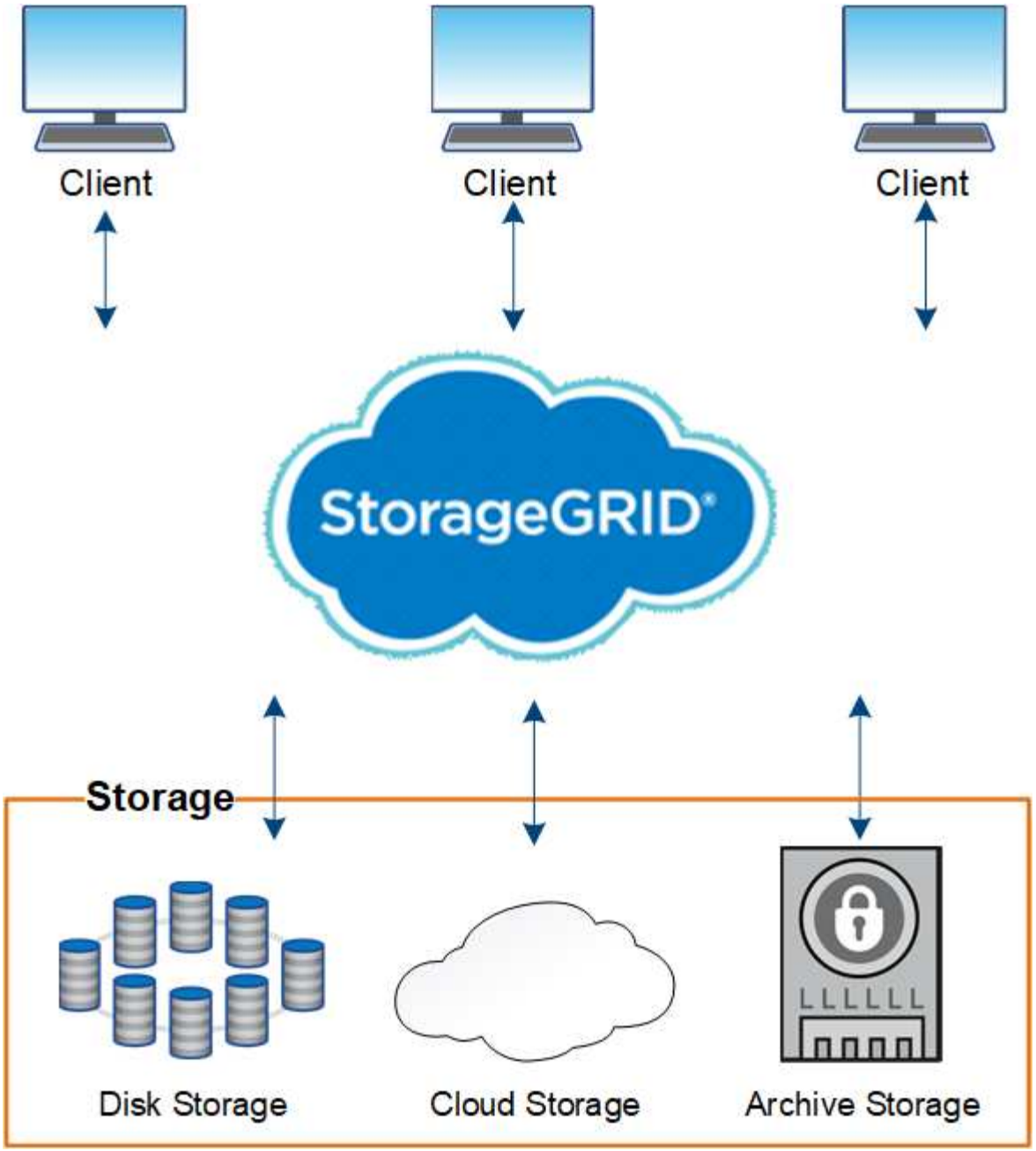
- "Sobre o StorageGRID"
- "Topologia de rede e arquitetura StorageGRID"
- "Como o StorageGRID gerencia dados"
- "Explorando o Gerenciador de Grade"
- "Explorando o gerente do locatário"
- "Usando o StorageGRID"

Sobre o StorageGRID

O NetApp StorageGRID é uma solução de storage baseada em objetos e definida por software compatível com APIs de objeto padrão do setor, incluindo a API Amazon Simple Storage Service (S3) e a API OpenStack Swift.

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.



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
- 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 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 e personalizar a localidade, a durabilidade, a performance, o custo e o tempo de retenção dos dados. A fita está disponível como um nível de arquivo integrado.
- 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.
  - Contentores Docker 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).

Informações relacionadas

"Nuvens híbridas com StorageGRID"

"Topologia de rede e arquitetura StorageGRID"

"Controlar o acesso à StorageGRID"

"Gerenciamento de locatários e conexões de clientes"

"Uso do gerenciamento do ciclo de vida das informações"

"Monitoramento das operações do StorageGRID"

"Configurar definições de rede"

"Executar procedimentos de manutenção"

Nuvens híbridas com StorageGRID

Você pode usar o StorageGRID em uma configuração de nuvem híbrida implementando gerenciamento de dados voltado a políticas para armazenar objetos em pools de storage de nuvem, aproveitando os serviços de plataforma StorageGRID e movendo dados 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, é possível mover objetos acessados com pouca frequência para storage de nuvem de baixo custo, como Amazon S3 Glacier, S3 Glacier Deep Archive ou a camada de acesso de arquivamento no storage Microsoft Azure Blob. 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 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 a receção de eventos do Simple Notification Service (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.

ONTAP data Tiering com StorageGRID

Você pode reduzir os custos do storage do ONTAP categorizando os dados no StorageGRID usando o FabricPool. O FabricPool é uma tecnologia NetApp Data Fabric que permite a disposição automatizada 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

"Administrar o StorageGRID"

"Use uma conta de locatário"

"Gerenciar objetos com ILM"

"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.

Para obter informações adicionais sobre topologia de rede, requisitos e comunicações em grade do StorageGRID, consulte as diretrizes de rede.

Informações relacionadas

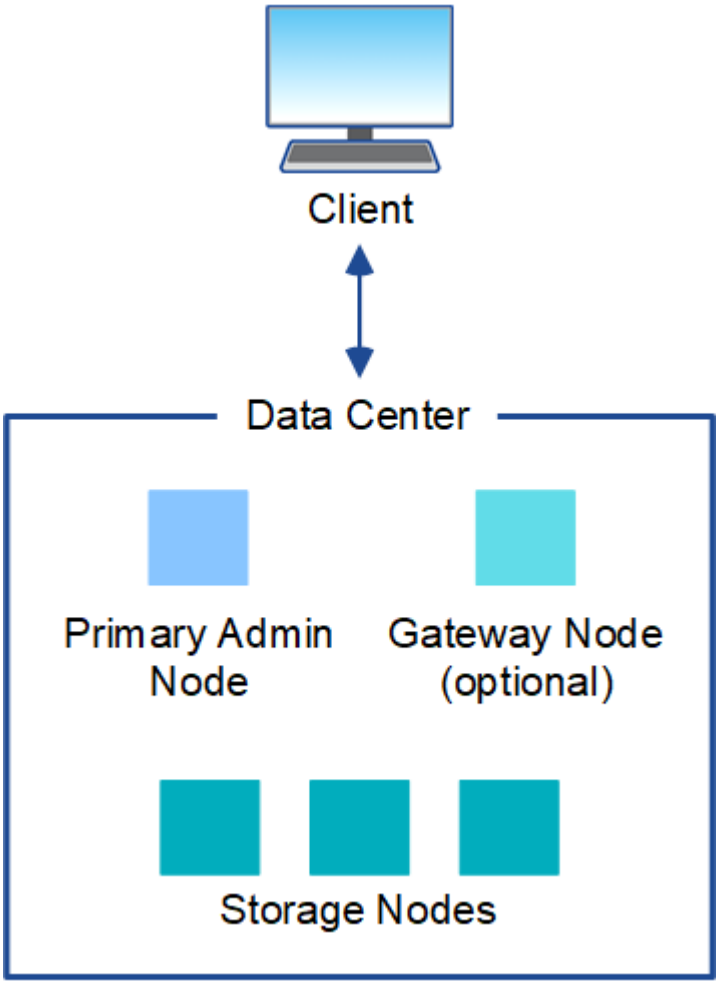
"Diretrizes de rede"

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

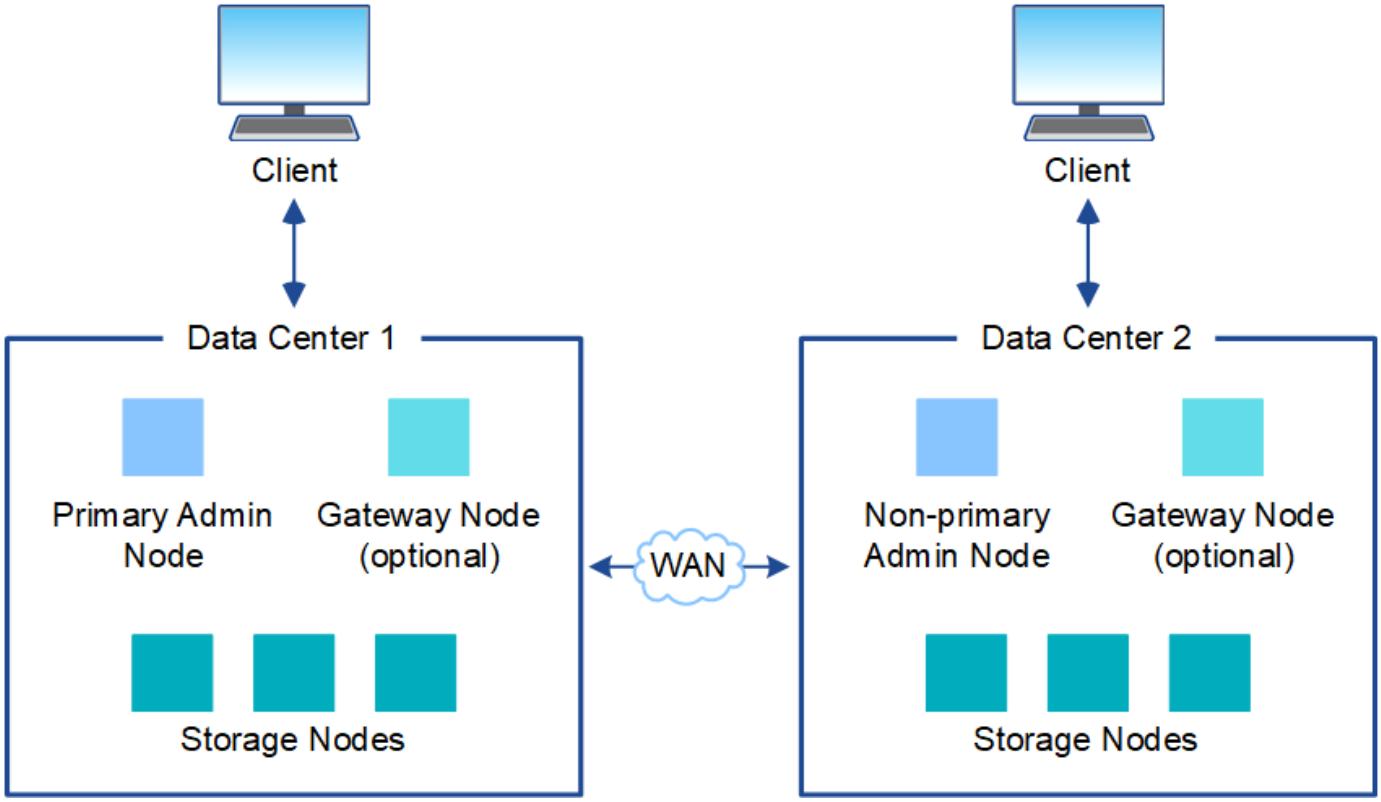
Em uma implantação com um único local, a infraestrutura e as operações do sistema StorageGRID são centralizadas.



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.



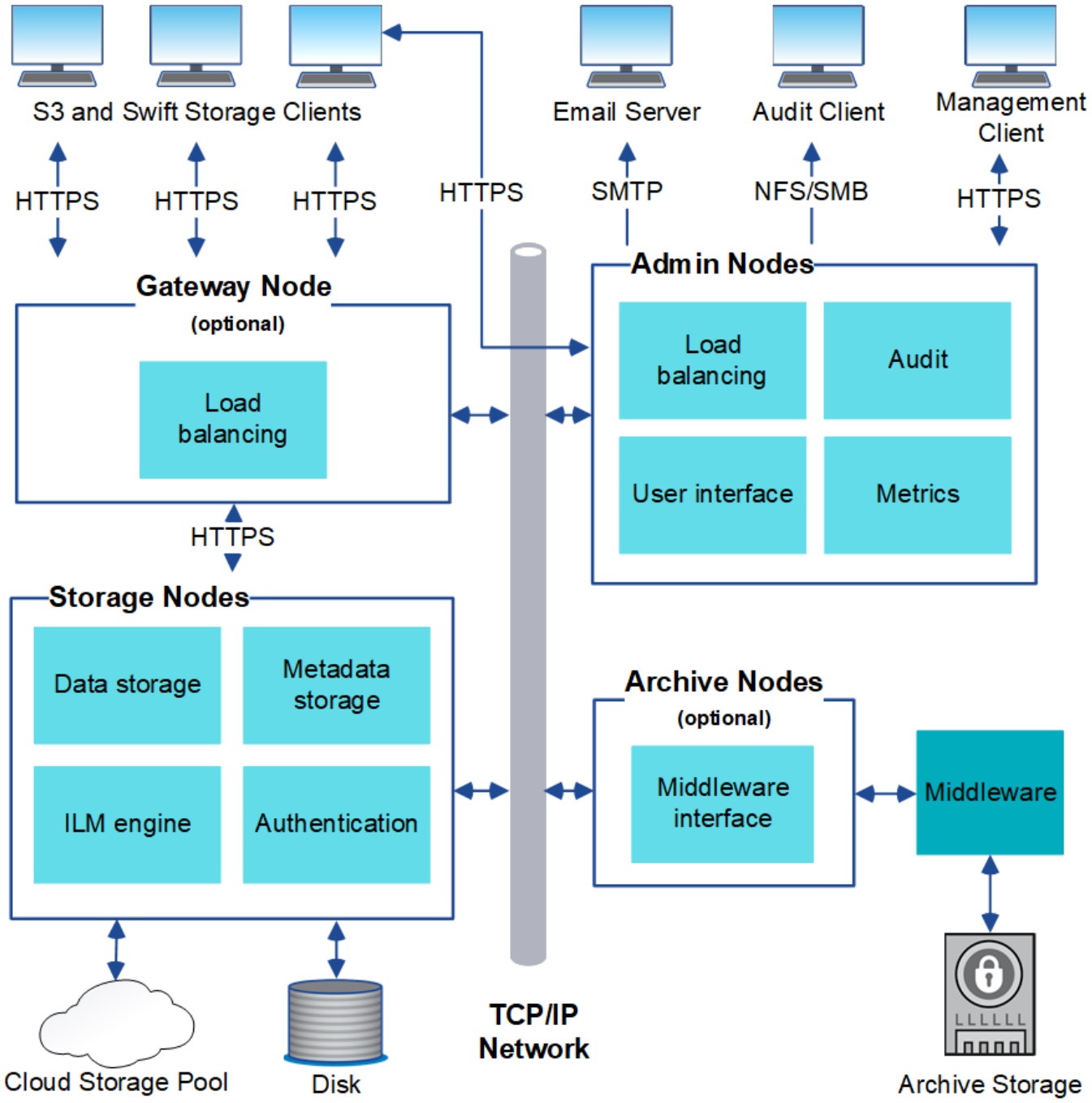
Vários locais lógicos também podem existir em um único data center para permitir o uso de replicação distribuída e codificação de apagamento para aumentar a disponibilidade e a resiliência.

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 e Swift 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 e Swift 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 e Swift 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, em Mídia de arquivamento externa, como fita, ou em Cloud Storage Pools, que consistem em buckets externos do S3 ou contêineres de storage Azure Blob.

Informações relacionadas

"Administrar o StorageGRID"

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.

O sistema StorageGRID usa quatro tipos de nós de grade:

- **Admin Nodes** fornecem serviços de gerenciamento, como configuração do sistema, monitoramento e Registro. 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 Admin também podem ser usados para equilibrar o tráfego de clientes S3 e Swift.

- **Nós de storage** gerenciam e armazenam dados e metadados de objetos. Cada sistema StorageGRID precisa ter pelo menos três nós de storage. Se você tiver vários locais, cada local no sistema StorageGRID também precisará ter três nós de storage.
- **Os nós de gateway (opcional)** fornecem 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. Você pode usar uma combinação de nós de Gateway e nós de administrador para balanceamento de carga ou implementar um balanceador de carga HTTP de terceiros.
- **Os nós de arquivo (opcional)** fornecem uma interface através da qual os dados de objetos podem ser arquivados em fita.

Nós baseados em software

Os nós de grade baseados em software podem ser implantados das seguintes maneiras:

- Como máquinas virtuais (VMs) no VMware vSphere Web Client
- Dentro de contentores Docker em hosts Linux. Os seguintes sistemas operacionais são suportados:
  - Red Hat Enterprise Linux
  - CentOS
  - Ubuntu
  - Debian

Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

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.

Estão disponíveis quatro tipos de dispositivos StorageGRID:

- Os dispositivos de serviços **SG100 e SG1000** são servidores de 1 unidades de rack (1UU) que podem operar cada um como nó de administrador principal, um nó de administrador não primário ou um nó de

gateway. Ambos os dispositivos podem operar como nós de gateway e nós de administração (primários e não primários) ao mesmo tempo.

- O **SG6000 Storage Appliance** funciona como um nó de armazenamento e combina o controlador de computação 1U SG6000-CN com uma gaveta de controladora de armazenamento 2U ou 4U. O SG6000 está disponível em dois modelos:
  - **SGF6024**: Combina o controlador de computação SG6000-CN com um compartimento de controladora de armazenamento 2U que inclui 24 unidades de estado sólido (SSDs) e controladores de armazenamento redundantes.
  - **SG6060**: Combina a controladora de computação SG6000-CN com um compartimento 4U que inclui 58 unidades NL-SAS, SSDs de 2 TB e controladores de storage redundantes. Cada dispositivo SG6060 dá suporte a uma ou duas gavetas de expansão de 60 unidades, fornecendo até 178 unidades dedicadas ao storage de objetos.
- O **SG5700 Storage Appliance** é uma plataforma de storage e computação integrada que opera como nó de armazenamento. O SG5700 está disponível em dois modelos:
  - **SG5712**: Um compartimento de 2U U que inclui 12 unidades NL-SAS e controladores de computação e storage integrados.
  - **SG5760**: Um compartimento de 4U U que inclui 60 unidades NL-SAS e controladores de computação e storage integrados.
- O **SG5600 Storage Appliance** é uma plataforma de storage e computação integrada que opera como nó de armazenamento. O SG5600 está disponível em dois modelos:
  - **SG5612**: Um compartimento de 2U U que inclui 12 unidades NL-SAS e controladores de computação e storage integrados.
  - **SG5660**: Um compartimento de 4U U que inclui 60 unidades NL-SAS e controladores de computação e storage integrados.

Consulte o NetApp Hardware Universe para obter as especificações completas.

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 do sistema.
Nó de gerenciamento de configuração (CMN)	Gerencia a configuração em todo o sistema. Somente nó de administração principal.
Interface do programa de aplicação de gerenciamento (mgmt-api)	Processa solicitações da API de gerenciamento de grade e da API de gerenciamento do locatário.
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.

Serviço	Função de chave
Balanceador de carga	Fornece balanceamento de carga de tráfego S3 e Swift de clientes para nós de storage. **Nota:** este serviço também é encontrado em nós de Gateway.
Sistema de gerenciamento de rede (NMS)	Fornece funcionalidade para o Gerenciador de Grade.
Prometheus	Coleta e armazena métricas.
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

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.
Cassandra	Armazena e protege metadados de objetos.
Cassandra Reaper	Executa reparos automáticos de metadados de objetos.
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.
Identidade (idnt)	Federa identidades de usuários do LDAP e do ative Directory.
Roteador 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 serviço da plataforma S3 sejam enviadas para seus respetivos endpoints.
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

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
Balanceador de carga de conexão (CLB)	Fornece balanceamento de carga das camadas 3 e 4 de tráfego S3 e Swift de clientes para nós de storage. Mecanismo de balanceamento de carga legado. **Nota:** o serviço CLB está obsoleto.
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 de tráfego S3 e Swift 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.
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

Serviços primários para nós de arquivamento

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

Serviço	Função de chave
Arquivo (ARC)	Comunica com um sistema de armazenamento de fita externo do Tivoli Storage Manager (TSM).
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

Serviços da StorageGRID

A seguir está uma lista completa de serviços do StorageGRID.

- * Agente de Serviço de conta*

  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. O serviço Load Balancer está presente em nós de administração e nós de gateway.

- **ADC Service (Administrative Domain Controller)**

  Mantém informações de topologia, fornece serviços de autenticação e responde a consultas dos serviços LDR e CMN. O serviço ADC está presente em cada um dos três primeiros nós de storage instalados em um local.

- **AMS Service (sistema de Gestão de Auditoria)**

  Monitora e Registra todos os eventos e transações do sistema auditados em um arquivo de log de texto. O serviço AMS está presente nos nós de administração.

- **Serviço ARC (Arquivo)**

  Fornece a interface de gerenciamento com a qual você configura conexões para armazenamento de arquivamento externo, como a nuvem por meio de uma interface S3 ou fita por meio de middleware TSM. O serviço ARC está presente nos nós de arquivo.

- **Cassandra Reaper serviço**

  Executa reparos automáticos de metadados de objetos. O serviço Cassandra Reaper está presente em todos os nós de storage.

- **Serviço Chunk**

  Gerencia dados codificados por apagamento e fragmentos de paridade. O serviço Chunk está presente nos nós de storage.

- **Serviço CLB (Connection Load Balancer)**

  Serviço obsoleto que fornece um gateway para o StorageGRID para aplicativos clientes que se conetam através de HTTP. O serviço CLB está presente nos nós de Gateway. O serviço CLB está obsoleto e será removido em uma versão futura do StorageGRID.

- **Serviço CMN (Configuration Management Node)**

  Gerencia configurações e tarefas de grade em todo o sistema. Cada grade tem um serviço CMN, que está presente no nó Admin principal.

- **Serviço DDS (armazenamento de dados distribuído)**

  Interfaces com o banco de dados Cassandra para gerenciar metadados de objetos. O serviço DDS está presente nos nós de storage.

- **Serviço DMV (Data Mover)**

  Move dados para pontos de extremidade da nuvem. O serviço DMV está presente nos nós de storage.

- **Serviço IP dinâmico**

  Monitora a grade para alterações dinâmicas de IP e atualiza configurações locais. O serviço Dynamic IP (dynip) está presente em todos os nós.

- **Serviço Grafana**

  Usado para visualização de métricas no Gerenciador de Grade. O serviço Grafana está presente nos nós de administração.

- **Serviço de alta disponibilidade**

  Gerencia IPs virtuais de alta disponibilidade em nós configurados na página grupos de alta disponibilidade. O serviço de alta disponibilidade está presente em nós de administração e nós de gateway. Este serviço também é conhecido como o serviço keepalived.

- **Serviço de identidade (idnt)**

  Federa identidades de usuários do LDAP e do ative Directory. O serviço de identidade (idnt) está presente em três nós de storage em cada local.

- **Serviço de balanceador de carga**

  Fornece balanceamento de carga de tráfego S3 e Swift de clientes para nós de storage. O serviço Load Balancer pode ser configurado através da página de configuração Load Balancer Endpoints. O serviço Load Balancer está presente em nós de administração e nós de gateway. Este serviço também é conhecido como o serviço nginx-gw.

- **Serviço LDR (Roteador de distribuição local)**

  Gerencia o armazenamento e a transferência de conteúdo dentro da grade. O serviço LDR está presente nos nós de armazenamento.

- **MISCd Information Service Control Daemon Service**

  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. O serviço MISCd está presente em todos os nós.

- **serviço 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. O serviço nginx está presente em todos os nós.

- **serviço nginx-gw**

  Alimenta o serviço Load Balancer. O serviço nginx-gw está presente em nós de administração e nós de gateway.

- **Serviço NMS (sistema de Gestão de rede)**

  Alimenta as opções de monitoramento, relatórios e configuração que são exibidas pelo Gerenciador de Grade. O serviço NMS está presente nos nós de administração.

- **Serviço de persistência**

  Gerencia arquivos no disco raiz que precisam persistir ao longo de uma reinicialização. O serviço de persistência está presente em todos os nós.

- **Serviço Prometheus**

  Coleta métricas de séries temporais de serviços em todos os nós. O serviço Prometheus está presente nos nós de administração.

- **Serviço RSM (Serviço de Máquina de Estado replicado)**

  Garante que as solicitações de serviço da plataforma sejam enviadas para seus respetivos endpoints. O serviço RSM está presente nos nós de storage que usam o serviço ADC.

- **Serviço SSM (Monitor de status do servidor)**

  Monitora as condições de hardware e os relatórios para o serviço NMS. Uma instância do serviço SSM está presente em todos os nós da grade.

- **Trace Collector Service**

  Executa a coleta de rastreamento para coletar informações para uso pelo suporte técnico. O serviço de coletor de rastreamento usa o software Jaeger de código aberto e está presente nos nós de administração.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"NetApp Hardware Universe"

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Administrar o StorageGRID"

Como o StorageGRID gerencia dados

À medida que você começa a trabalhar com o sistema StorageGRID, é útil entender como o sistema StorageGRID gerencia os dados.

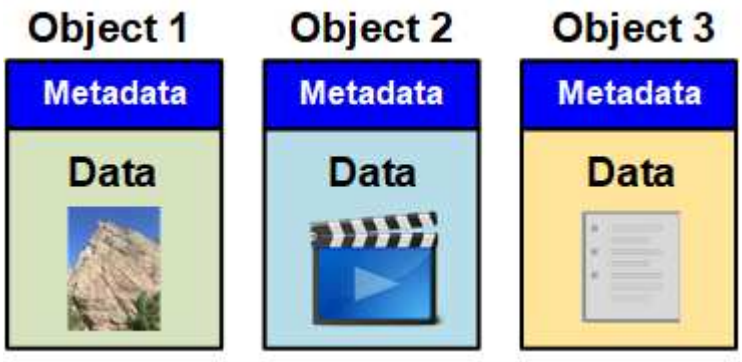
- "O que é um objeto"
- "Como os dados do objeto são protegidos"

- "A vida de um objeto"

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.



Dados de objeto

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

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 "Gerenciamento do storage de metadados de objetos".

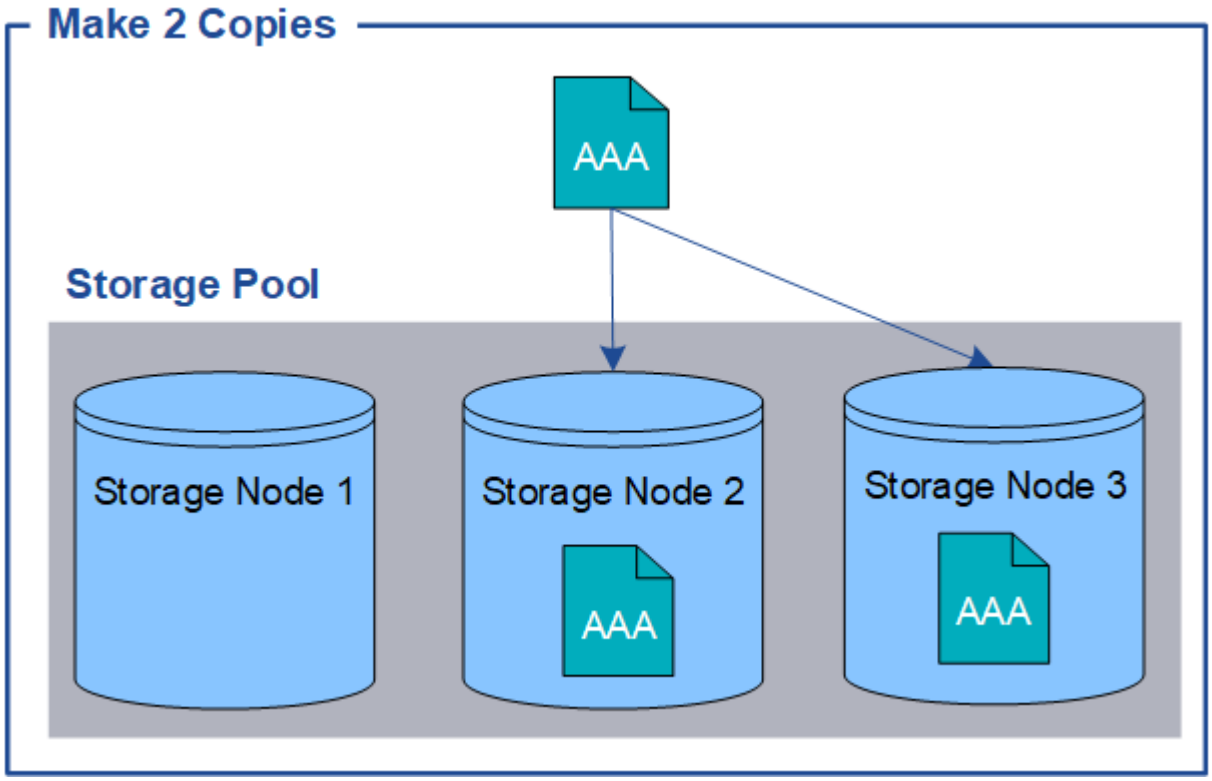
Como os dados do objeto são protegidos

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, nós de arquivamento 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.

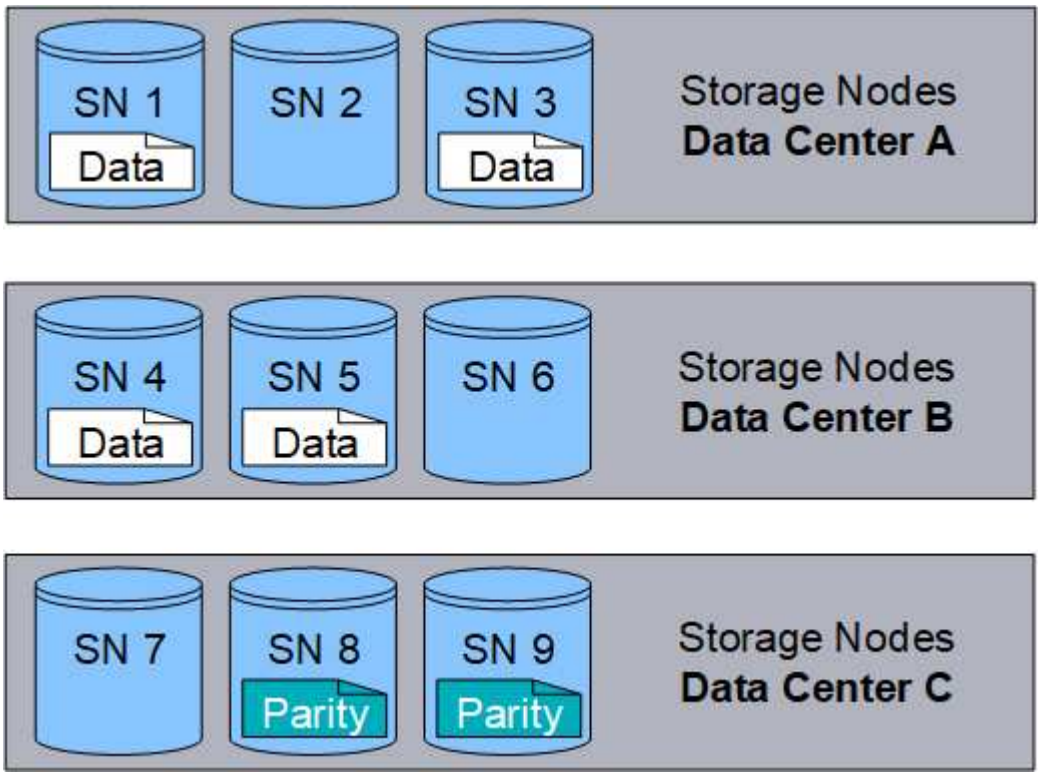


Codificação de apagamento

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"

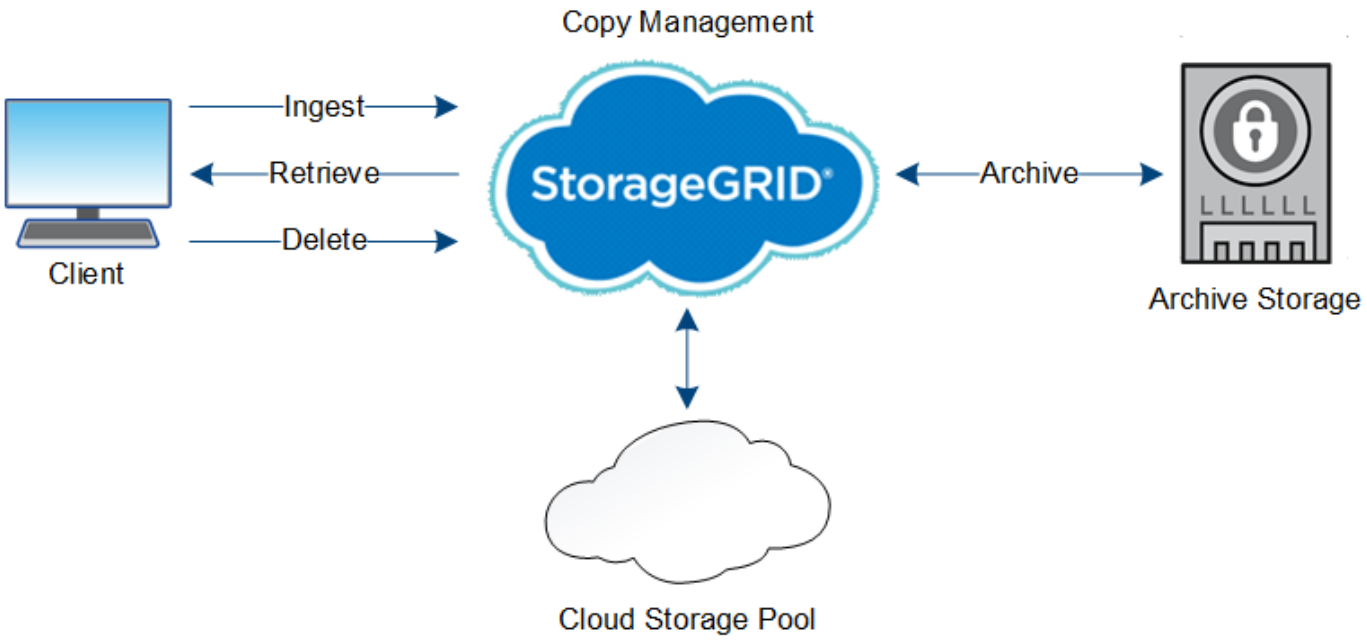
"Uso do gerenciamento do ciclo de vida das informações"

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 ou Swift 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 na política ativa 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, em um pool de storage de nuvem ou no nó de arquivamento.
- **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, pool de armazenamento em nuvem ou nó de arquivamento.
- **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"

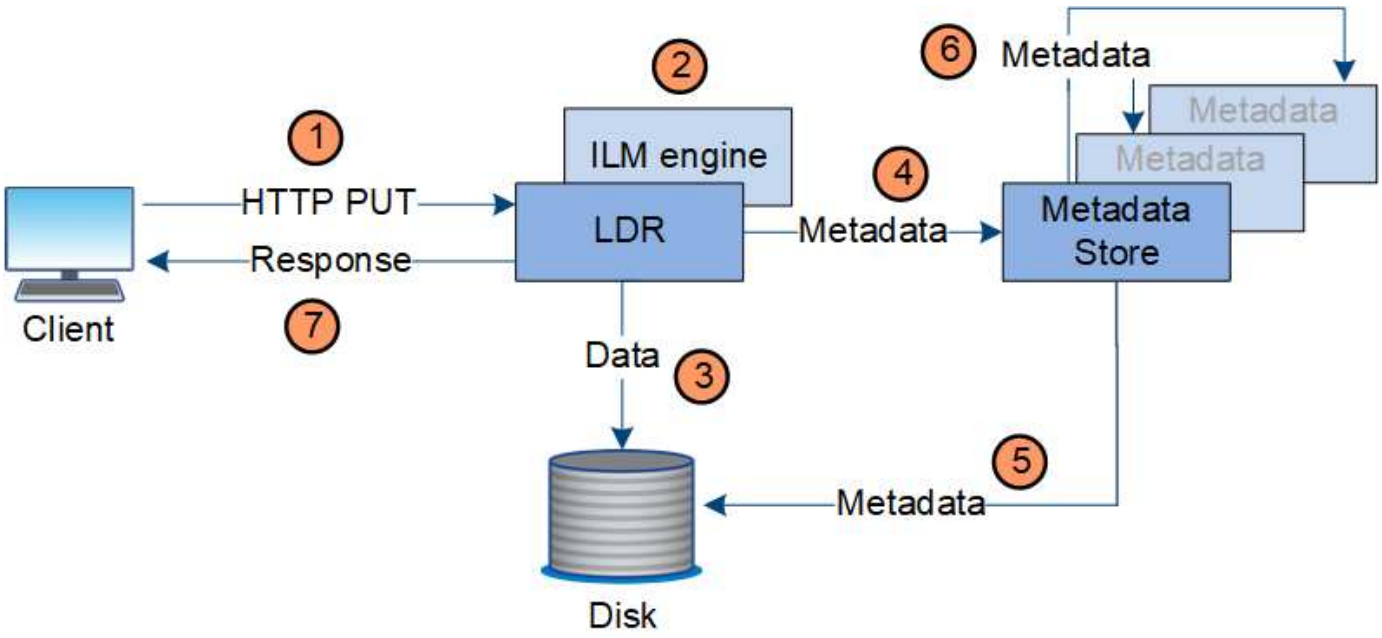
"Uso do gerenciamento do ciclo de vida das informações"

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 salva um objeto no 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 de 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 pela política ILM ativa e suas regras 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.

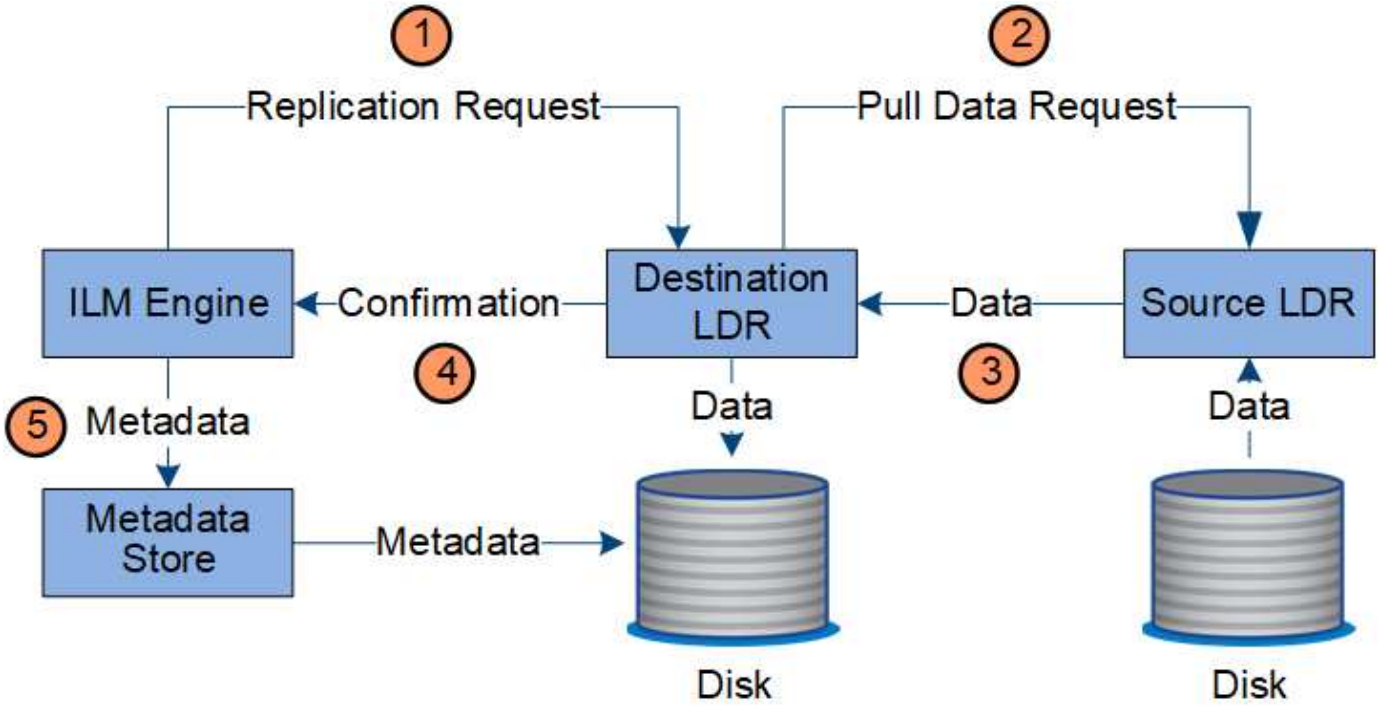
Os dados do objeto são geridos pelo serviço LDR.

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.

Fluxo de dados

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.



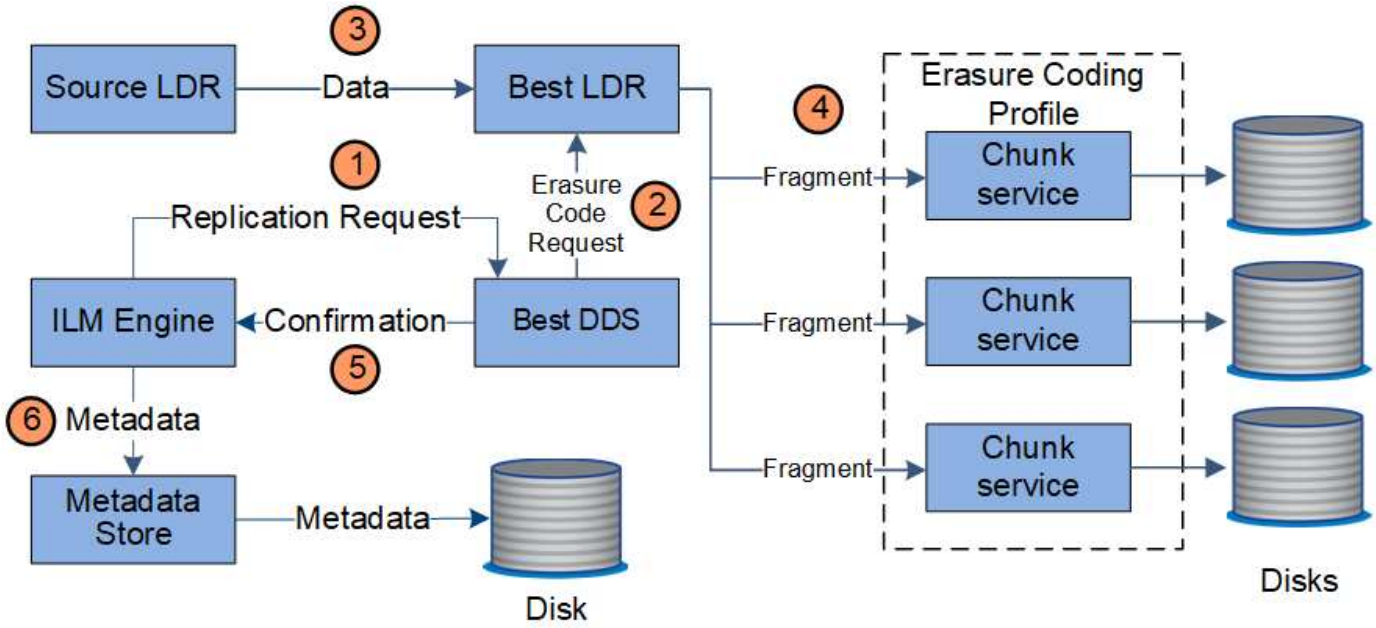
1. O mecanismo ILM consulta o serviço ADC para determinar o melhor serviço LDR de destino dentro do pool de armazenamento especificado pela regra ILM. Em seguida, envia um comando para iniciar a replicação ao serviço LDR.
2. O serviço LDR de destino consulta o serviço ADC para obter a melhor localização 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 de apagamento de dados de objeto, o esquema de codificação de apagamento aplicável quebra os dados de objeto em dados e fragmentos de paridade e distribui esses fragmentos entre os nós de storage configurados no perfil de codificação de apagamento.

Fluxo de dados

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.



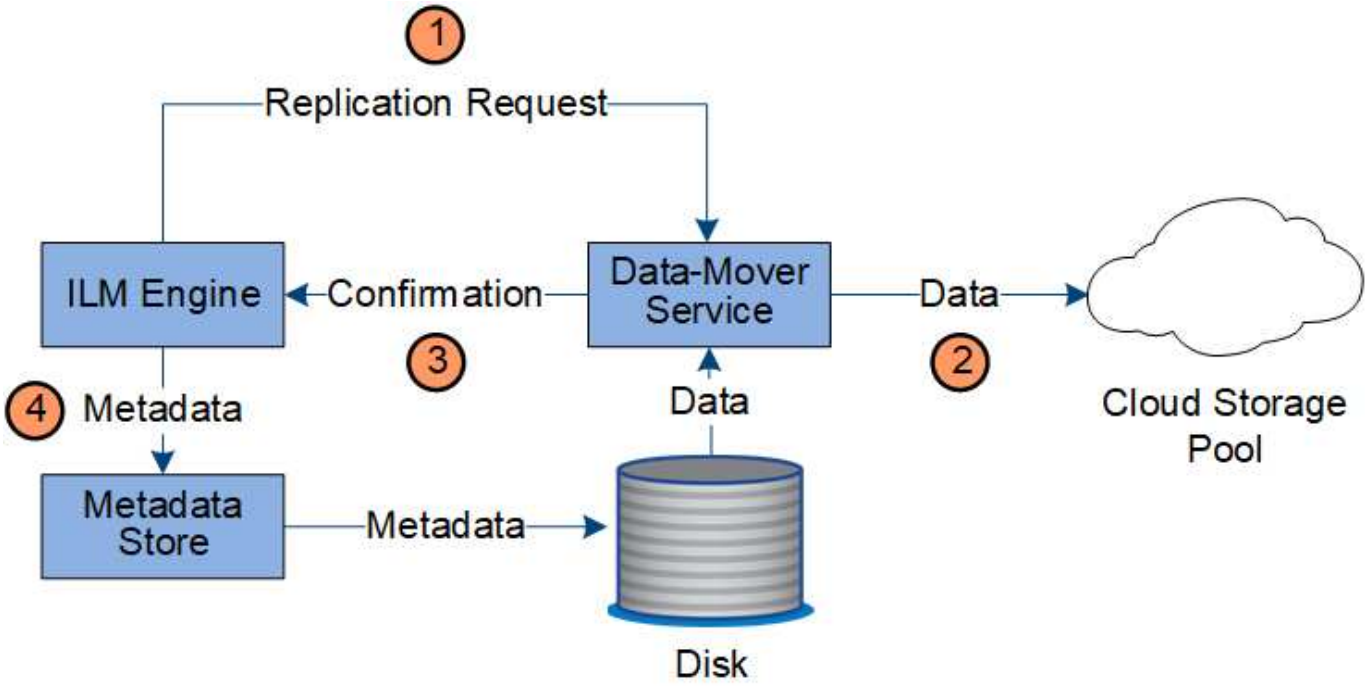
1. O mecanismo ILM consulta o serviço ADC para determinar qual serviço DDS pode executar melhor a operação de codificação de apagamento. Uma vez determinado, o motor ILM envia um pedido de "iniciar" para esse serviço.
2. O serviço DDS instrui um LDR a apagar os dados do objeto.
3. O serviço LDR de origem envia uma cópia para o serviço LDR selecionado para codificação de apagamento.
4. Uma vez quebrado no 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 objeto serão movidos para o bucket externo do S3 ou para o contêiner de storage Azure Blob especificado para o Cloud Storage Pool.

Fluxo de dados

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.

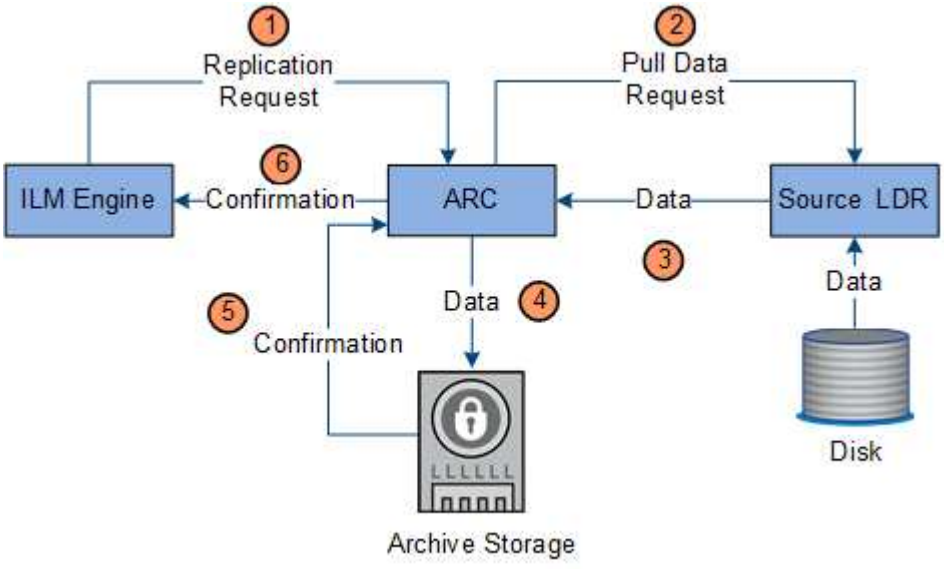


1. O mecanismo ILM seleciona um serviço Data Mover para replicação no Cloud Storage Pool.
2. O serviço Data Mover envia os dados do objeto para o Cloud Storage Pool.
3. O serviço Data Mover notifica o mecanismo ILM de que os dados do objeto foram armazenados.
4. O mecanismo ILM atualiza o armazenamento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

Proteção de conteúdo: Arquivo

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

Se a política ILM exigir que uma cópia dos dados do objeto seja arquivada, o mecanismo ILM, que é um componente do serviço LDR, envia uma solicitação para o nó de arquivo, que por sua vez envia uma cópia dos dados do objeto para o sistema de armazenamento de arquivos visado.



1. O mecanismo ILM envia um pedido ao serviço ARC para armazenar uma cópia em suportes de arquivo.

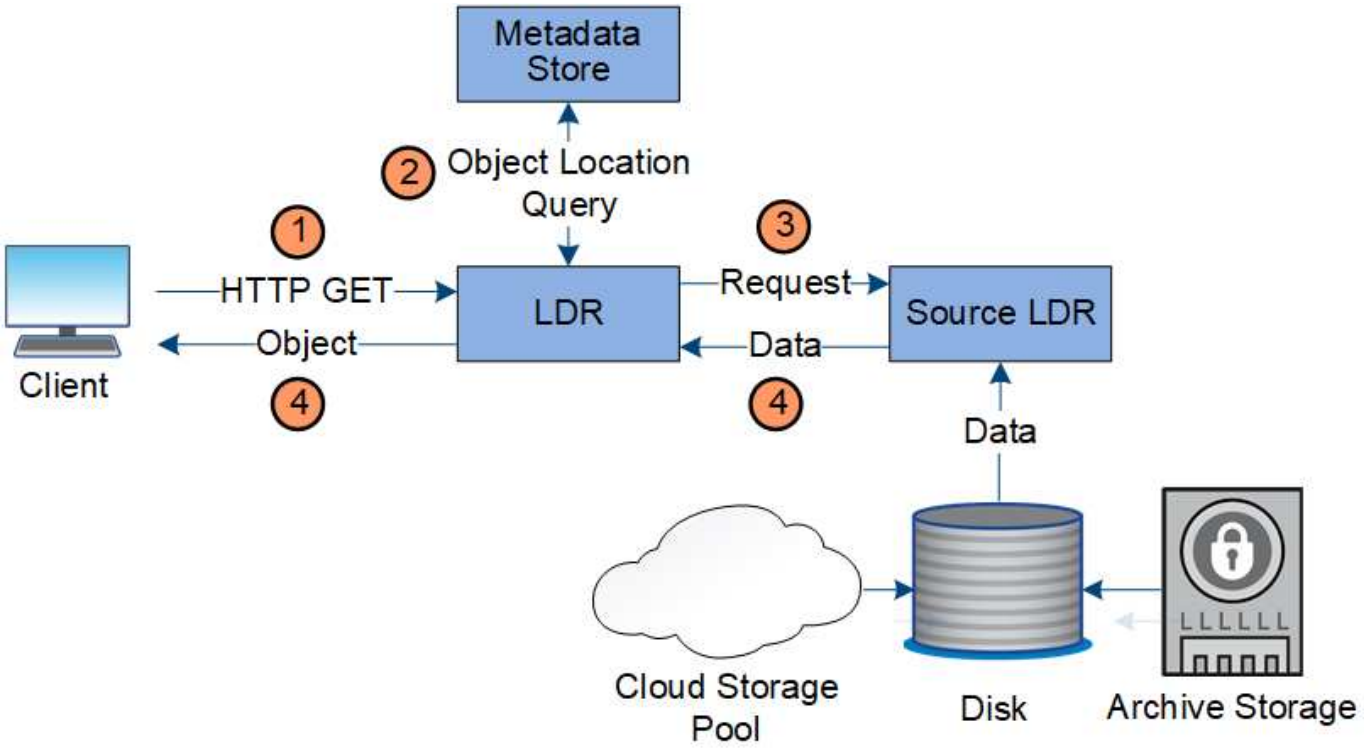
2. O serviço ARC consulta o serviço ADC para obter a melhor localização de origem e envia uma solicitação para o serviço LDR de origem.
3. O serviço ARC recupera dados de objeto do serviço LDR.
4. O serviço ARC envia os dados do objeto para o destino do suporte de arquivo.
5. O suporte de dados de arquivo notifica o serviço ARC de que os dados do objeto foram armazenados.
6. O serviço ARC notifica o motor ILM de que os dados do objeto foram armazenados.

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 ou nó de arquivo.

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 ou para um nó de arquivamento.

> Se a única cópia de objeto estiver no storage do AWS Glacier ou no nível do Azure Archive, o aplicativo cliente deverá emitir uma solicitação de restauração PÓS-Objeto S3 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.

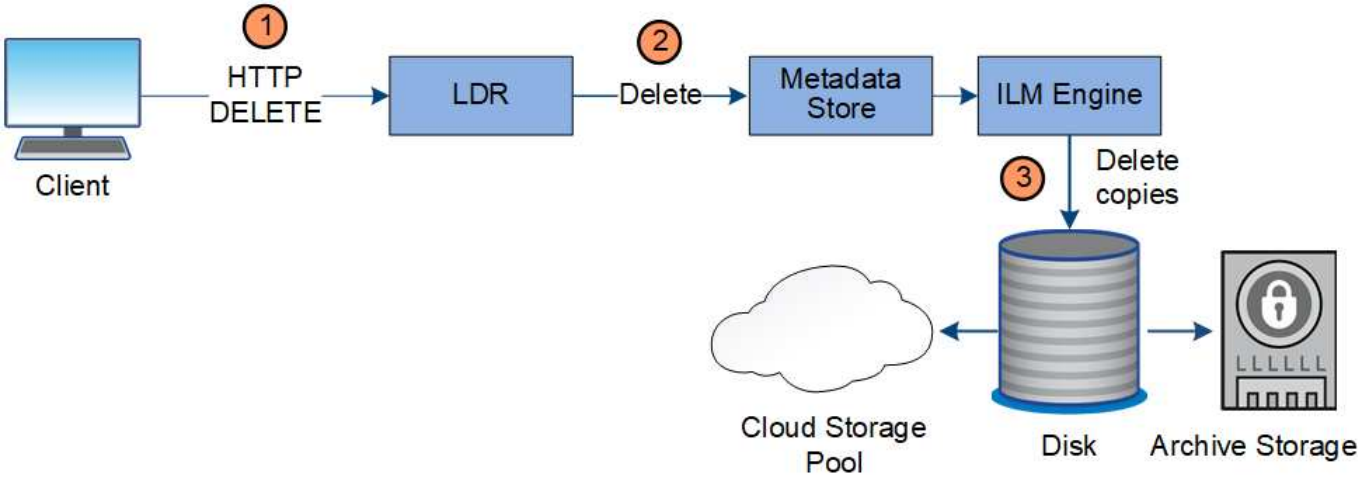
Hierarquia de exclusão

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 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.
- **Solicitação de exclusão do cliente**: Um cliente S3 ou Swift pode emitir uma solicitação de exclusão de objeto. Quando um cliente exclui um objeto, todas as cópias do objeto são removidas 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.

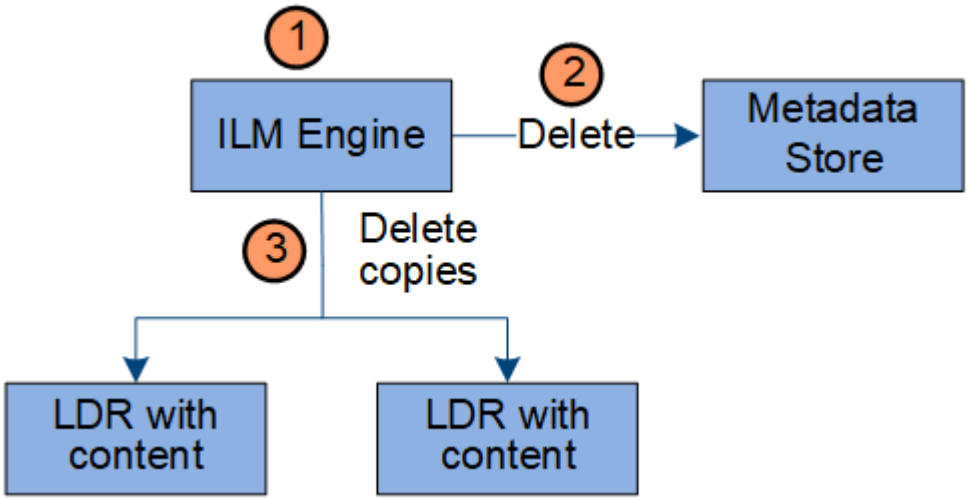
> ⓘ A ação de expiração em um ciclo de vida do bucket do S3 sempre substitui as configurações do ILM. Como resultado, um objeto pode ser retido na grade mesmo depois que quaisquer instruções ILM para colocar o objeto tenham expirado.

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.

Explorando o Gerenciador de Grade

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

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 compatível.

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

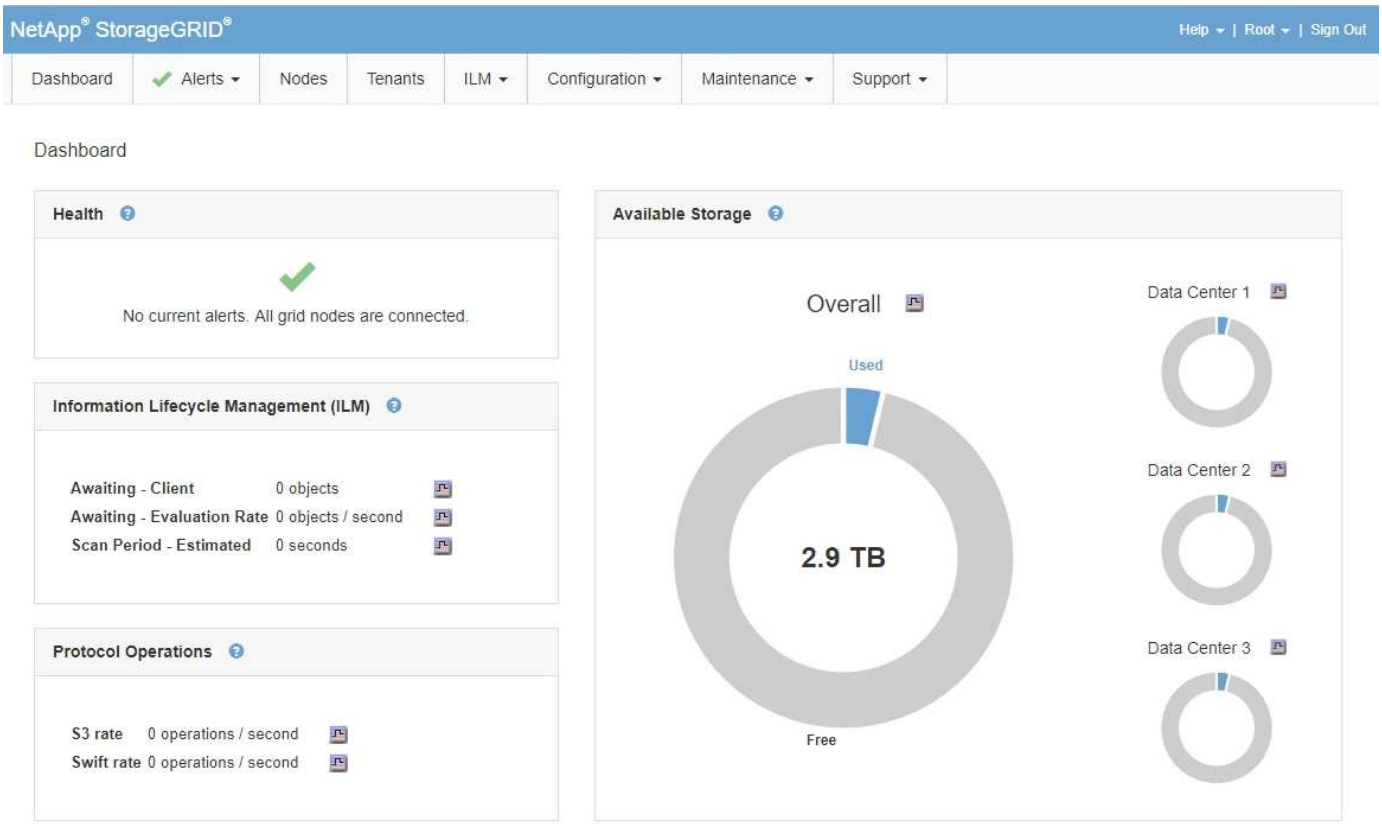
Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Painel do Grid Manager

Ao iniciar sessão pela primeira vez no Gestor de grelha, pode utilizar o Painel para monitorizar rapidamente as atividades do sistema.

O Dashboard inclui informações resumidas sobre a integridade do sistema, o uso do storage, os processos ILM e as operações S3 e Swift.



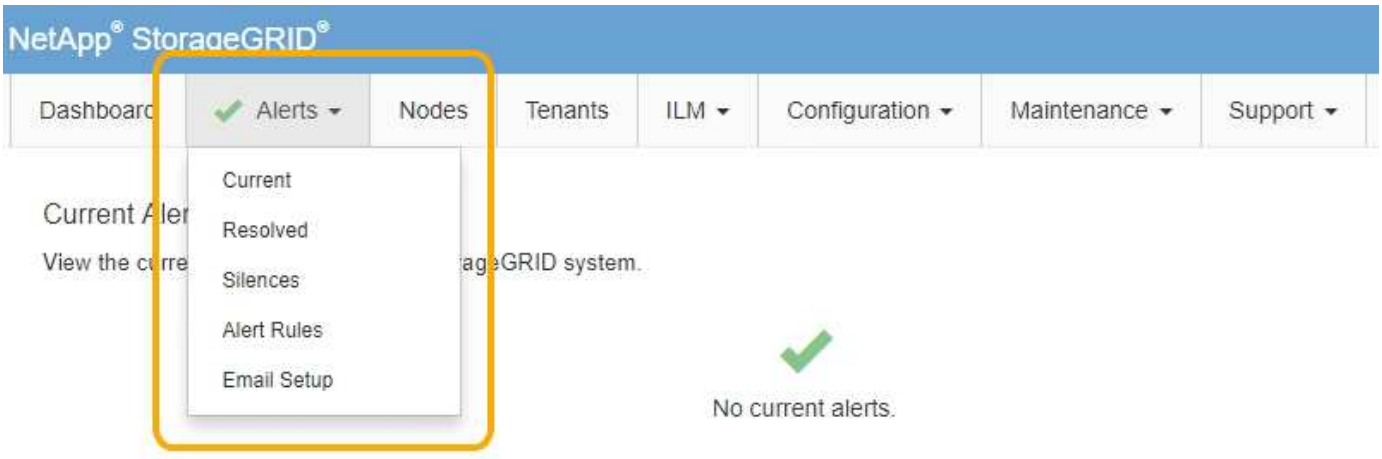
Para obter uma explicação das informações em cada painel, clique no ícone de ajuda desse painel.

Informações relacionadas

"Monitorizar Resolução de problemas"

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:

- Reveja os alertas atuais
- Reveja os alertas resolvidos

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

Informações relacionadas

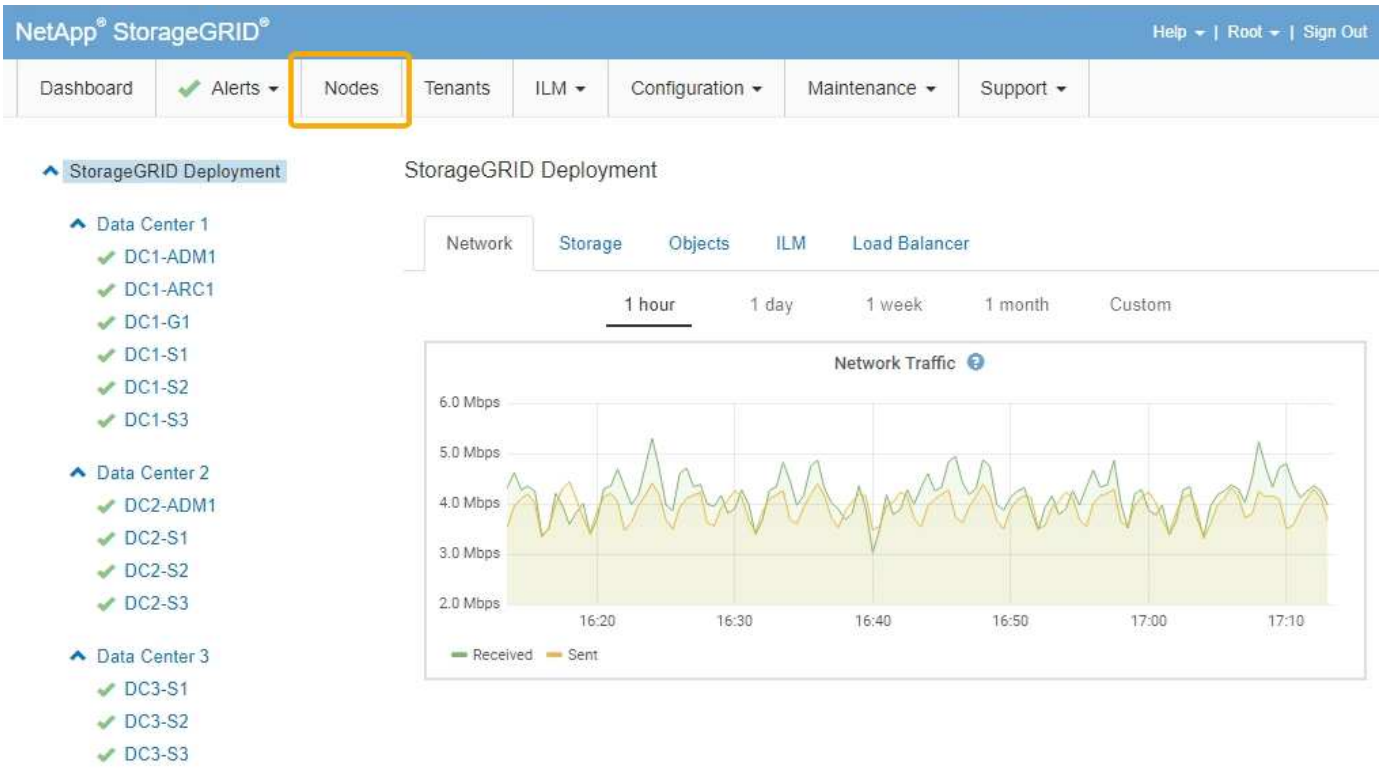
"Monitoramento e gerenciamento de alertas"

"Monitorizar Resolução de problemas"

Página de nós

A página 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, clique no link apropriado à esquerda.



Informações relacionadas

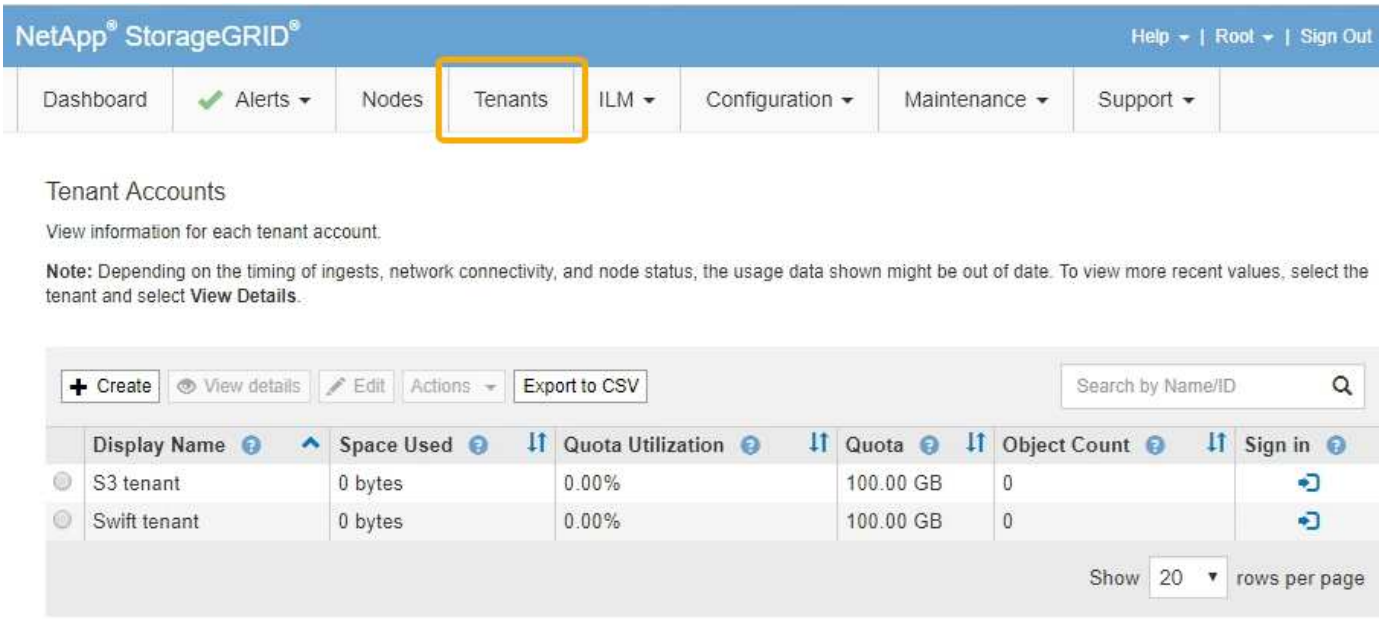
"Exibindo a página de nós"

"Monitorizar Resolução de problemas"

Página de contas de inquilino

A página Contas do locatário permite criar e monitorar as contas de locatário de storage do 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 Contas do locatário também fornece detalhes de uso para cada locatário, incluindo a quantidade de armazenamento usado e o número de objetos. Se você definir uma cota quando criou o locatário, poderá ver quanto dessa cota foi usada.



Informações relacionadas

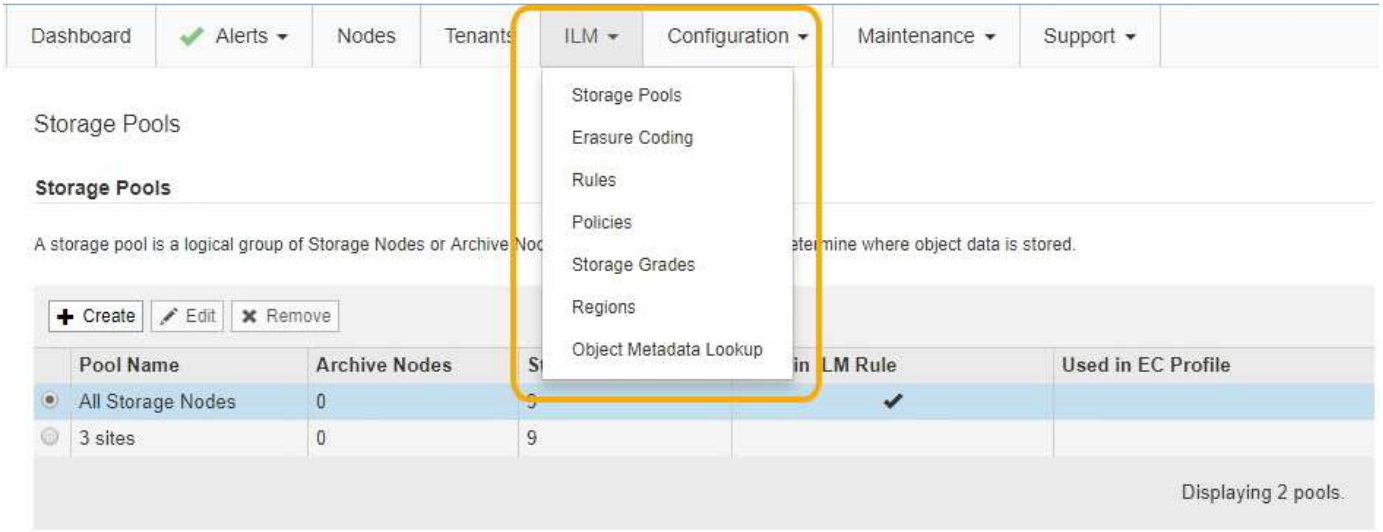
"Gerenciamento de locatários e conexões de clientes"

"Administrar o StorageGRID"

"Use uma conta de locatário"

Menu ILM

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



Informações relacionadas

"Uso do gerenciamento do ciclo de vida das informações"

"Gerenciar objetos com ILM"

Menu de configuração

O menu Configuration (Configuração) permite especificar definições de rede, definições do sistema, opções de monitorização e opções de controlo de acesso.

Informações relacionadas

"Configurar definições de rede"

"Gerenciamento de locatários e conexões de clientes"

"Rever mensagens de auditoria"

"Controlar o acesso à StorageGRID"

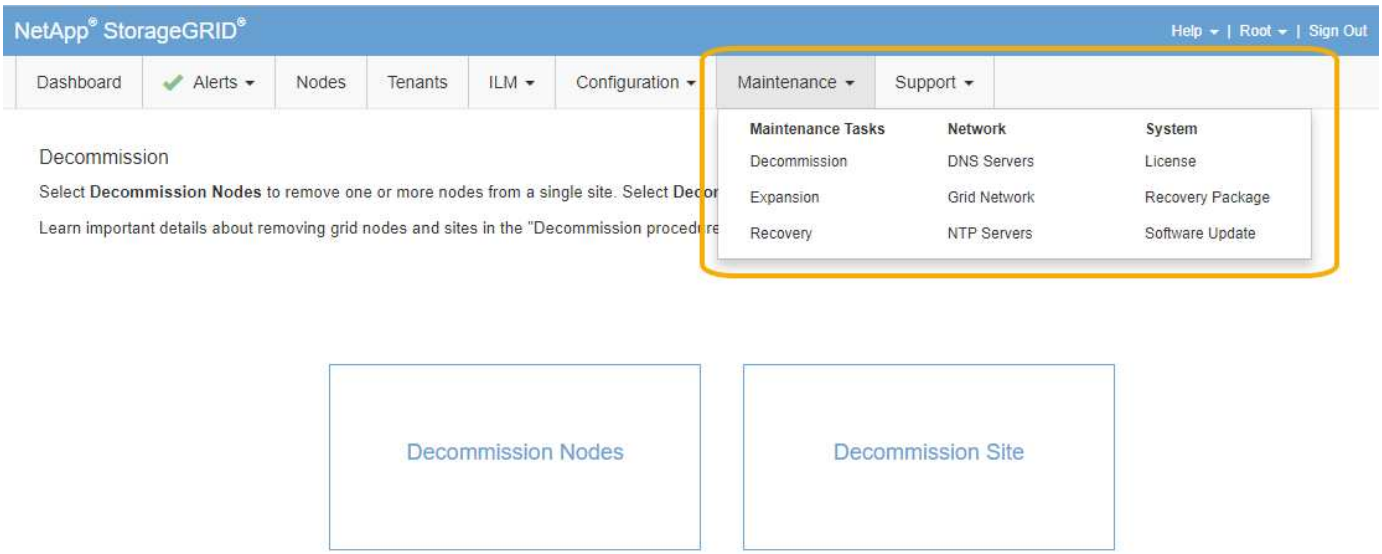
"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

"Rever registos de auditoria"

Menu de manutenção

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



Tarefas de manutenção

As tarefas de manutenção incluem:

- Desativar operações para remover locais e nós de grade não utilizados.
- Operações de expansão para adicionar novos nós de grade e locais.
- Operações de recuperação para substituir um nó com falha e restaurar dados.

Rede

As tarefas de rede que podem ser executadas no menu Manutenção incluem:

- Editando informações sobre servidores DNS.
- Configurando as sub-redes que são usadas na rede de Grade.
- Editando informações sobre servidores NTP.

Sistema

As tarefas do sistema que podem ser executadas no menu Manutenção incluem:

- Rever detalhes da licença atual do StorageGRID ou carregar uma nova licença.
- Gerando um pacote de recuperação.
- Executar atualizações de software do StorageGRID, incluindo atualizações de software, hotfixes e atualizações do software SANtricity os em dispositivos selecionados.

Informações relacionadas

"Executar procedimentos de manutenção"

"Transferir o pacote de recuperação"

"Expanda sua grade"

"Atualizar o software"

"Manter recuperar"

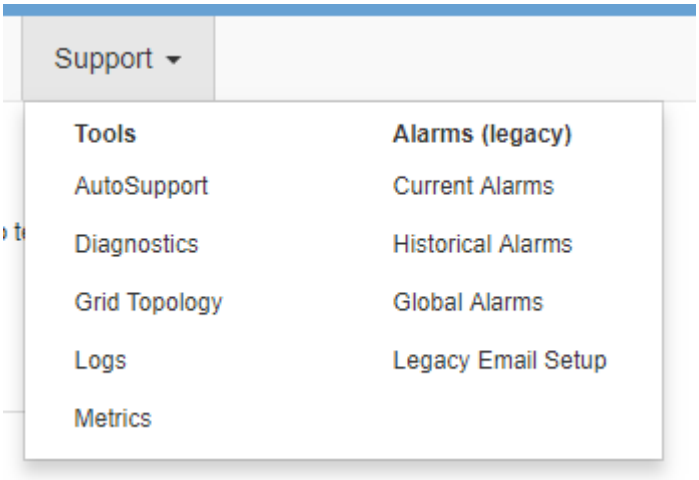
"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

Menu de suporte

O menu suporte fornece opções que ajudam o suporte técnico a analisar e solucionar problemas do seu sistema. Existem duas partes no menu suporte: Ferramentas e Alarmes (legado).



Ferramentas

Na seção Ferramentas do menu suporte, você pode:

- Ative o AutoSupport.
- Execute um conjunto de verificações de diagnóstico no estado atual da grelha.
- Acesse a árvore de topologia de grade para exibir informações detalhadas sobre nós, serviços e atributos de grade.
- Recuperar arquivos de log e dados do sistema.
- Analise métricas e gráficos detalhados.

> 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)

Na seção Alarmes (legado) do menu suporte, você pode revisar alarmes atuais, históricos e globais e configurar notificações por e-mail para alarmes legados e AutoSupport.

Informações relacionadas

"Topologia de rede e arquitetura StorageGRID"

"Atributos do StorageGRID"

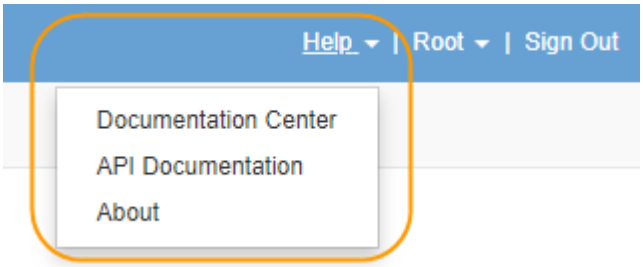
"Usando as opções de suporte do StorageGRID"

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

Menu Ajuda

A opção Ajuda fornece acesso ao Centro de Documentação do StorageGRID para a versão atual e para a documentação da API. Você também pode determinar qual versão do StorageGRID está instalada atualmente.



Informações relacionadas

"Administrar o StorageGRID"

Explorando o gerente do locatário

O Tenant Manager é a interface gráfica baseada em navegador que os usuários locatários acessam para configurar, gerenciar e monitorar suas contas de storage.

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

Informações relacionadas

"Explorando o Gerenciador de Grade"

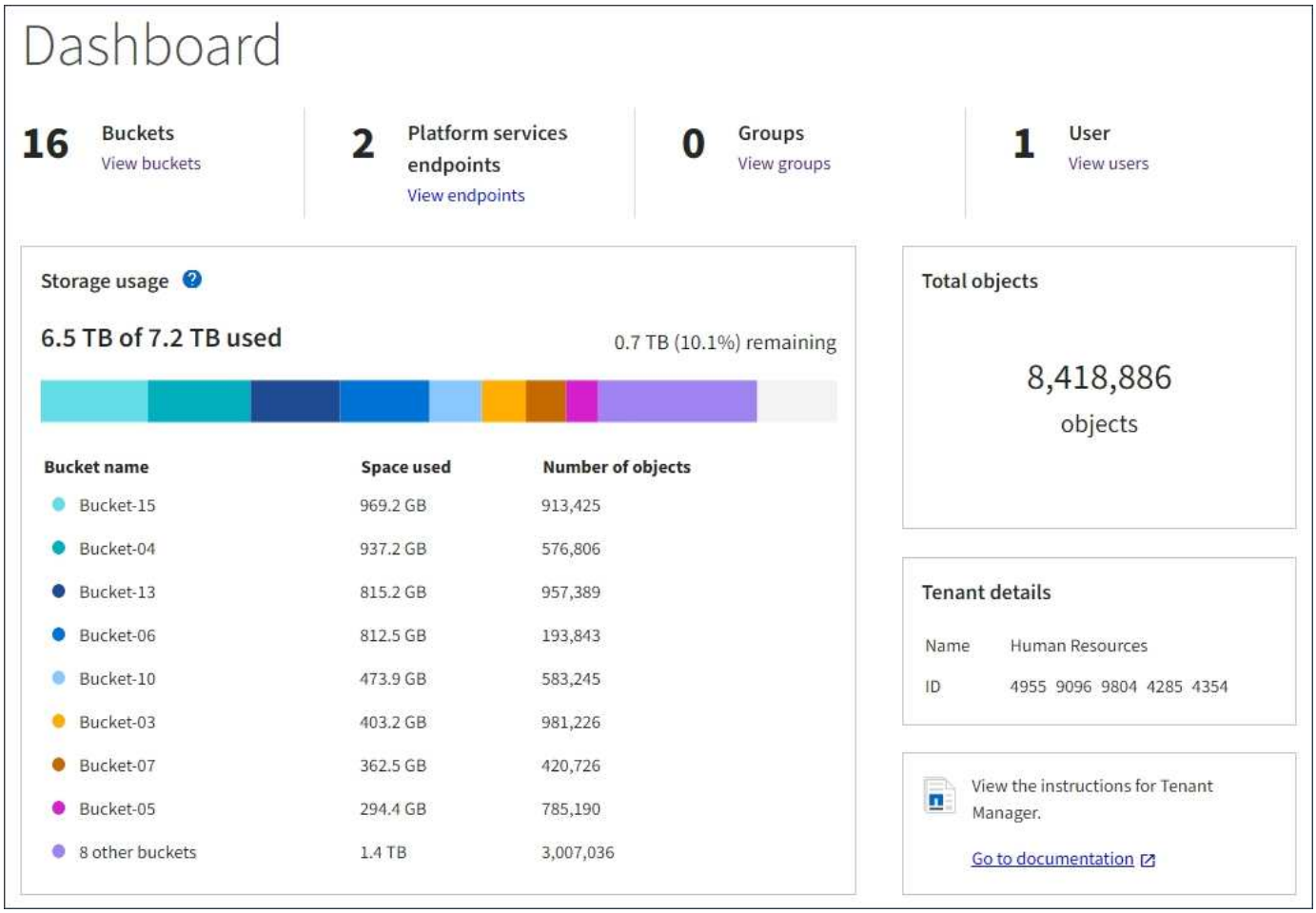
"Use uma conta de locatário"

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 storage (somente S3 locatários)

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 e excluam buckets e gerenciem endpoints de serviço da plataforma.

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 relacionadas aos 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 as definições do nível de consistência
- Configurar o compartilhamento de recursos entre origens (CORS)
- Ative e desative as configurações de atualização da última hora de acesso para os buckets pertencentes ao locatário
- Exclua buckets vazios

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:

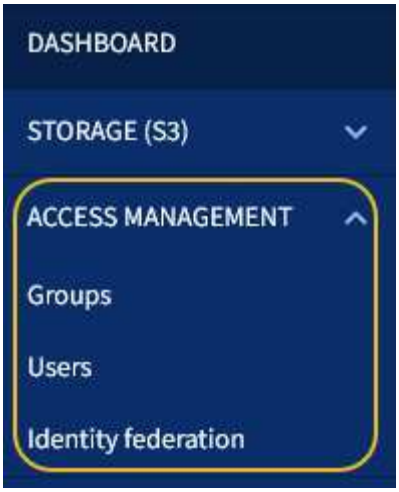
- Configure as notificações de eventos do S3, que podem ser enviadas para um serviço de destino compatível com o AWS Simple Notification Service (SNS).
- Configure a replicação do CloudMirror, que permite que o locatário replique automaticamente objetos para um bucket externo do S3.
- Configure a integração 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 do S3 com a permissão Gerenciar Endpoints poderá configurar um endpoint de destino para cada serviço de plataforma.

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.



Usando o StorageGRID

Depois de instalar nós de grade e redes StorageGRID, você pode começar a configurar e usar o StorageGRID. Algumas das tarefas que você executará incluem controlar o acesso do usuário às funções de administração do sistema, configurar contas de locatários , gerenciar conexões de clientes, definir opções de configuração, gerenciar locais de objetos com ILM, monitorar a integridade e as atividades diárias do seu sistema StorageGRID e realizar atividades de manutenção rotineiras e não rotineiras.

- "Controlar o acesso à StorageGRID"
- "Gerenciamento de locatários e conexões de clientes"
- "Configurar definições de rede"
- "Configurar as definições do sistema"
- "Uso do gerenciamento do ciclo de vida das informações"
- "Monitoramento das operações do StorageGRID"
- "Executar procedimentos de manutenção"
- "Usando as opções de suporte do StorageGRID"

Controlar 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.

Controlar 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 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. 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 permissões diferentes 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.

Ativar o início de sessão único

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0). Quando o SSO está ativado, 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 utilizadores locais não podem iniciar sessão no StorageGRID.

Quando o SSO está ativado e os usuários entram no StorageGRID, eles são redirecionados para a página SSO da sua organização para validar suas credenciais. Quando os usuários fazem logout de um nó de administrador, eles são automaticamente excluídos de todos os nós de administração.

Usando certificados de cliente

Você pode usar certificados de cliente para permitir que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. Os certificados de cliente fornecem uma maneira segura de usar ferramentas externas para monitorar o StorageGRID. Você pode fornecer seu próprio certificado de cliente ou gerar um usando o Gerenciador de Grade.

Alterando senhas de grade

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. Pode alterar esta frase-passe conforme necessário.

Informações relacionadas

"Administrar o StorageGRID"

"Use uma conta de locatário"

Gerenciamento de locatários e conexões de clientes

Como administrador de grade, você cria e gerencia as contas de locatário que os clientes S3 e Swift usam para armazenar e recuperar objetos e gerencia as opções de configuração que controlam como os clientes se conetam ao seu sistema StorageGRID.

Contas de inquilino

Uma conta de locatário permite que você especifique quem pode usar seu sistema StorageGRID para armazenar e recuperar objetos e qual funcionalidade está disponível para eles. As contas de locatário permitem que aplicativos clientes que suportam a API REST do S3 ou a API REST do Swift armazenem e recuperem objetos no StorageGRID. Cada conta de locatário usa o protocolo cliente S3 ou o protocolo cliente

Swift.

Você deve criar pelo menos uma conta de locatário para cada protocolo de cliente que será usado para armazenar objetos em seu sistema StorageGRID. Opcionalmente, você pode criar contas de locatário adicionais se quiser segregar os objetos armazenados em seu sistema por diferentes entidades. Cada conta de locatário tem seus próprios grupos e usuários federados ou locais, e seus próprios buckets (contentores para Swift) e objetos.

Você pode usar o Gerenciador de Grade ou a API de Gerenciamento de Grade para criar contas de locatário. Ao criar uma conta de locatário, você especifica as seguintes informações:

- Nome de exibição para o locatário (o ID da conta do locatário é atribuído automaticamente e não pode ser alterado).
- Se a conta de locatário usará o S3 ou Swift.
- Para contas de inquilino S3: Se a conta de inquilino tem permissão para usar serviços de plataforma. Se o uso de serviços de plataforma for permitido, a grade deve ser configurada para suportar seu uso.
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).
- Se a federação de identidade estiver ativada para o sistema StorageGRID, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.
- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.

Se as contas de locatário do S3 precisarem cumprir os requisitos regulamentares, os administradores de grade poderão habilitar a configuração global de bloqueio de objetos do S3 para o sistema StorageGRID. Quando o bloqueio de objeto S3 está ativado para o sistema, todas as contas de inquilino S3 podem criar buckets com o bloqueio de objeto S3 ativado e, em seguida, especificar as configurações de retenção e retenção legal para as versões de objeto nesse bucket.

Depois que uma conta de locatário for criada, os usuários do locatário poderão entrar no Gerenciador do locatário.

Conexões de cliente com nós StorageGRID

Antes que os usuários do locatário possam usar clientes S3 ou Swift para armazenar e recuperar dados no StorageGRID, você deve decidir como esses clientes se conetarão aos nós do StorageGRID.

Os aplicativos clientes podem armazenar ou recuperar objetos conetando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway. Esta é a ligação recomendada.
- O serviço CLB nos nós de Gateway.

  O serviço CLB está obsoleto.

- Nós de storage, com ou sem um balanceador de carga externo.

Ao configurar o StorageGRID para que os clientes possam usar o serviço Load Balancer, execute as seguintes etapas:

1. Configure endpoints para o serviço Load Balancer. O serviço Load Balancer em nós de administração ou

nós de gateway distribui conexões de rede recebidas de aplicativos clientes para nós de storage. Ao criar um endpoint de balanceador de carga, você especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).

2. Opcionalmente, especifique que a rede de cliente de um nó não é confiável para garantir que todas as conexões à rede de cliente do nó ocorram nos pontos de extremidade do balanceador de carga.
3. Configurar opcionalmente grupos de alta disponibilidade (HA). Se você criar um grupo de HA, as interfaces de vários nós de Admin e nós de Gateway serão colocadas em uma configuração de backup ativo. As conexões de cliente são feitas usando o endereço IP virtual do grupo HA.

Informações relacionadas

"Administrar o StorageGRID"

"Use uma conta de locatário"

"Use S3"

"Use Swift"

"Explorando o gerente do locatário"

"Configurar definições de rede"

Configurar definições de rede

Você pode configurar várias configurações de rede do Gerenciador de Grade para ajustar a operação do sistema StorageGRID.

Nomes de domínio

Se você planeja oferecer suporte a S3 solicitações virtuais de estilo hospedado, você deve configurar a lista de nomes de domínio de endpoint aos quais os clientes S3 se conetam. Exemplos incluem s3.example.com, s3.example.co.uk e s3-east.example.com.

Os certificados de servidor configurados devem corresponder aos nomes de domínio de endpoint.

Grupos de alta disponibilidade

Os grupos de alta disponibilidade usam endereços IP virtuais (VIPs) para fornecer acesso de backup ativo aos serviços do nó de gateway ou nó de administrador. Um grupo de HA consiste em uma ou mais interfaces de rede em nós de administração e nós de gateway. Ao criar um grupo HA, você seleciona interfaces de rede pertencentes à rede Grid (eth0) ou à rede Client (eth2).

A rede de administração não suporta VIPs HA.

Um grupo de HA mantém um ou mais endereços IP virtuais que são adicionados à interface ativa no grupo. Se a interface ativa ficar indisponível, os endereços IP virtuais serão movidos para outra interface. Esse 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.

Você pode querer usar grupos de alta disponibilidade (HA) por vários motivos.

- 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 e Swift.
- Um grupo de HA que contém apenas uma interface permite fornecer muitos endereços VIP e definir explicitamente endereços IPv6.

Vincular custos

Você pode ajustar os custos de link para refletir a latência entre sites. Quando existem dois ou mais locais de data center, os custos de link priorizam qual local de data center deve fornecer um serviço solicitado.

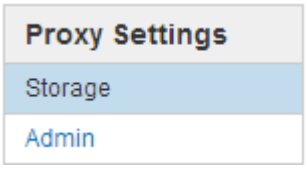
Pontos de extremidade do balanceador de carga

Você pode usar um balanceador de carga para lidar com cargas de trabalho de ingestão e recuperação de clientes S3 e Swift. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo cargas de trabalho e conexões entre vários nós de storage.

Se você quiser usar o serviço balanceador de carga do StorageGRID, que está incluído em nós de administração e nós de gateway, configure um ou mais pontos de extremidade do balanceador de carga. Cada endpoint define uma porta de nó de gateway ou nó de administrador para solicitações S3 e Swift para nós de storage.

Configurações de proxy

Se você estiver usando serviços de plataforma S3 ou pools de storage em nuvem, poderá configurar um servidor proxy não transparente entre nós de storage e os pontos de extremidade externos do S3. Se você enviar mensagens AutoSupport usando HTTPS ou HTTP, poderá configurar um servidor proxy não transparente entre nós de administração e suporte técnico.



Certificados de servidor

Você pode carregar dois tipos de certificados de servidor:

- Certificado do servidor de interface de gerenciamento, que é o certificado usado para acessar a interface de gerenciamento.
- Object Storage API Service Endpoints Server Certificate, que protege os endpoints S3 e Swift para conexões diretamente aos nós de armazenamento ou ao usar o serviço CLB em um nó de gateway.

> O serviço CLB está obsoleto.

Os certificados do balanceador de carga são configurados na página pontos finais do balanceador de carga. Os certificados do servidor de gerenciamento de chaves (KMS) são configurados na página servidor de gerenciamento de chaves.

Políticas de classificação de tráfego

As políticas de classificação de tráfego permitem criar regras para identificar e lidar com 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.

Redes de clientes não confiáveis

Se você estiver usando uma rede cliente, você pode ajudar a proteger o StorageGRID contra ataques hostis especificando que a rede cliente em cada nó não é 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.

Por exemplo, você pode querer que um nó de gateway recuse todo o tráfego de entrada na rede cliente, exceto para solicitações HTTPS S3. Ou, talvez você queira habilitar o tráfego de serviço de plataforma S3 de saída de um nó de armazenamento, ao mesmo tempo em que evita conexões de entrada para esse nó de armazenamento na rede do cliente.

Informações relacionadas

"Administrar o StorageGRID"

"Gerenciamento de locatários e conexões de clientes"

Configurar as definições do sistema

Você pode configurar várias configurações do sistema a partir do Gerenciador de Grade para ajustar a operação do seu sistema StorageGRID.

Opções de visualização

As opções de exibição permitem especificar o período de tempo limite para sessões do usuário e suprimir notificações de e-mail para alarmes legados e mensagens AutoSupport acionadas por eventos.

Opções de grelha

Você pode usar Opções de Grade para configurar as configurações de todos os objetos armazenados no seu sistema StorageGRID, incluindo compactação de objetos armazenados, criptografia de objetos armazenados e hash de objetos armazenados.

Você também pode usar essas opções para especificar configurações globais para operações de cliente S3 e Swift.

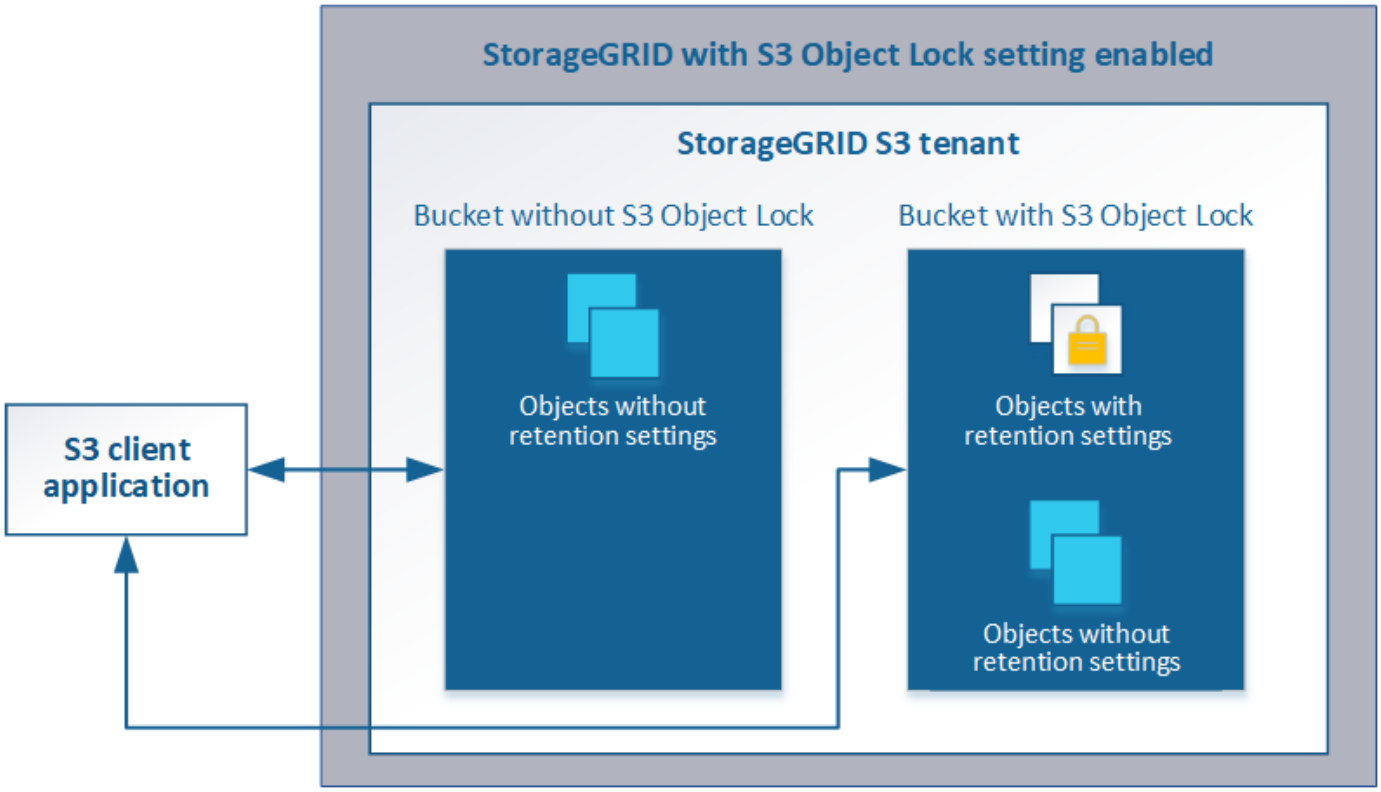
Servidores de gerenciamento de chaves

Você pode configurar um ou mais servidores de gerenciamento de chaves externos (KMS) para fornecer chaves de criptografia para serviços StorageGRID e dispositivos de armazenamento. Cada cluster de KMS ou KMS usa o Key Management Interoperability Protocol (KMIP) para fornecer uma chave de criptografia aos nós do dispositivo no site associado do StorageGRID. O uso de servidores 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.

S3 bloqueio de objetos

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). Você pode habilitar a configuração global de bloqueio de objeto S3 para um sistema StorageGRID para permitir que as contas de locatário S3 criem buckets com o bloqueio de objeto S3 ativado. O locatário pode então usar um aplicativo cliente S3 para especificar opcionalmente as configurações de retenção (reter até a data, retenção legal ou ambos) para os objetos nesses buckets.



Opções de armazenamento

As opções de armazenamento permitem controlar a segmentação de objetos e definir marcas d'água de armazenamento para gerenciar o espaço de armazenamento utilizável de um nó de armazenamento.

Uso do gerenciamento do ciclo de vida das informações

Use o gerenciamento do ciclo de vida das informações (ILM) para controlar o posicionamento, a duração e a proteção de dados 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.

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, em pools de storage de nuvem ou em nós de arquivamento.

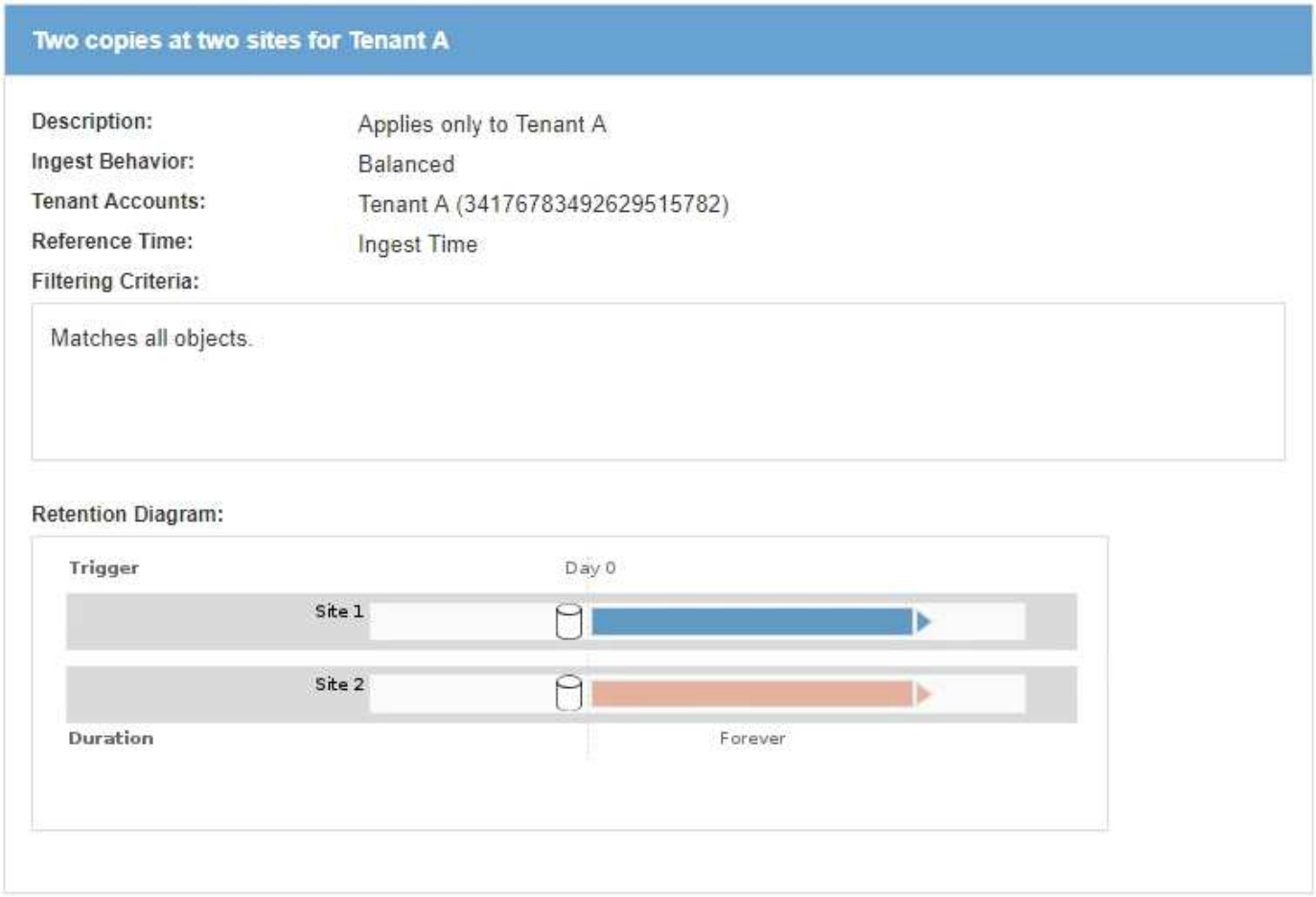
- O tipo de cópias de objeto feitas. As cópias podem ser replicadas ou codificadas para apagamento.
- Para cópias replicadas, o número de cópias feitas.
- Para cópias codificadas de apagamento, o esquema de codificação de apagamento usado.
- As alterações ao longo do tempo para o local de armazenamento 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. As cópias são distribuídas uniformemente por todos os nós de storage.

Exemplo de regra ILM

Este exemplo de regra ILM aplica-se aos objetos pertencentes ao locatário A. Ele faz duas cópias replicadas desses objetos e armazena cada cópia em um local diferente. As duas cópias são retidas para sempre, o que significa que o StorageGRID não as apagará 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.

Esta regra usa a opção equilibrada para o 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

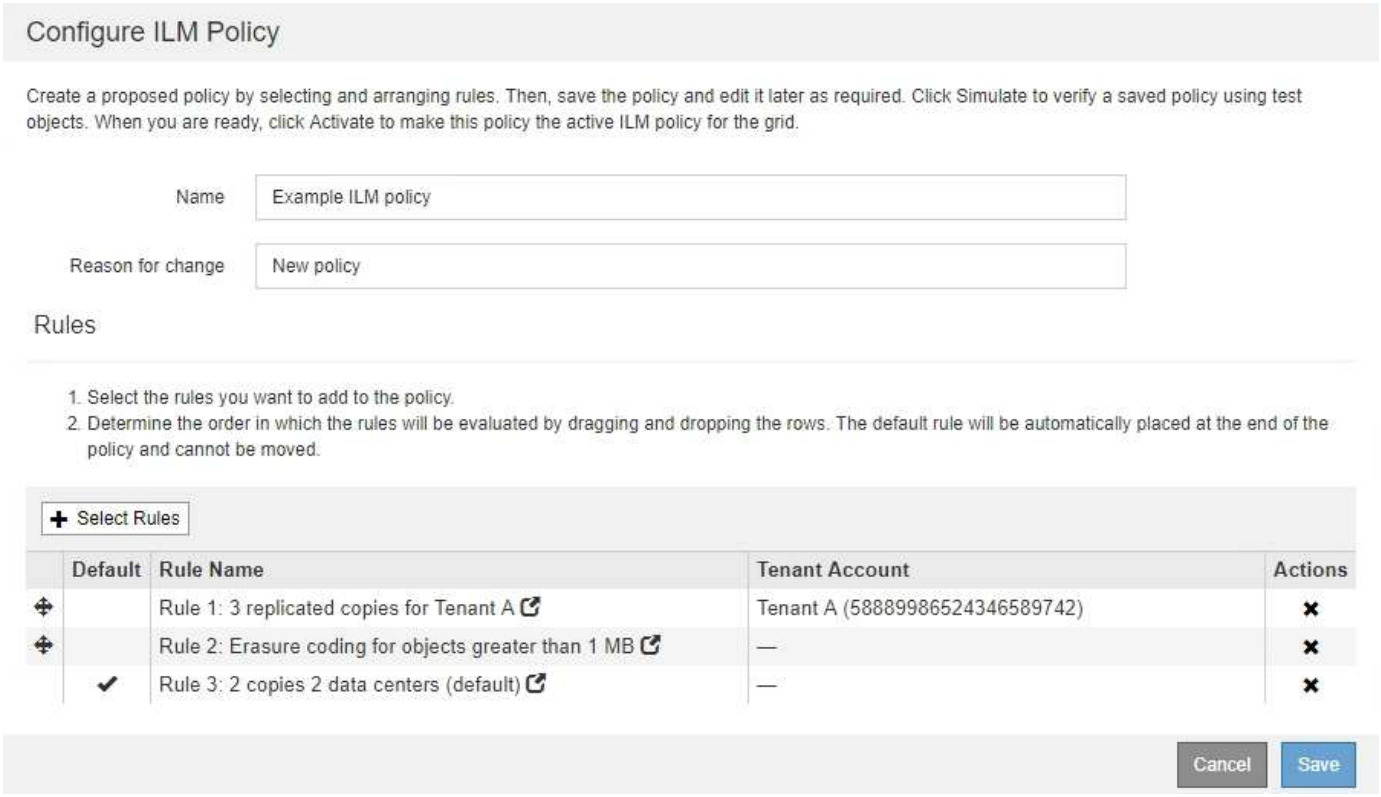
A política de ILM ativa do seu sistema StorageGRID controla o posicionamento, a duração e a proteção de dados de todos os objetos.

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.

Exemplo de política ILM

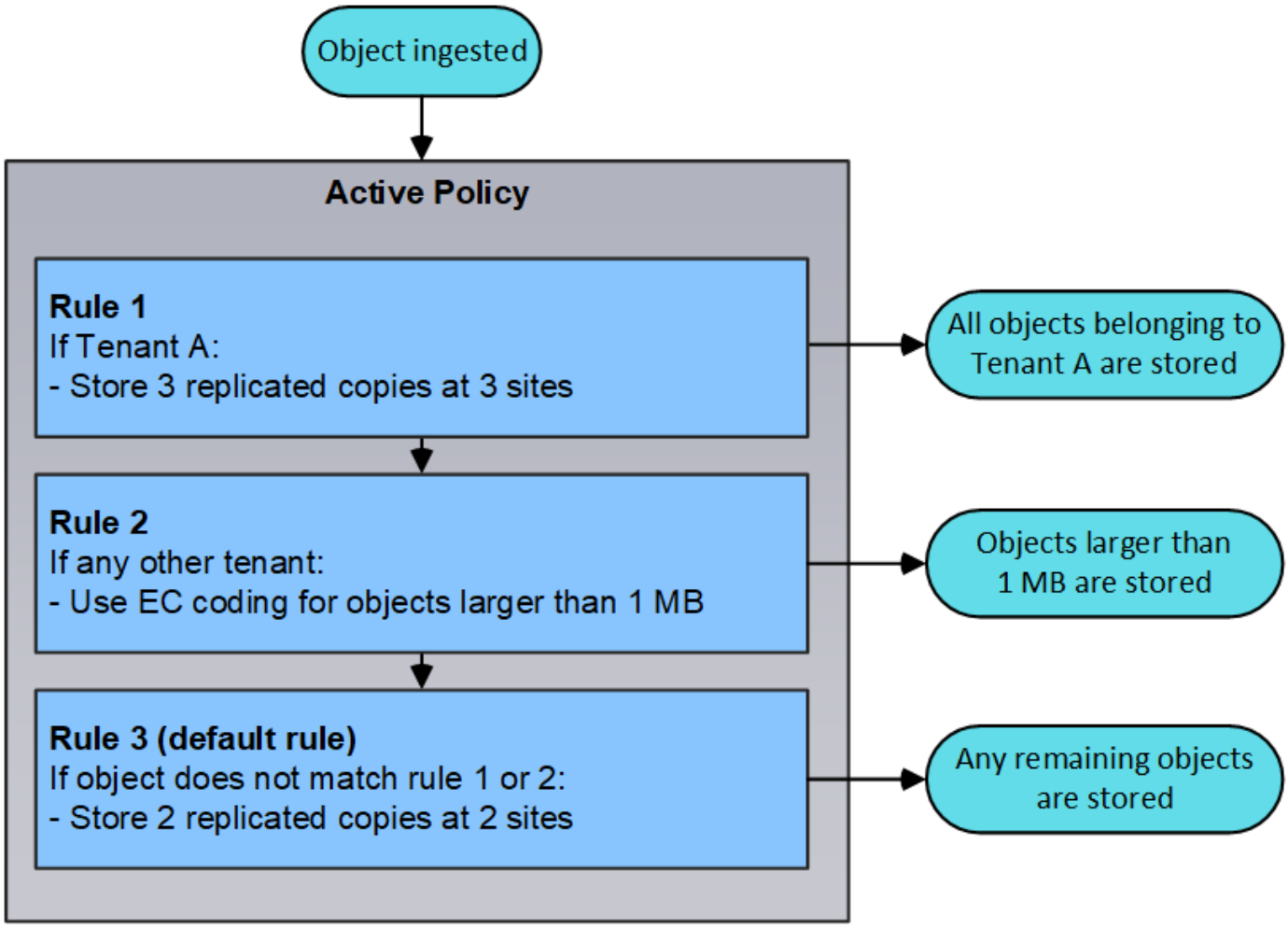
Este exemplo de política ILM usa três regras ILM.



Neste exemplo, a regra 1 corresponde a todos os objetos pertencentes ao locatário A. esses objetos são armazenados como três cópias replicadas em três locais. Os objetos pertencentes a outros inquilinos não são correspondidos pela regra 1, por isso são avaliados em relação à regra 2.

A regra 2 corresponde a 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. A regra 2 não corresponde a objetos de 1 MB ou menores, portanto, esses objetos são avaliados em relação à regra 3.

A regra 3 é a última regra padrão da política e não usa filtros. A regra 3 faz duas cópias replicadas de todos os objetos não correspondidos pela regra 1 ou pela regra 2 (objetos que não pertencem ao locatário A com 1 MB ou menos).



Informações relacionadas

"Gerenciar objetos com ILM"

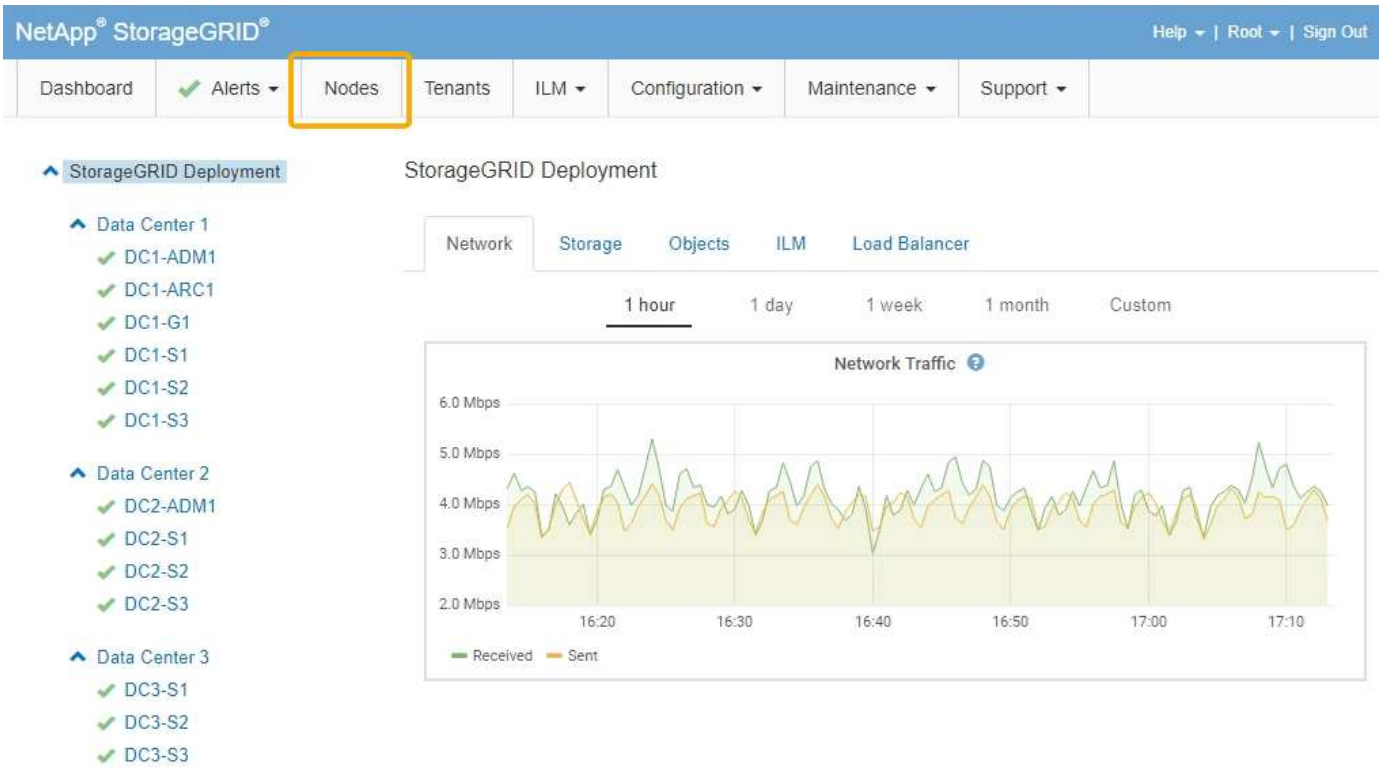
Monitoramento das operações do StorageGRID

O Gerenciador de Grade fornece informações para monitorar as atividades diárias do seu sistema StorageGRID, incluindo sua integridade.

- "Exibindo a página de nós"
- "Monitoramento e gerenciamento de alertas"
- "Utilizar a monitorização SNMP"
- "Rever mensagens de auditoria"

Exibindo a página de nós

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



Na exibição em árvore à esquerda, você pode ver todos os sites e todos os nós no seu sistema StorageGRID. O ícone de cada nó indica se o nó está conetado ou se há alertas ativos.

Ícones de estado da ligação

Se um nó for desconetado da grade, a exibição em árvore mostrará um ícone de estado de conexão azul ou cinza, e não o ícone de alertas subjacentes.

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

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

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

Ícones de alerta

Se um nó estiver conetado à grade, a exibição em árvore mostrará um dos ícones a seguir, dependendo se houver algum alerta atual para o nó.

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

subjacentes para garantir que a condição anormal não pare a operação normal de um nó ou serviço StorageGRID.

- **Minor** ⚠: o sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.
- **Normal** ✔: nenhum alerta está ativo e o nó está conetado à grade.

Exibindo detalhes de um sistema, site ou nó

Para visualizar as informações disponíveis, clique nos links apropriados à esquerda, como segue:

- Selecione o nome da grade para ver um resumo agregado das estatísticas de todo o seu sistema StorageGRID. (A captura de tela mostra um sistema chamado implantação do 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.

Informações relacionadas

"Monitorizar Resolução de problemas"

Guias para a página nós

As guias na parte superior da página nós são baseadas no que você seleciona na árvore à esquerda.

Nome do separador	Descrição	Incluído para
Visão geral	• Fornece informações básicas sobre cada nó. • Mostra todos os alarmes atuais e não reconhecidos que afetam o nó.	Todos os nós
Hardware	• Exibe a utilização da CPU e o uso da memória para cada nó • Para nós do dispositivo, fornece informações adicionais de hardware.	Todos os nós
Rede	Exibe um gráfico mostrando o tráfego de rede recebido e enviado através das interfaces de rede.	Todos os nós, cada local e toda a grade
Armazenamento	• Fornece detalhes para os dispositivos de disco e volumes em cada nó. • Para nós de storage, cada local e toda a grade incluem gráficos que mostram o storage de dados de objetos e o storage de metadados usados ao longo do tempo.	Todos os nós, cada local e toda a grade
Eventos	Exibe uma contagem de qualquer erro de sistema ou evento de falha, incluindo erros como erros de rede.	Todos os nós

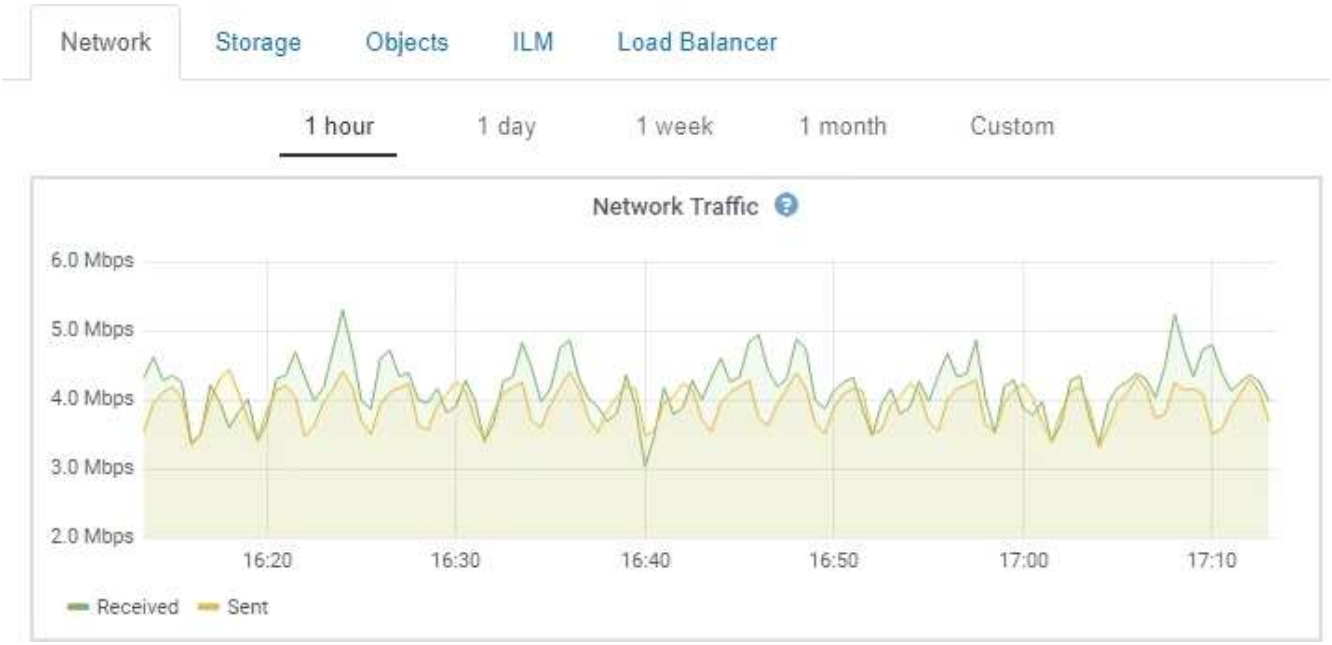
Nome do separador	Descrição	Incluído para
Objetos	• Fornece informações sobre as taxas de ingestão e recuperação S3 e Swift. • Para nós de storage, fornece contagens de objetos e informações sobre consultas de armazenamento de metadados e verificação em segundo plano.	Nós de storage, cada local e toda a grade
ILM	Fornece informações sobre as operações do Information Lifecycle Management (ILM). • Para nós de storage, fornece detalhes sobre a avaliação do ILM e a verificação em segundo plano para objetos codificados de apagamento. • Para cada local e toda a grade, mostra um gráfico da fila ILM ao longo do tempo. • Para toda a grade, fornece o tempo estimado para concluir uma varredura ILM completa de todos os objetos.	Nós de storage, cada local e toda a grade
Balanceador de carga	Inclui gráficos de desempenho e diagnóstico relacionados com o serviço Load Balancer. • Para cada site, fornece um resumo agregado das estatísticas de todos os nós nesse site. • Para toda a grade, fornece um resumo agregado das estatísticas para todos os sites.	Nós de administração e nós de gateway, cada local e toda a grade
Serviços de plataforma	Fornece informações sobre qualquer operação de serviço da plataforma S3 em um site.	Cada local
Gerente do sistema da SANtricity	Fornece acesso ao Gerenciador do sistema do SANtricity. No SANtricity System Manager, você pode revisar as informações ambientais e de diagnóstico de hardware para o controlador de armazenamento, bem como os problemas relacionados às unidades.	Nós de dispositivos de storage **Nota:** a guia Gerenciador de sistema do SANtricity não aparecerá se o firmware do controlador no dispositivo de armazenamento for inferior a 8,70.

Métricas Prometheus

O serviço Prometheus nos Admin Nodes coleta métricas de séries temporais dos serviços em todos os nós.

As métricas coletadas por Prometheus são usadas em vários locais no Gerenciador de Grade:

- **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 de Gerenciamento de Grade (**Ajuda 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 **suporte Ferramentas Diagnóstico** e a página **suporte Ferramentas métricas**: Essas páginas, que são destinadas principalmente ao uso pelo suporte técnico, fornecem uma série de 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.

Informações relacionadas

"Monitoramento e gerenciamento de alertas"

"Usando as opções de suporte do StorageGRID"

"Monitorizar Resolução de problemas"

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 locais no Gerenciador de Grade:

- **Página de nós**: Muitos dos valores mostrados na página de nós são atributos StorageGRID. (As métricas Prometheus também são mostradas nas páginas de nós.)
- **Alarmes**: Quando os atributos atingem valores de limite definidos, os alarmes StorageGRID (sistema legado) são acionados em níveis de gravidade específicos.
- **Grid Topology tree**: Os valores de atributo são mostrados na árvore Grid Topology (**Support Tools Grid Topology**).
- **Eventos**: Os eventos do sistema ocorrem quando certos atributos Registram uma condição de erro ou falha para um nó, incluindo erros como erros de rede.

Valores de atributo

Os atributos são reportados com o melhor esforço e estão aproximadamente corretos. As atualizações de atributos podem ser perdidas em algumas circunstâncias, como a falha de um serviço ou a falha e reconstrução de um nó de grade.

Além disso, os atrasos de propagação podem retardar o relatório de atributos. Os valores atualizados para a maioria dos atributos são enviados para o sistema StorageGRID em intervalos fixos. Pode demorar vários minutos até que uma atualização seja visível no sistema, e dois atributos que mudam mais ou menos simultaneamente podem ser reportados em momentos ligeiramente diferentes.

Informações relacionadas

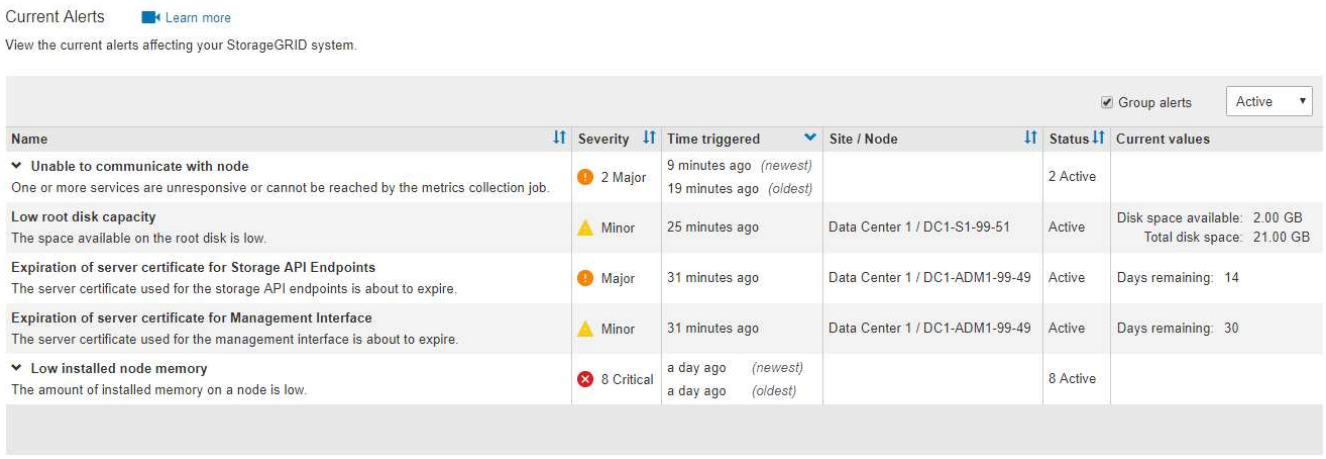
"Monitorizar Resolução de problemas"

Monitoramento e gerenciamento de alertas

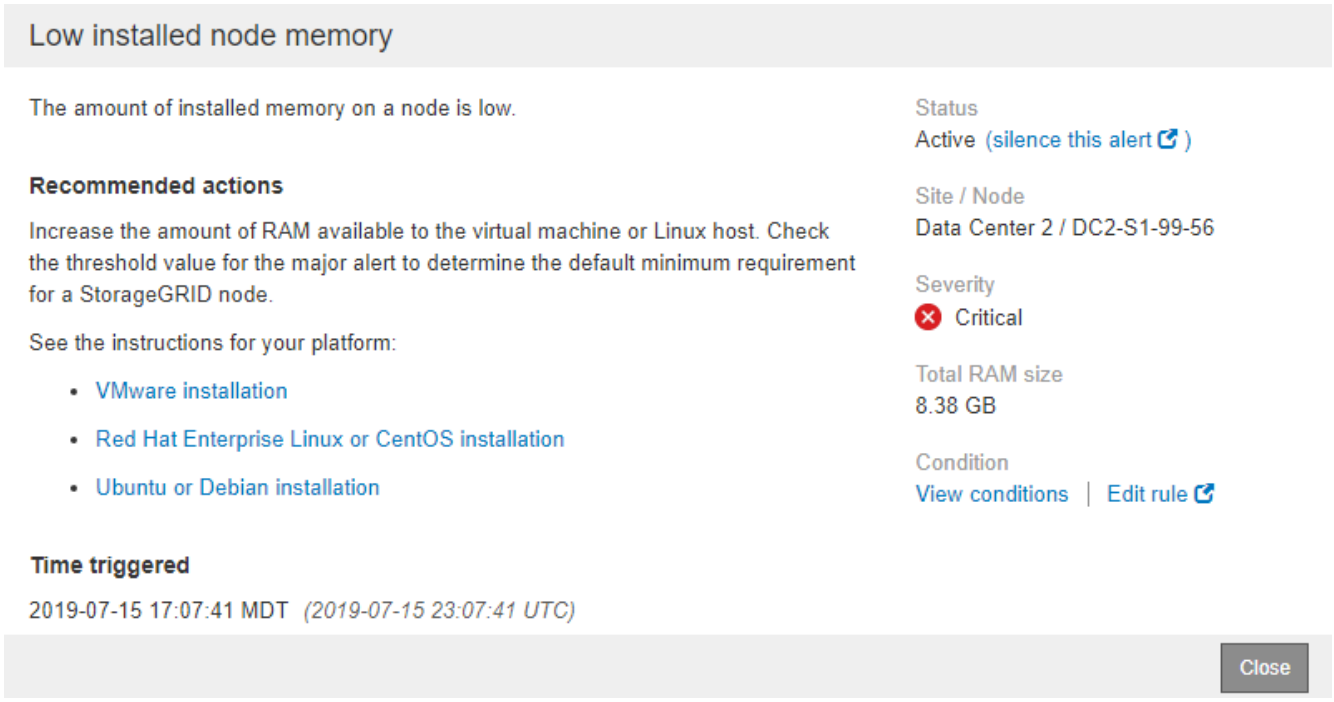
O sistema de alerta fornece uma interface fácil de usar para detetar, avaliar e resolver os problemas que podem ocorrer durante a operação do StorageGRID.

O sistema de alerta foi concebido para ser a sua principal ferramenta para monitorizar quaisquer problemas que possam ocorrer no seu sistema StorageGRID.

- O sistema de alerta se concentra em problemas acionáveis no sistema. Os alertas são acionados para eventos que exigem sua atenção imediata, não para eventos que podem ser ignorados com segurança.
- As páginas Alertas atuais e Alertas resolvidos fornecem uma interface amigável para a visualização de problemas atuais e históricos. Você pode classificar a lista por alertas individuais e grupos de alertas. Por exemplo, talvez você queira classificar todos os alertas por nó/site para ver quais alertas estão afetando um nó específico. Ou, talvez você queira classificar os alertas em um grupo por tempo acionado para encontrar a instância mais recente de um alerta específico.
- Vários alertas do mesmo tipo são agrupados em um e-mail para reduzir o número de notificações. Além disso, vários alertas do mesmo tipo são exibidos como um grupo nas páginas Alertas atuais e Alertas resolvidos. Você pode expandir e recolher grupos de alerta para mostrar ou ocultar os alertas individuais. Por exemplo, se vários nós estiverem relatando o alerta **não é possível se comunicar com nó**, apenas um email é enviado e o alerta é mostrado como um grupo na página Alertas atuais.



- Os alertas usam nomes e descrições intuitivas para ajudá-lo a entender mais rapidamente qual é o problema. As notificações de alerta incluem detalhes sobre o nó e o site afetado, a gravidade do alerta, o tempo em que a regra de alerta foi acionada e o valor atual das métricas relacionadas ao alerta.
- As notificações de alerta por e-mail e as listagens de alerta nas páginas Alertas atuais e alertas resolvidos fornecem ações recomendadas para resolver um alerta. Essas ações recomendadas geralmente incluem links diretos para a documentação do StorageGRID para facilitar a localização e o acesso a procedimentos de solução de problemas mais detalhados.



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

Gerenciamento de alertas

Todos os usuários do StorageGRID podem visualizar alertas. Se você tiver a permissão Acesso root ou Gerenciar Alertas, também poderá gerenciar alertas, como segue:

- Se você precisar suprimir temporariamente as notificações de um alerta em um ou mais níveis de gravidade, poderá silenciar facilmente uma regra de alerta específica por uma duração especificada. Você

pode silenciar uma regra de alerta para toda a grade, um único local ou um único nó.

- Você pode editar as regras de alerta padrão conforme necessário. Você pode desativar completamente uma regra de alerta ou alterar suas condições de ativação e duração.
- Você pode criar regras de alerta personalizadas para direcionar as condições específicas que são relevantes para a sua situação e para fornecer suas próprias ações recomendadas. Para definir as condições para um alerta personalizado, você cria expressões usando as métricas Prometheus disponíveis na seção métricas da API de Gerenciamento de Grade.

  Por exemplo, essa 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 < 24000000000
```

Informações relacionadas

"Monitorizar Resolução de problemas"

Utilizar a monitorização SNMP

Se você quiser monitorar o StorageGRID usando o Protocolo de Gerenciamento de rede simples (SNMP), você pode usar o Gerenciador de Grade para configurar o agente SNMP.

Cada nó do StorageGRID executa um agente SNMP, ou daemon, que fornece uma base de informações de gerenciamento (MIB). O MIB do StorageGRID contém definições de tabela e notificação para alertas e alarmes. Cada nó StorageGRID também suporta um subconjunto de objetos MIB-II.

Inicialmente, o SNMP está desativado em todos os nós. Quando você configura o agente SNMP, todos os nós do StorageGRID recebem a mesma configuração.

O agente SNMP do StorageGRID suporta todas as três versões do protocolo SNMP. O agente fornece acesso MIB somente leitura para consultas e pode enviar dois tipos de notificações orientadas a eventos para um sistema de gerenciamento:

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

Notificações de 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 configurar um silêncio para o alerta. As notificações de alerta são enviadas por qualquer nó Admin configurado para ser o remetente preferido.
- Certos alarmes (sistema legado) são acionados em níveis de gravidade especificados ou superiores.

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

Informações relacionadas

"Monitorizar Resolução de problemas"

Rever mensagens de auditoria

As mensagens de auditoria podem ajudá-lo a entender melhor as operações detalhadas do seu sistema StorageGRID. Você pode usar logs de auditoria para solucionar problemas e avaliar o desempenho.

Durante a operação normal do sistema, todos os serviços StorageGRID geram mensagens de auditoria, como segue:

- As mensagens de auditoria do sistema estão relacionadas ao próprio sistema de auditoria, aos estados dos nós da grade, à atividade de tarefas em todo o sistema e às operações de backup de serviço.
- As mensagens de auditoria de storage de objetos estão relacionadas ao armazenamento e gerenciamento de objetos no StorageGRID, incluindo armazenamento de objetos e recuperações, transferências de nó de grade para nó de grade e verificações.
- As mensagens de auditoria de leitura e gravação do cliente são registradas quando um aplicativo cliente S3 ou Swift faz uma solicitação para criar, modificar ou recuperar um objeto.
- As mensagens de auditoria de gerenciamento Registram solicitações de usuários para a API de gerenciamento.

Cada nó Admin armazena mensagens de auditoria em arquivos de texto. O compartilhamento de auditoria contém o arquivo ativo (audit.log), bem como logs de auditoria compatados de dias anteriores.

Para facilitar o acesso aos logs de auditoria, você pode configurar o acesso do cliente ao compartilhamento de auditoria para NFS e CIFS (obsoleto). Você também pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

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

Informações relacionadas

"Rever registos de auditoria"

"Administrar o StorageGRID"

Executar procedimentos de manutenção

Executa vários procedimentos de manutenção para manter o sistema StorageGRID atualizado e para garantir que está a funcionar de forma eficiente. O Gerenciador de Grade fornece ferramentas e opções para facilitar o processo de execução de tarefas de manutenção.

Atualizações de software

Você pode executar três tipos de atualizações de software na página Atualização de Software no Gerenciador de Grade:

- Atualização do software StorageGRID
- Hotfix do StorageGRID
- Atualização do sistema operacional SANtricity

Atualizações de software StorageGRID

Quando uma nova versão do recurso StorageGRID está disponível, a página Atualização de software orienta você pelo processo de upload do arquivo necessário e atualização do sistema StorageGRID. É necessário atualizar todos os nós de grade para todos os locais de data center a partir do nó de administração principal.

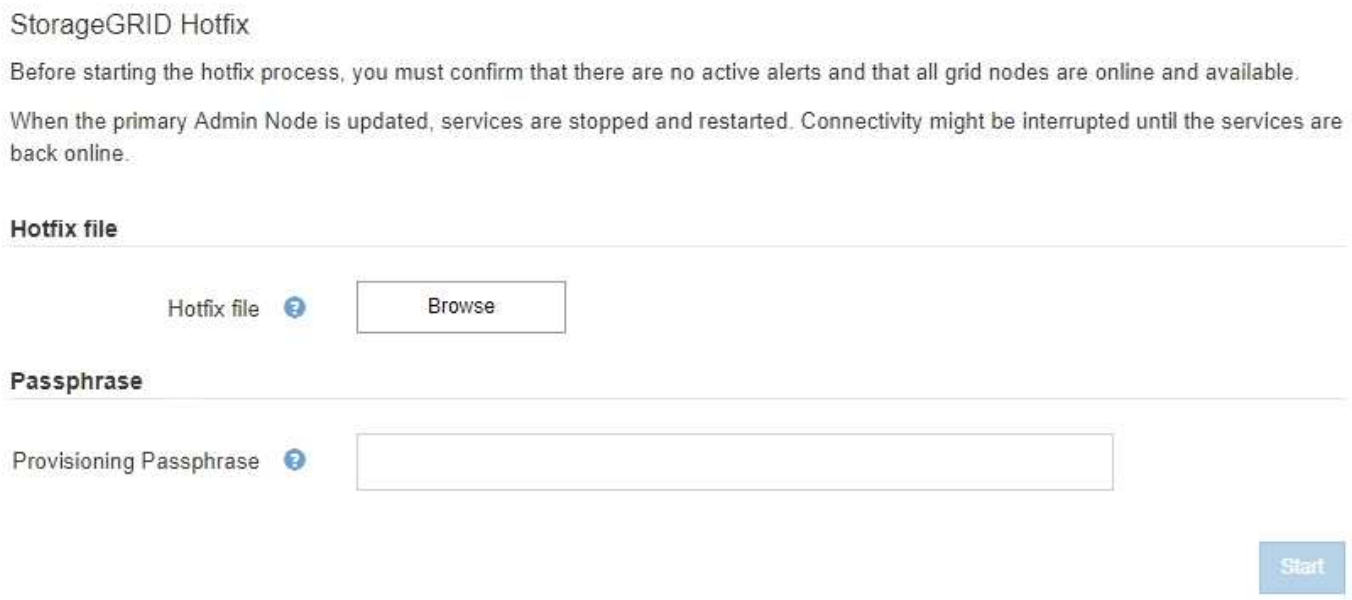
Durante uma atualização do software StorageGRID, os aplicativos clientes podem continuar a obter e obter dados de objetos.

Hotfixes

Se os problemas com o software forem detetados e resolvidos entre versões de recursos, talvez seja necessário aplicar um hotfix ao sistema StorageGRID.

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.

A página de hotfix do StorageGRID, mostrada abaixo, permite que você carregue um arquivo de hotfix.



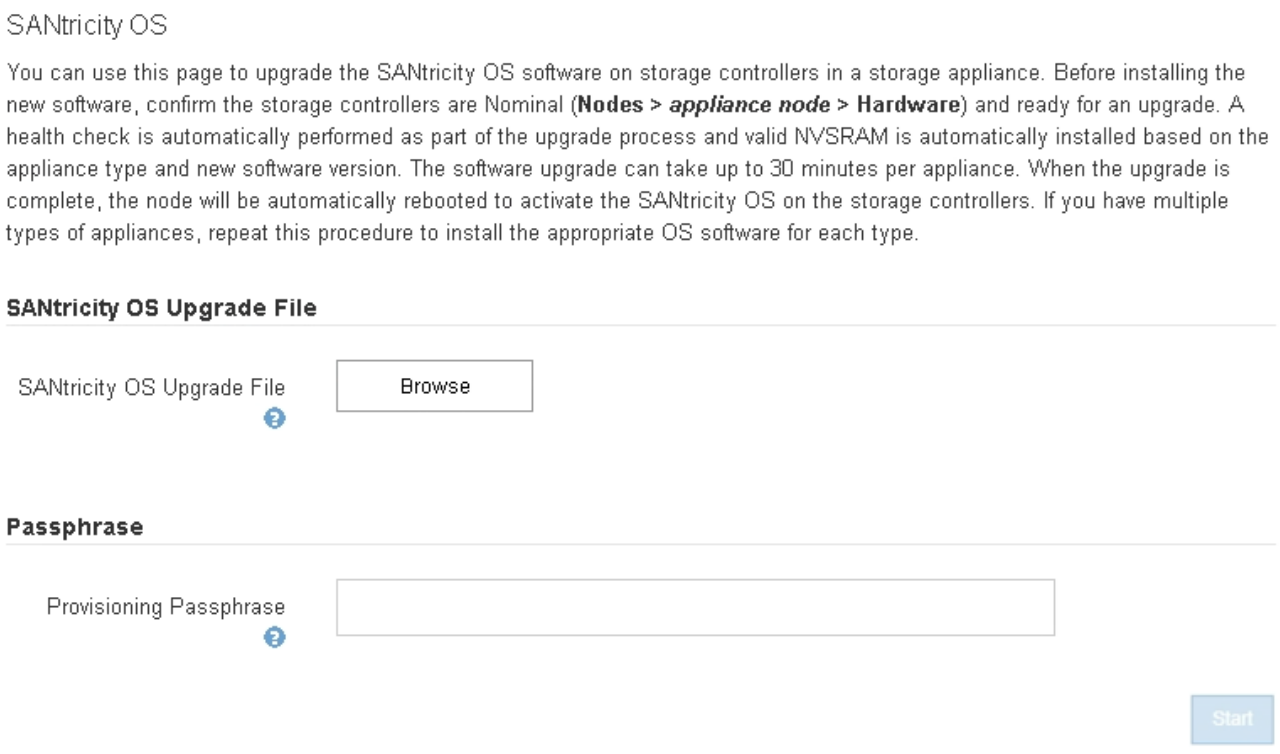
O hotfix é aplicado primeiro ao nó de administração principal. Em seguida, você deve aprovar o aplicativo do hotfix para outros nós de grade até que todos os nós do sistema StorageGRID estejam executando a mesma versão de software. Você pode personalizar a sequência de aprovação selecionando para aprovar nós de grade individuais, grupos de nós de grade ou todos os nós de grade.

Embora todos 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.

Atualizações do sistema operacional SANtricity

Talvez seja necessário atualizar o software SANtricity os nos controladores de storage dos dispositivos de storage, se os controladores não estiverem funcionando corretamente. Você pode fazer o upload do arquivo do SANtricity os para o nó de administrador principal no sistema StorageGRID e aplicar a atualização do Gerenciador de Grade.

A página SANtricity, mostrada abaixo, permite que você carregue o arquivo de atualização do SANtricity os.

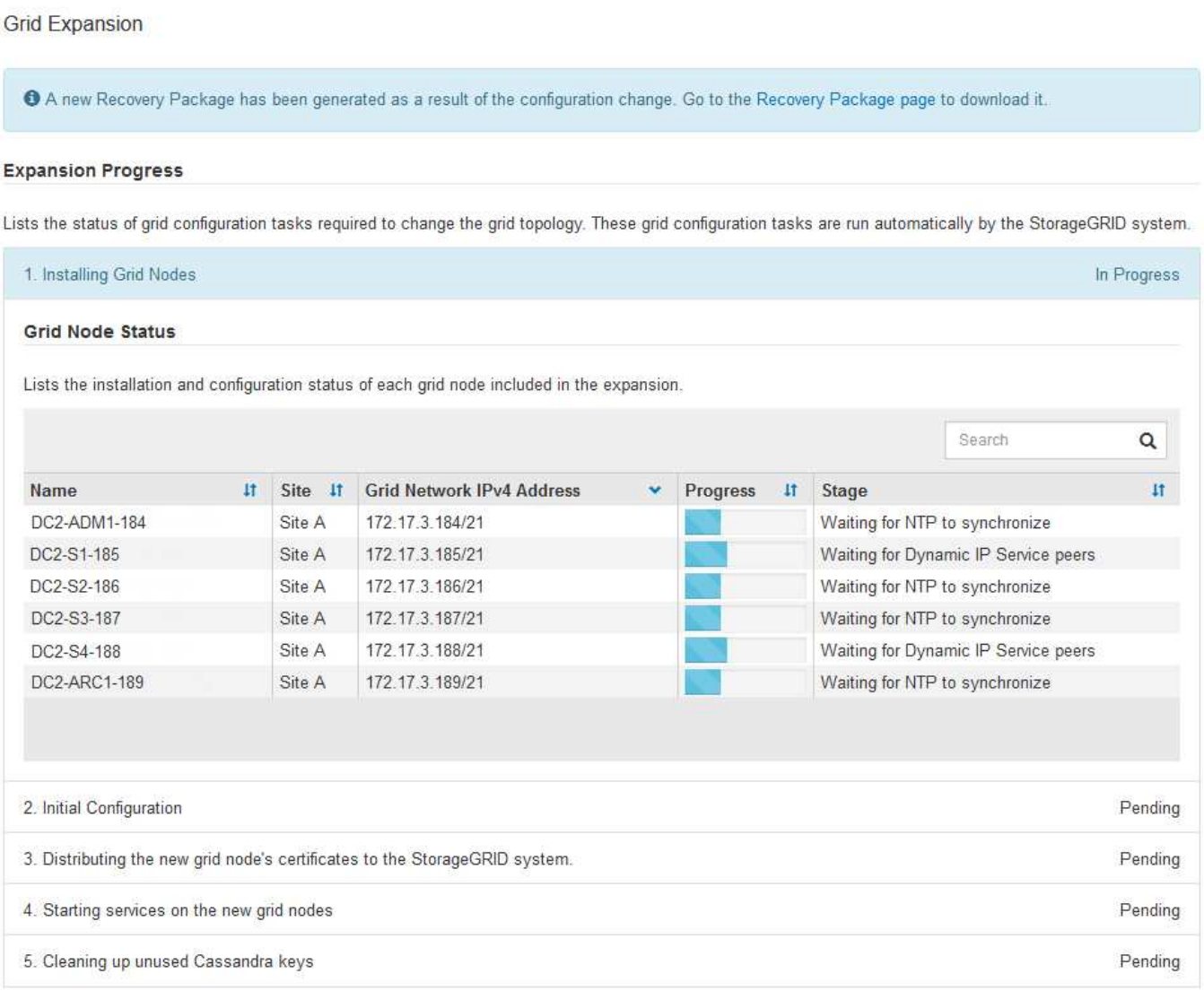


Depois de fazer o upload do arquivo, você pode aprovar a atualização em nós de storage individuais ou em todos os nós. A capacidade de aprovar seletivamente nós torna mais fácil para você agendar a atualização. Depois de aprovar um nó para atualização, o sistema executa uma verificação de integridade e instala a atualização, se aplicável ao nó.

Procedimentos de expansão

Você pode expandir um sistema StorageGRID adicionando volumes de storage aos nós de storage, adicionando novos nós de grade a um local existente ou adicionando um novo local de data center. Se você tiver nós de storage que usam o dispositivo de storage SG6060, poderá adicionar uma ou duas gavetas de expansão para dobrar ou triplicar a capacidade de storage do nó.

Você pode realizar expansões sem interromper a operação do seu sistema atual. Quando você adiciona nós ou um site, primeiro você implanta os novos nós e, em seguida, executa o procedimento de expansão na página expansão de Grade.

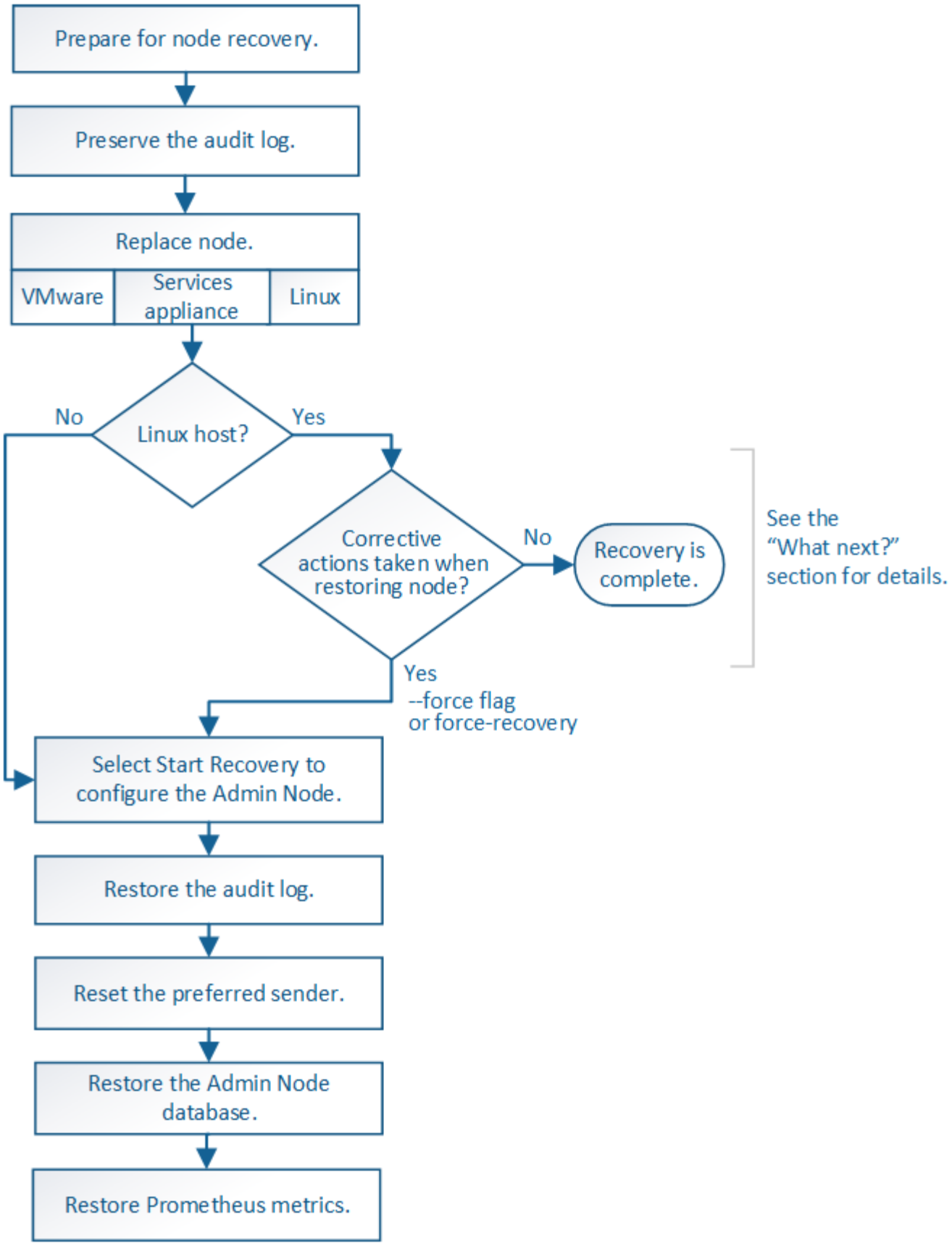


Procedimentos de recuperação do nó

Os nós de grade podem falhar se uma falha de hardware, virtualização, sistema operacional ou software tornar o nó inoperável ou não confiável.

As etapas para recuperar um nó de grade dependem da plataforma onde o nó de grade está hospedado e do tipo de nó de grade. Cada tipo de nó de grade tem um procedimento de recuperação específico, que você deve seguir exatamente. Geralmente, você tenta preservar os dados do nó de grade com falha, sempre que possível, reparar ou substituir o nó com falha, usar a página recuperação para configurar o nó de substituição e restaurar os dados do nó.

Por exemplo, este fluxograma mostra o procedimento de recuperação se um nó Admin tiver falhado.



Procedimentos de desativação

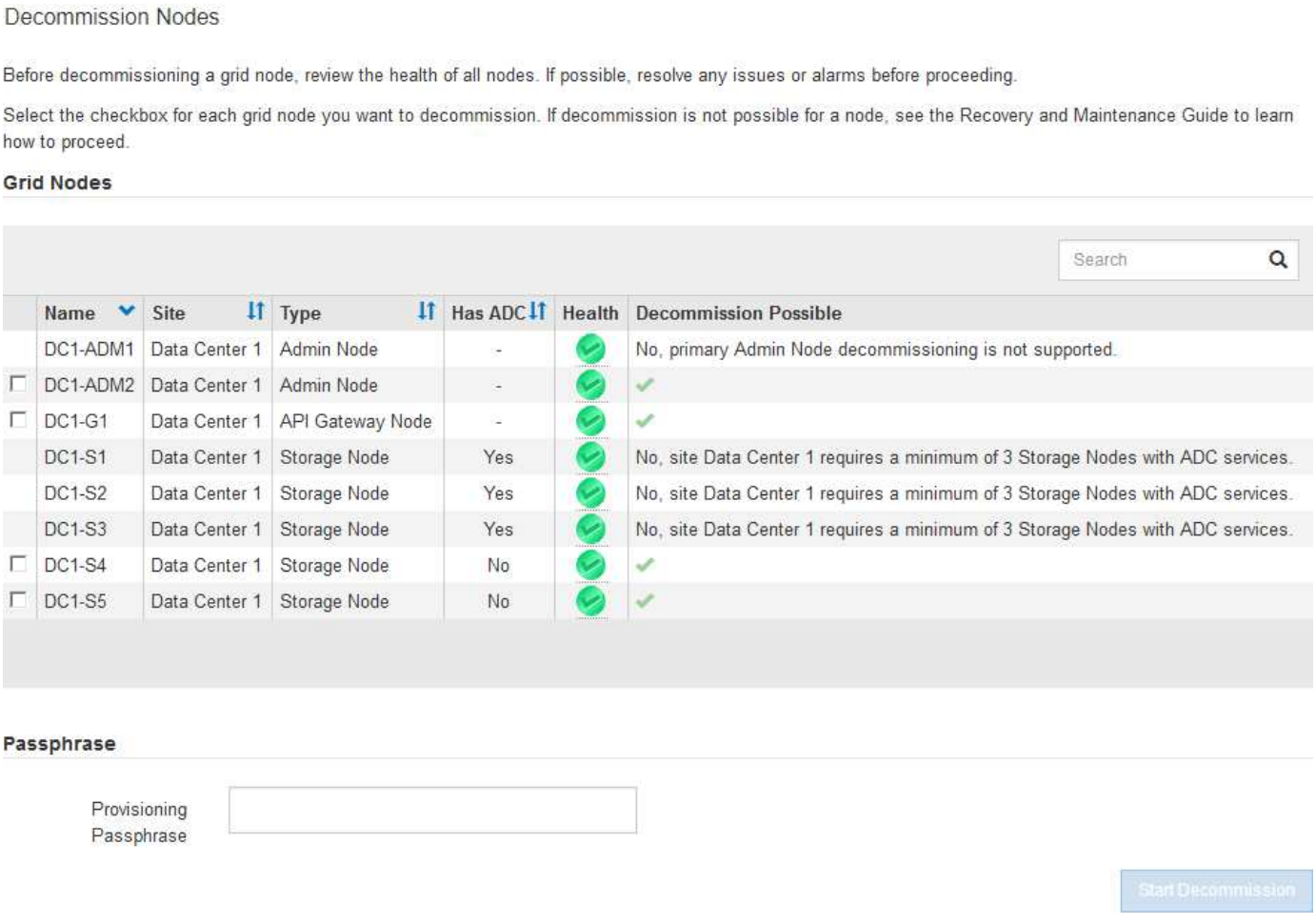
Você pode querer remover permanentemente nós de grade ou um site inteiro de data center do seu sistema StorageGRID.

Por exemplo, você pode querer desativar um ou mais nós de grade nestes casos:

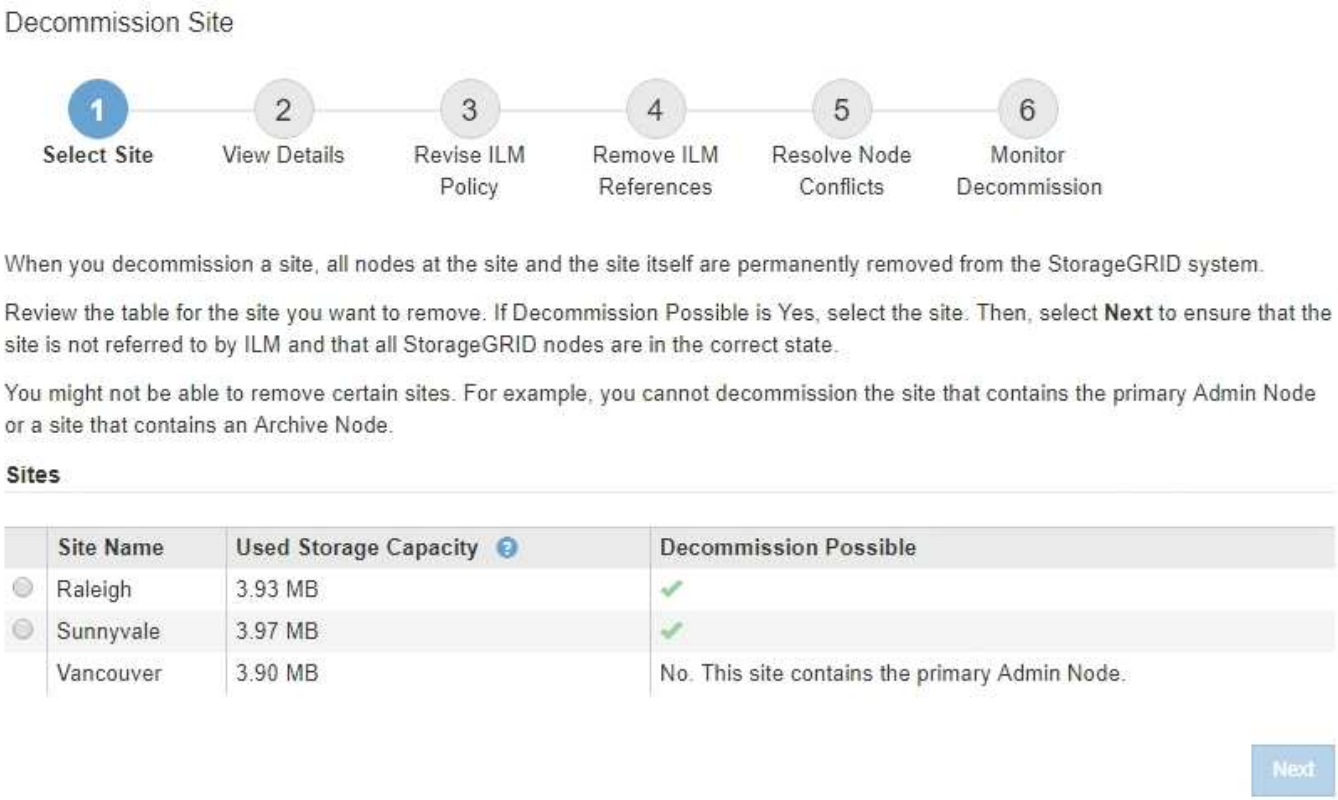
- Você adicionou um nó de storage maior ao sistema e deseja remover um ou mais nós de storage menores, preservando ao mesmo tempo objetos.
- Você exige menos storage total.
- Não é mais necessário um nó de gateway ou um nó de administrador não primário.
- Sua grade inclui um nó desconetado que você não pode recuperar ou trazer de volta on-line.

Você pode usar a página Decommission Nodes no Gerenciador de Grade para remover os seguintes tipos de nós de grade:

- Nós de storage, a menos que não haja nós suficientes, permaneceriam no local para dar suporte a certos requisitos
- Nós de gateway
- Nós de administração não primários



Você pode usar a página Decommission Site no Gerenciador de Grade para remover um site. A desativação de um site conetado remove um site operacional e preserva os dados. A desativação de um site desconetado remove um site com falha, mas não preserva os dados. O assistente Decommission Site orienta você pelo processo de seleção do site, visualização de detalhes do site, revisão da política ILM, remoção de referências de sites de regras ILM e resolução de conflitos de nó.



Procedimentos de manutenção da rede

Alguns dos procedimentos de manutenção de rede que você pode precisar executar incluem o seguinte:

- Atualizando as sub-redes na rede de Grade
- Usando a ferramenta alterar IP para alterar a configuração de rede que foi inicialmente definida durante a implantação da grade
- Adicionar, remover ou atualizar servidores DNS (sistema de nomes de domínio)
- Adicionar, remover ou atualizar servidores NTP (Network Time Protocol) para garantir que os dados sejam sincronizados com precisão entre nós de grade
- Restaurar a conetividade de rede para nós que podem ter ficado isolados do resto da grade

Procedimentos de nível de host e middleware

Alguns procedimentos de manutenção são específicos para nós StorageGRID que são implantados no Linux ou VMware, ou são específicos para outros componentes da solução StorageGRID. Por exemplo, você pode querer migrar um nó de grade para um host Linux diferente ou executar manutenção em um nó de arquivo conetado ao Tivoli Storage Manager (TSM).

Clonagem do nó do dispositivo

A clonagem do nó do dispositivo permite substituir facilmente um nó do dispositivo (origem) existente na grade por um dispositivo compatível (destino) que faz parte do mesmo local lógico da StorageGRID. O processo transfere todos os dados para o novo dispositivo, colocando-os em serviço para substituir o nó antigo do dispositivo e deixando o dispositivo antigo em um estado de pré-instalação. A clonagem fornece um processo de atualização de hardware fácil de executar e fornece um método alternativo para a substituição de dispositivos.

Procedimentos de nó de grade

Talvez seja necessário executar determinados procedimentos em um nó de grade específico. Por exemplo, talvez seja necessário reinicializar um nó de grade ou parar e reiniciar manualmente um serviço de nó de grade específico. Alguns procedimentos de nó de grade podem ser executados a partir do Gerenciador de Grade; outros exigem que você faça login no nó de grade e use a linha de comando do nó.

Informações relacionadas

"Administrar o StorageGRID"

"Atualizar o software"

"Expanda sua grade"

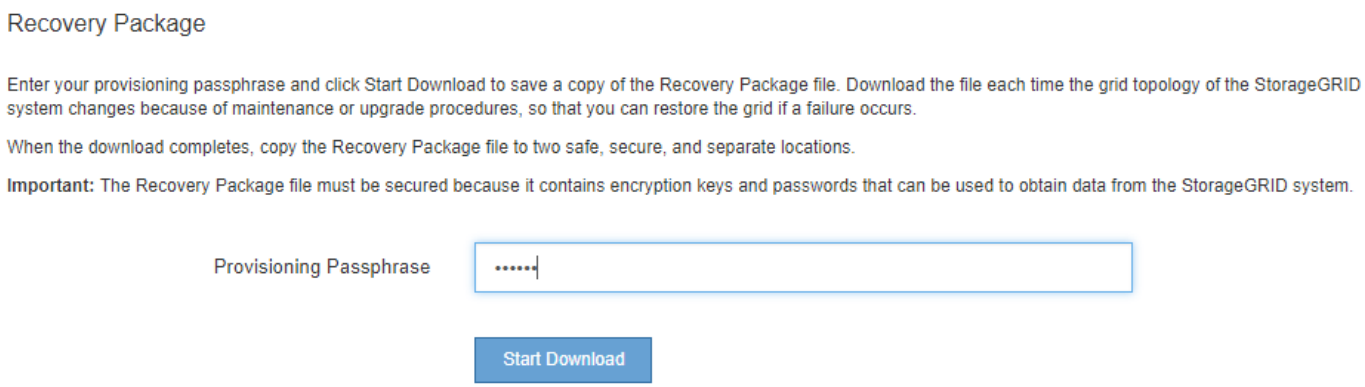
"Manter recuperar"

Transferir o pacote de recuperação

O Pacote de recuperação é um arquivo .zip para download que contém arquivos específicos de implantação e software necessários para instalar, expandir, atualizar e manter um sistema StorageGRID.

O arquivo Recovery Package também contém informações de configuração e integração específicas do sistema, incluindo nomes de host de servidor e endereços IP, e senhas altamente confidenciais necessárias durante a manutenção, atualização e expansão do sistema. O Pacote de recuperação é necessário para se recuperar da falha do nó de administração principal.

Ao instalar um sistema StorageGRID, é necessário baixar o arquivo do Pacote de recuperação e confirmar que você pode acessar com sucesso o conteúdo deste arquivo. Você também deve baixar o arquivo sempre que a topologia de grade do sistema StorageGRID mudar devido a procedimentos de manutenção ou atualização.



Depois de baixar o arquivo Recovery Package e confirmar que você pode extrair o conteúdo, copie o arquivo Recovery Package para dois locais seguros, seguros e separados.

> O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

Informações relacionadas

"Atualizar o software"

"Expanda sua grade"

"Manter recuperar"

Usando as opções de suporte do StorageGRID

O Gerenciador de Grade fornece opções para ajudá-lo a trabalhar com suporte técnico se surgir um problema com o seu sistema StorageGRID.

Configurando o AutoSupport

O recurso AutoSupport permite que o sistema StorageGRID envie mensagens de status e integridade para o suporte técnico. 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 as mensagens do AutoSupport para serem enviadas para um destino adicional.

Informações incluídas nas mensagens do AutoSupport

As mensagens do AutoSupport incluem informações como as seguintes:

- Versão do software StorageGRID
- Versão do sistema operativo
- Informações sobre atributos no nível do sistema e no nível da localização
- Alertas e alarmes recentes (sistema legado)
- Status atual de todas as tarefas de grade, incluindo dados históricos
- Informações de eventos conforme listado na página **nodes *node* Eventos**
- Utilização da base de dados do Admin Node
- Número de objetos perdidos ou perdidos
- Definições de configuração da grelha
- Entidades NMS
- Política ILM ativa
- Arquivo de especificação de grade provisionada
- Métricas de diagnóstico

Você pode ativar o recurso AutoSupport e as opções individuais do AutoSupport quando instalar o StorageGRID pela primeira vez, ou ativá-los posteriormente. Se o AutoSupport não estiver habilitado, uma mensagem será exibida no Painel de Gerenciamento de Grade. A mensagem inclui um link para a página de configuração do AutoSupport.

Você pode selecionar o símbolo "x" para fechar a mensagem. A mensagem não aparecerá novamente até que o cache do navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

Usando o Active IQ

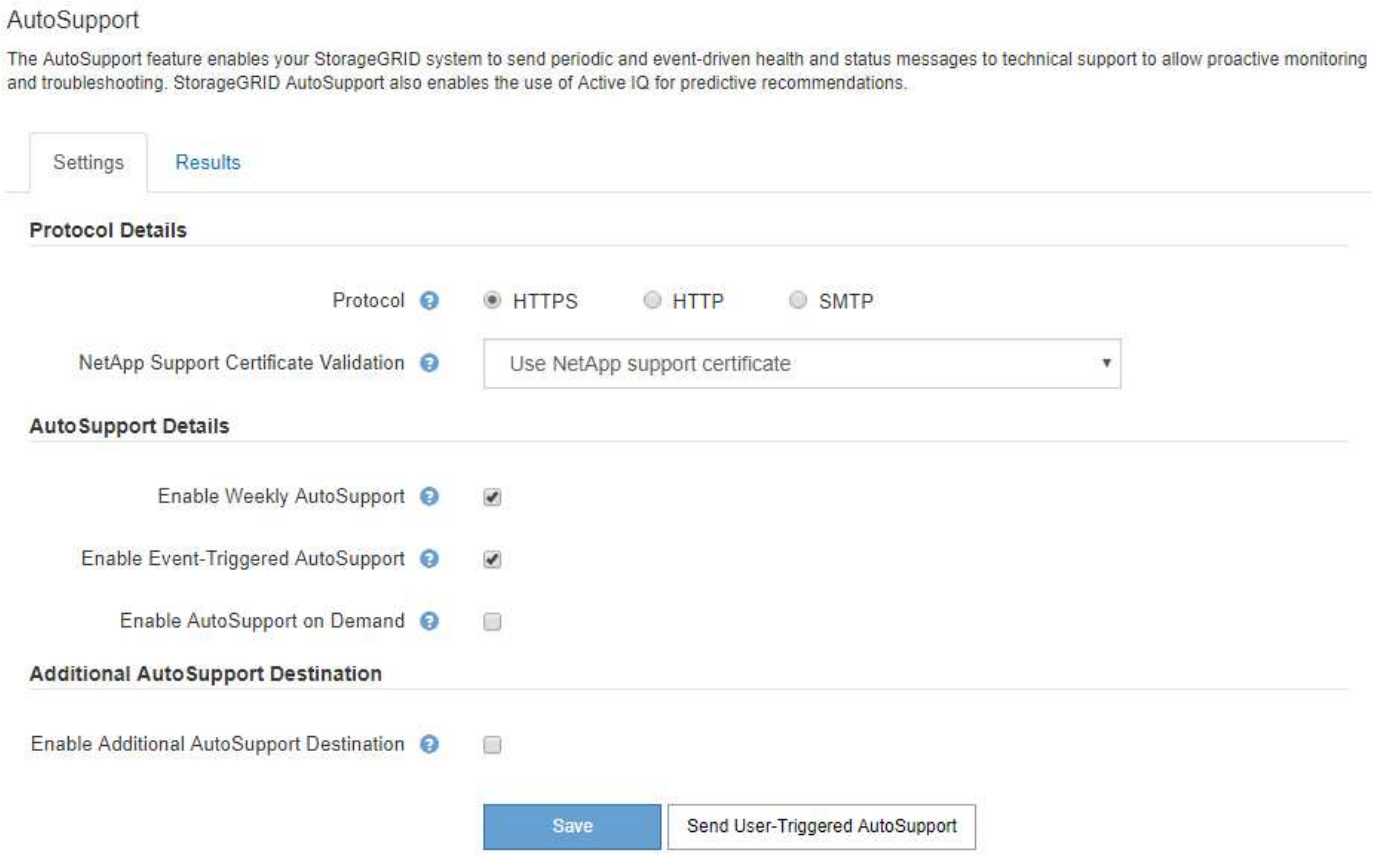
O Active IQ é um consultor digital baseado na nuvem que utiliza as análises preditivas e o conhecimento da comunidade da base instalada da NetApp. Suas avaliações de risco contínuas, alertas preditivos, orientações prescritivas e ações automatizadas ajudam a evitar problemas antes que eles ocorram, levando a uma melhor integridade do sistema e maior disponibilidade do sistema.

Você deve habilitar o AutoSupport se quiser usar os painéis e a funcionalidade do Active IQ no site de suporte da NetApp.

"Documentação do consultor digital da Active IQ"

Aceder às definições do AutoSupport

Você configura o AutoSupport usando o Gerenciador de Grade (**suporte** > **Ferramentas** > **AutoSupport**). A página **AutoSupport** tem duas guias: **Configurações** e **resultados**.



Protocolos para envio de mensagens AutoSupport

Você pode escolher um dos três protocolos para enviar mensagens AutoSupport:

- HTTPS
- HTTP
- SMTP

Se você enviar mensagens AutoSupport usando HTTPS ou HTTP, poderá configurar um servidor proxy não transparente entre nós de administração e suporte técnico.

Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de configurar um servidor de correio SMTP.

Opções de AutoSupport

Você pode usar qualquer combinação das seguintes opções para enviar mensagens do AutoSupport para o suporte técnico:

- **Semanal**: Enviar automaticamente mensagens AutoSupport uma vez por semana. Predefinição: Activado.
- **Event-dispolled**: Envie automaticamente mensagens AutoSupport 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 mensagens AutoSupport automaticamente, o que é útil quando eles estão trabalhando ativamente em um problema (requer protocolo de transmissão HTTPS AutoSupport). Predefinição: Desativada.
- **Ativado pelo usuário**: Envie mensagens AutoSupport manualmente a qualquer momento.

Informações relacionadas

"Administrar o StorageGRID"

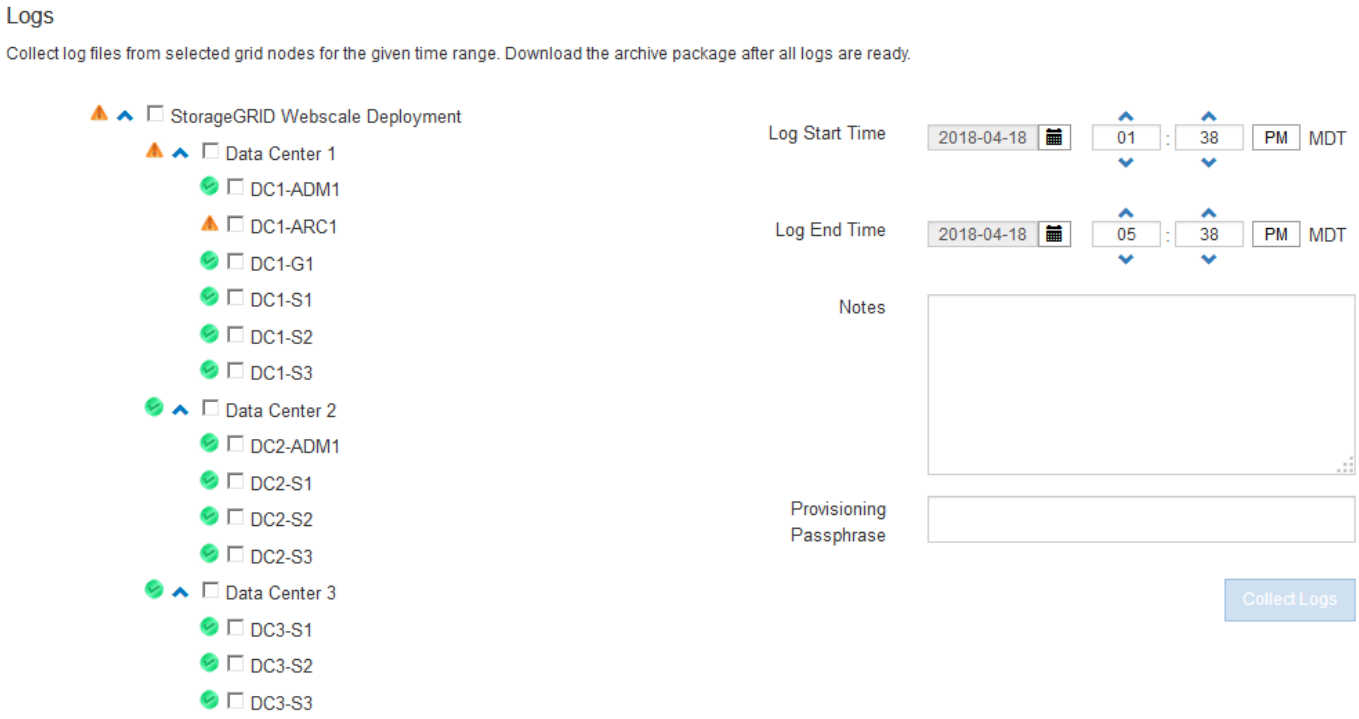
"Configurar definições de rede"

Coletando logs do StorageGRID

Para ajudar a solucionar um problema, talvez seja necessário coletar arquivos de log e encaminhá-los para o suporte técnico.

O StorageGRID usa arquivos de log para capturar eventos, mensagens de diagnóstico e condições de erro. O arquivo bycast.log é mantido para cada nó de grade e é o principal arquivo de solução de problemas. O StorageGRID também cria arquivos de log para serviços StorageGRID individuais, arquivos de log relacionados a atividades de implantação e manutenção e arquivos de log relacionados a aplicativos de terceiros.

Os usuários que têm as permissões apropriadas e que conhecem a senha de provisionamento para seu sistema StorageGRID podem usar a página Logs no Gerenciador de Grade para coletar arquivos de log, dados do sistema e dados de configuração. Ao coletar logs, você seleciona um nó ou nós e especifica um período de tempo. Os dados são coletados e arquivados em um `.tar.gz` arquivo, que você pode baixar para um computador local. Dentro deste arquivo, há um arquivo de log para cada nó de grade.



Informações relacionadas

"Monitorizar Resolução de problemas"

"Administrar o StorageGRID"

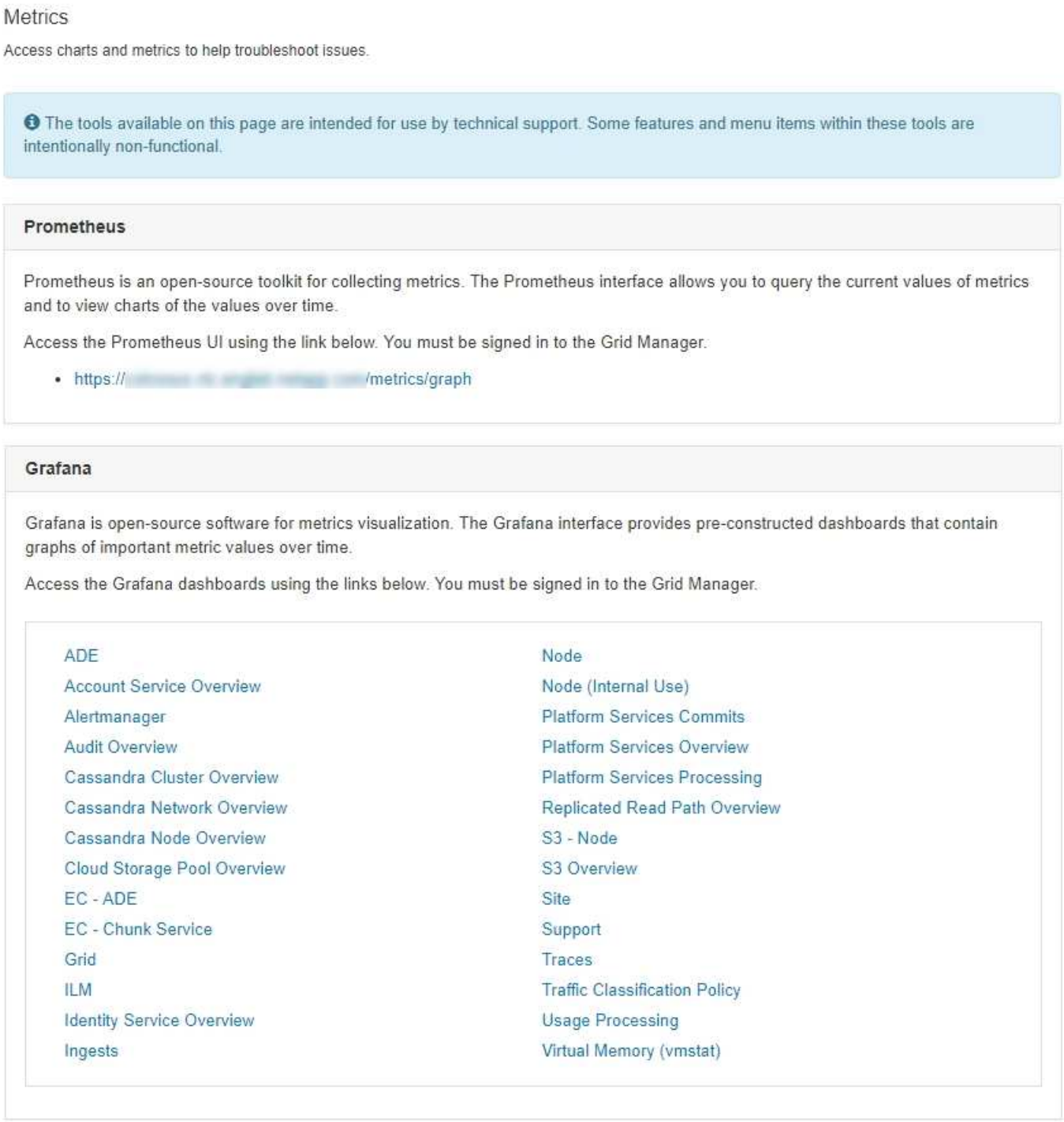
Usando métricas e executando diagnósticos

Ao solucionar um problema, você pode trabalhar com suporte técnico para analisar métricas e gráficos detalhados do seu sistema StorageGRID. Você também pode executar consultas de diagnóstico pré-construídas para avaliar proativamente os principais valores do seu sistema StorageGRID.

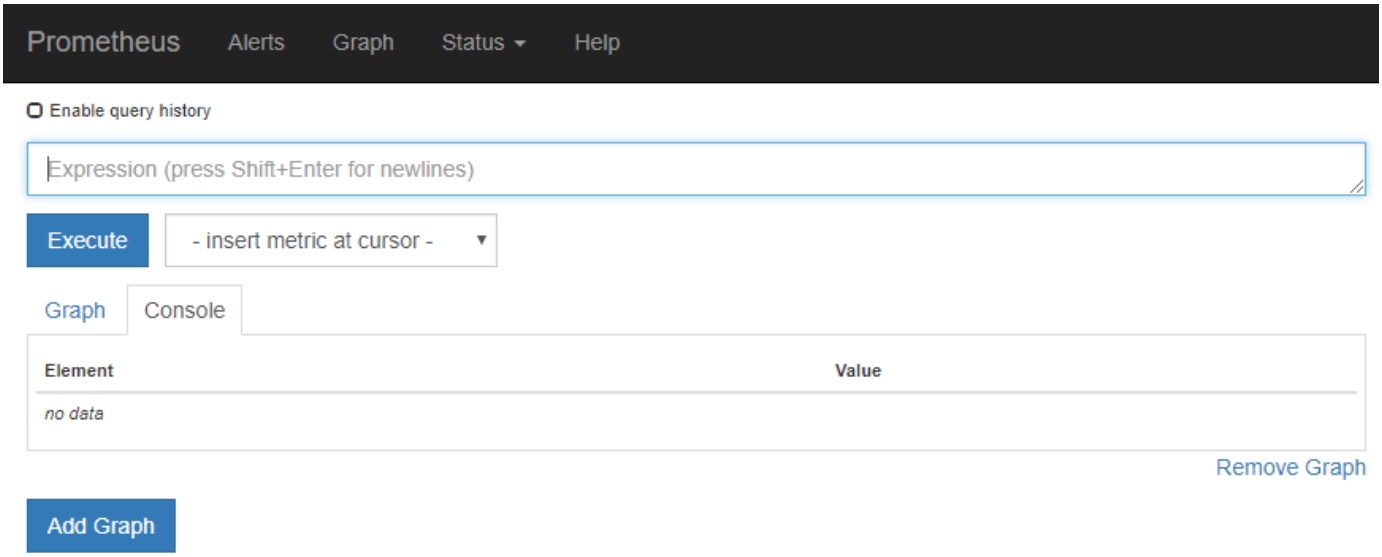
Página de métricas

A página Metrics fornece acesso às 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.



O link na seção Prometheus da página Metrics permite consultar os valores atuais das métricas do StorageGRID e visualizar gráficos dos valores ao longo do tempo.

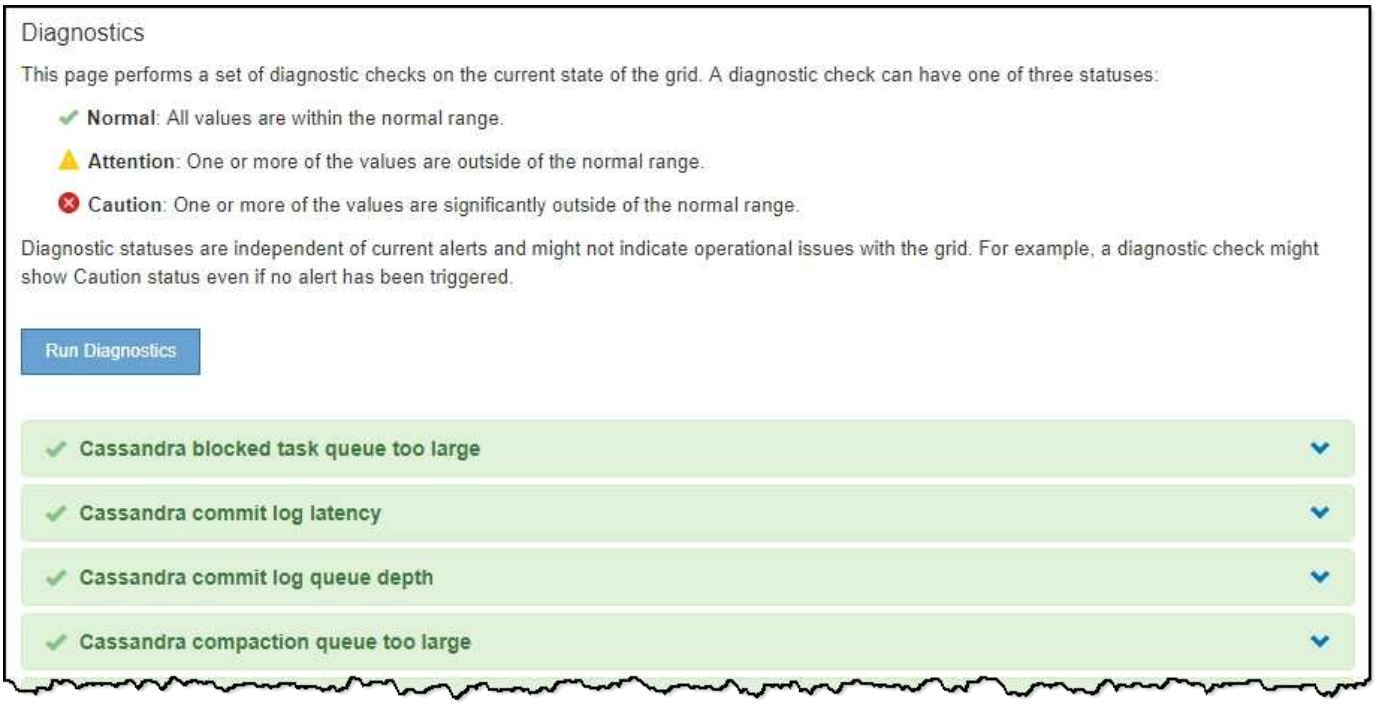


As métricas que incluem *private* em seus nomes são destinadas apenas para uso interno e estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

Os links na seção Grafana da página métricas permitem acessar painéis pré-construídos contendo gráficos de métricas do StorageGRID ao longo do tempo.

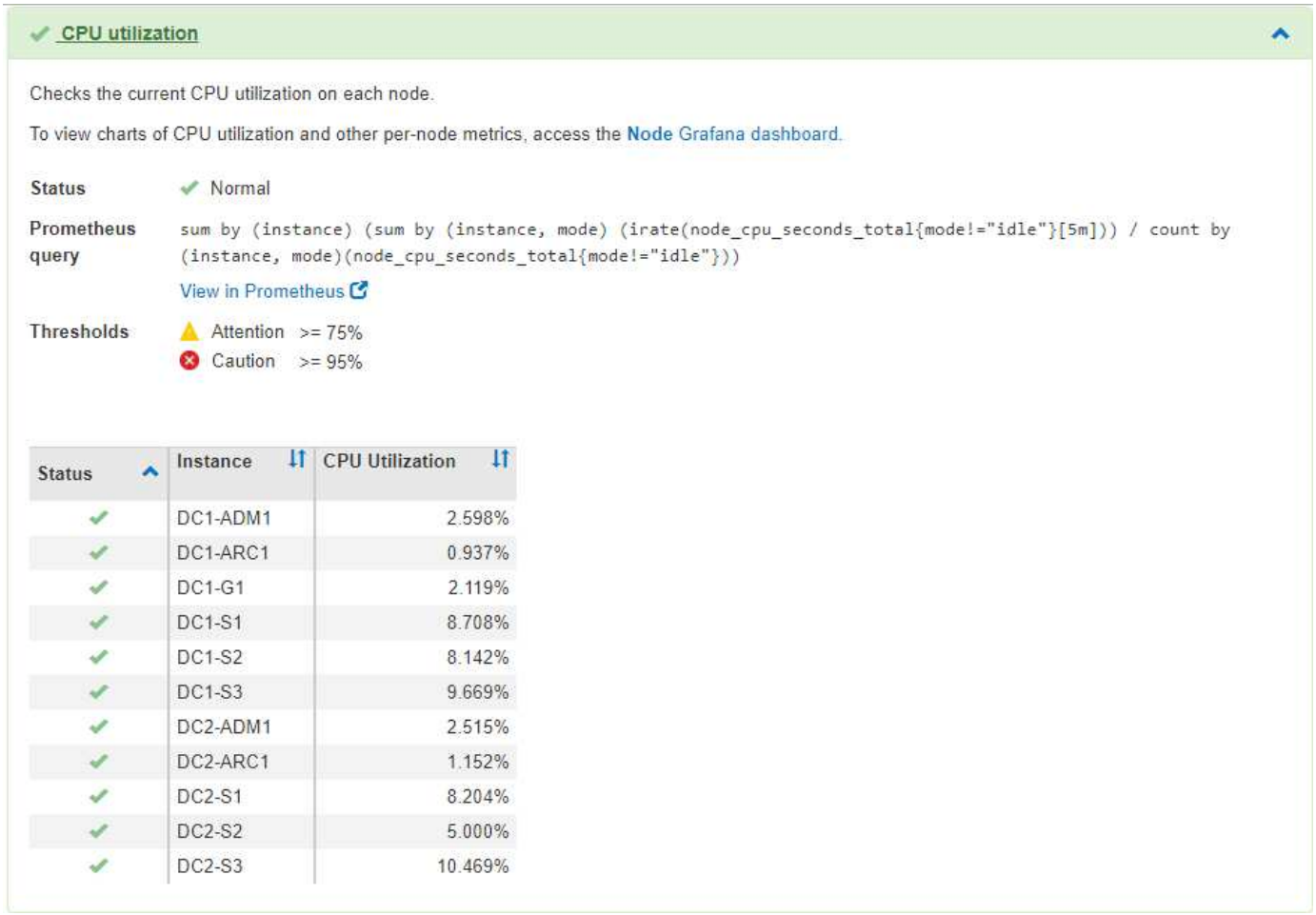
Página de diagnóstico

A página Diagnósticos executa um conjunto de verificações de diagnóstico pré-construídas no estado atual da grade. No exemplo, todos os diagnósticos têm um status normal.



Clicar em um diagnóstico específico permite que você veja detalhes sobre o diagnóstico e seus resultados atuais.

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.



Informações relacionadas

"Monitorizar Resolução de problemas"

Diretrizes de rede

Saiba mais sobre a arquitetura e as topologias de rede do StorageGRID. Familiarize-se com os requisitos de configuração e provisionamento de rede.

- "Visão geral da rede StorageGRID"
- "Requisitos e diretrizes de rede"
- "Considerações de rede específicas da implantação"
- "Instalação e provisionamento de rede"
- "Diretrizes de pós-instalação"
- "Referência da porta de rede"

Visão geral da rede StorageGRID

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 no *cartilha* de grade.

Antes de implantar e configurar o StorageGRID, você deve configurar a infraestrutura de rede. A comunicação precisa ocorrer entre todos os nós na 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.

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

Informações relacionadas

"Primário de grelha"

"Administrar o StorageGRID"

"Notas de lançamento"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

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)
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 e Swift.	Rede cliente (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.

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 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.

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 não pretender configurar um gateway para uma rede, deve utilizar o endereço IP como endereço de gateway.

Os grupos de alta disponibilidade (HA) fornecem a capacidade de adicionar endereços IP virtuais à interface Grid ou rede de clientes. Para obter mais informações, consulte as instruções para administrar o StorageGRID.

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 a 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.

Ao usar uma rede de administração, o tráfego administrativo e de manutenção não precisa viajar pela rede de grade. Os usos típicos da rede de administração incluem acesso à interface de usuário do Grid Manager; acesso a serviços críticos como NTP, DNS, gerenciamento de chaves externas (KMS) e LDAP (Lightweight Directory Access Protocol); acesso a logs de auditoria em nós de administração; e 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 a 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 e Swift. 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. Para obter mais informações sobre o recurso rede cliente não confiável e o serviço de balanceamento de carga, consulte as instruções para administrar o StorageGRID.

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 StorageGRID Load Balancer e acesso aos clientes S3 e Swift à grade.
- Nós de storage, porque esses nós fornecem acesso aos protocolos S3 e Swift, e aos Cloud Storage Pools e ao serviço de replicação 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 a 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.

Informações relacionadas

"Requisitos e diretrizes de rede"

"Administrar o StorageGRID"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Instale o VMware"

Exemplos de topologia de rede

Além da rede de Grade necessária, você pode escolher se deseja configurar as interfaces de rede de administração e rede de cliente ao projetar a topologia de rede para uma implantação de um ou vários locais.

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. Para obter mais informações sobre portas internas e externas, consulte a referência da porta de rede.

Se você especificar que a interface de rede do cliente de um nó não é confiável, configure um ponto de extremidade do balanceador de carga para aceitar o tráfego de entrada. Para obter informações sobre como configurar redes de clientes não confiáveis e pontos de extremidade do balanceador de carga, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

"Referência da porta de rede"

Topologia de rede de grade

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

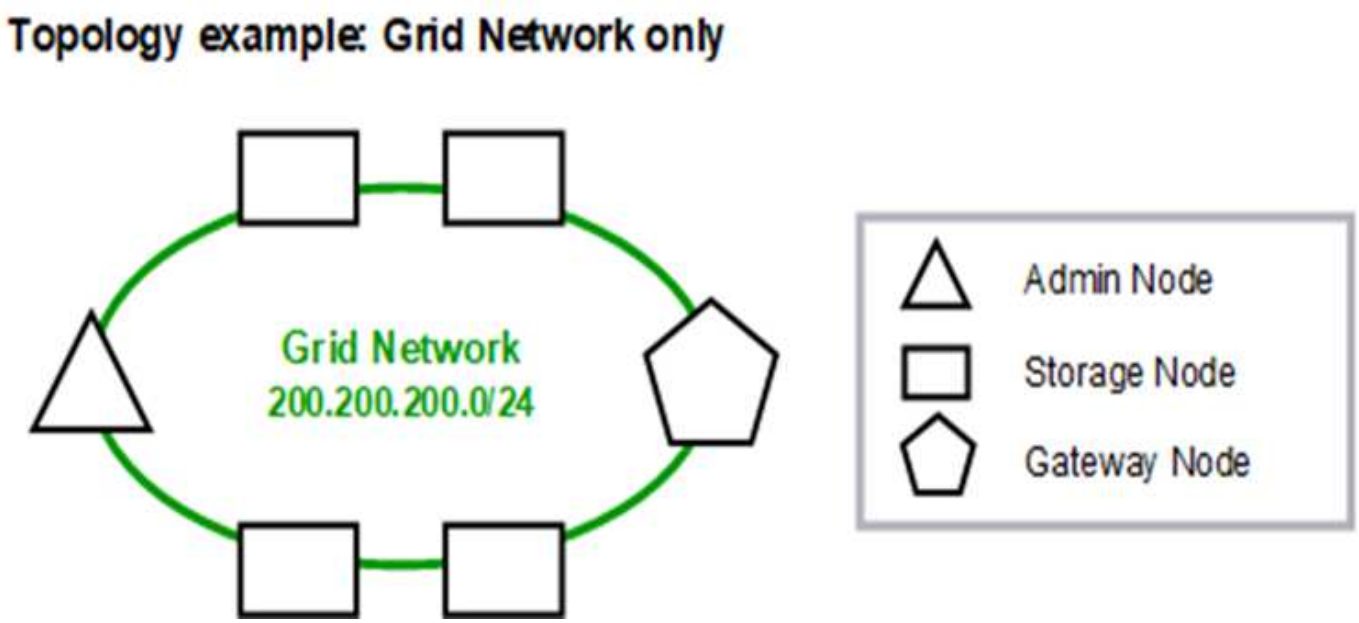
Ao configurar a rede de Grade, você estabelece o endereço IP do host, a máscara de sub-rede e o endereço IP do gateway para a interface eth0 para cada nó de grade.

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 tráfego relacionado a solicitações de clientes S3 e Swift 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

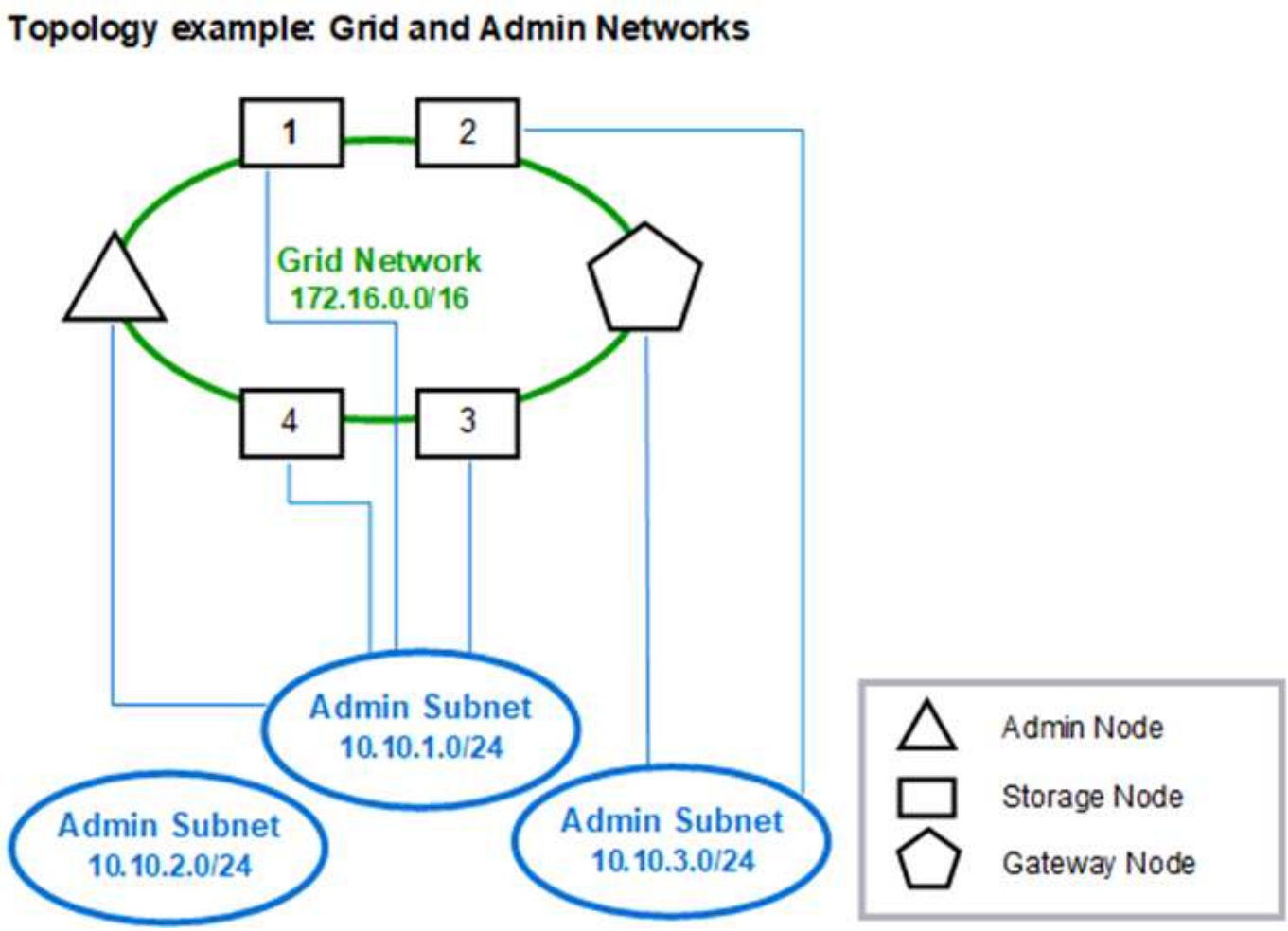
Ter uma rede de administração é opcional. Uma maneira de usar uma rede Admin e uma rede de Grade é configurar uma rede de Grade roteável e uma rede Admin limitada para cada nó.

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 Swift e gerenciamento de objetos. Enquanto a rede de administração é usada para funções administrativas.



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

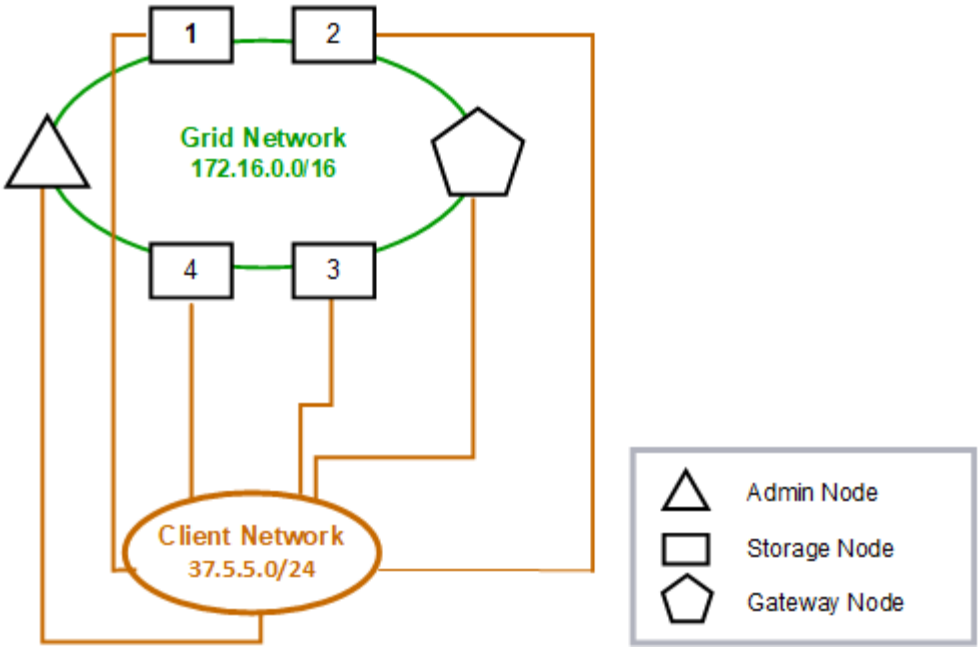
Ter uma rede de clientes é opcional. O uso de uma rede cliente permite que o tráfego de rede cliente (por exemplo, S3 e Swift) seja separado do tráfego interno da grade, o que permite que a rede de grade seja mais segura. O tráfego administrativo pode ser Tratado pelo Cliente ou rede de Grade quando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

Nodes	Grid Network IP/mask	Client Network IP/mask	Client Network 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

Topologia para todas as três redes

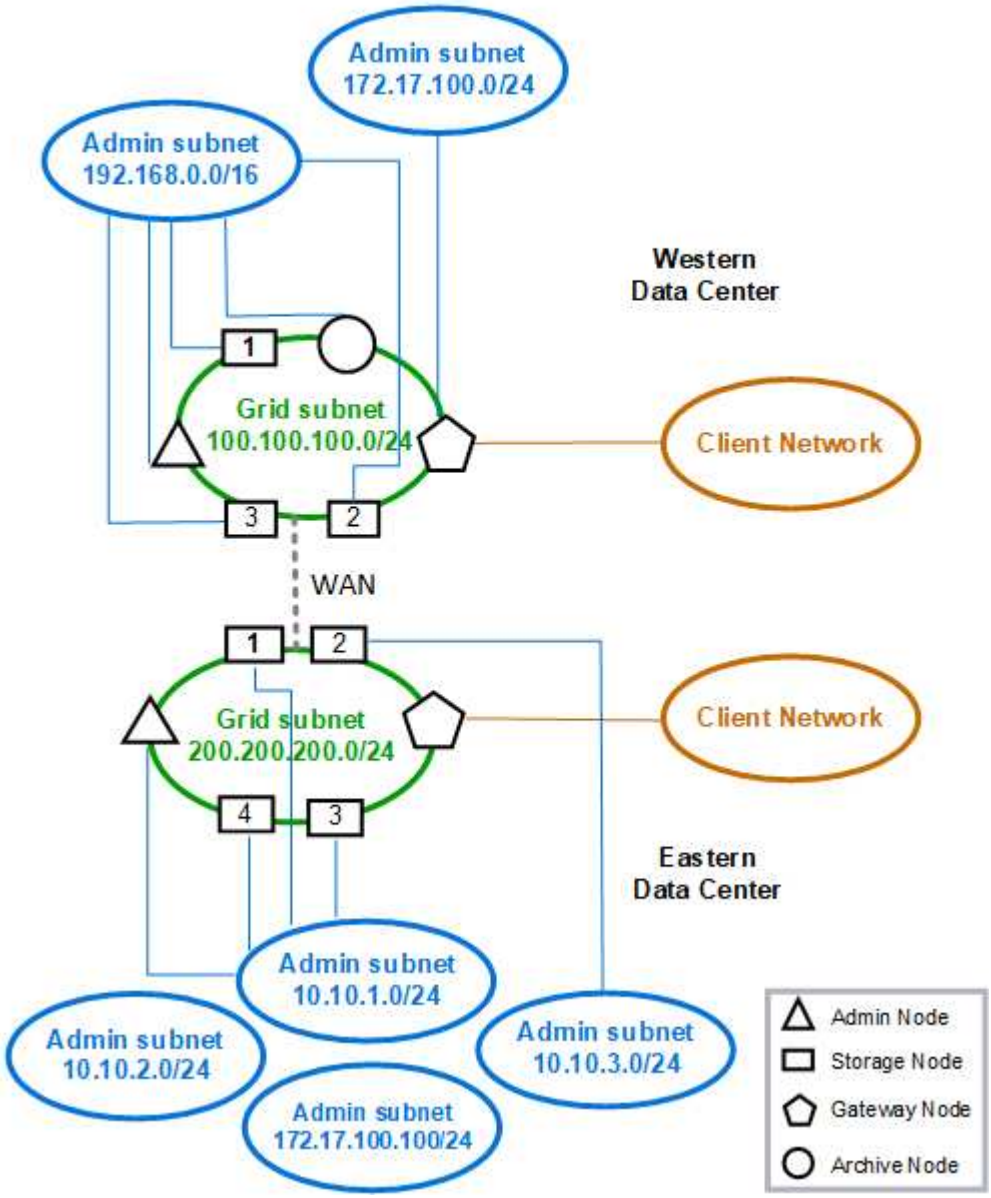
Você pode configurar todas as três redes em uma topologia de rede que consiste em uma rede de grade privada, redes de administração específicas de sites limitados e

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 de clientes é usada para tráfego relacionado a solicitações de clientes S3 e Swift.

Topology example: Grid, Admin, and Client Networks



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 eithersupport.NetApp.com ou 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 e Swift.
- Solicitações de saída de serviços da plataforma StorageGRID, como a replicação do Cloud Mirror ou de pools de storage de nuvem.

Se o StorageGRID não conseguir entrar em Contato com qualquer um dos servidores NTP ou DNS provisionados usando as regras de roteamento padrão, ele tentará automaticamente o Contato em todas as redes (Grade, Admin 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, você pode configurar essas redes após a conclusão da instalação usando a ferramenta Change IP, conforme descrito nas instruções de recuperação e manutenção.

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. Consulte as informações sobre grupos de alta disponibilidade nas instruções para administrar o StorageGRID.

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.

Informações relacionadas

"Primário de grelha"

"Administrar o StorageGRID"

"Manter recuperar"

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 na 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 a quaisquer sub-redes 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.

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 e Swift. 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. Consulte as informações sobre como gerenciar o balanceamento de carga e o gerenciamento de redes de clientes não confiáveis nas instruções de administração do StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Considerações de rede específicas da implantação

Dependendo das plataformas de implantação que você usa, você pode ter considerações adicionais sobre o design da rede StorageGRID.

Os nós de grade podem ser implantados como:

- Nós de grade baseados em software implantados como máquinas virtuais no VMware vSphere Web Client
- Nós de grade baseados em software implantados em contentores Docker em hosts Linux
- Nós baseados no dispositivo

Para obter informações adicionais sobre nós de grade, consulte *Grid primer*.

Informações relacionadas

"Primário de grelha"

Implantações Linux

Para eficiência, confiabilidade e segurança, o sistema StorageGRID é executado no Linux como uma coleção de contentores Docker. A configuração de rede relacionada ao Docker não é necessária em um 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.

Veja as instruções de instalação para implantações Red Hat Enterprise Linux/CentOS ou Ubuntu/Debian.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Configuração de rede de host para implantações do Docker

Antes de iniciar a implantação do StorageGRID em uma plataforma de contentor Docker, 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.

Recomendações mínimas de largura de banda

A tabela a seguir fornece as recomendações de largura de banda mínima 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
Administrador	10 Gbps	1 Gbps	1 Gbps
Gateway	10 Gbps	1 Gbps	10 Gbps
Armazenamento	10 Gbps	1 Gbps	10 Gbps
Arquivar	10 Gbps	1 Gbps	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 as informações sobre como configurar a rede host nas instruções de instalação da sua plataforma Linux.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale 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. 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. Neste exemplo, o recurso rede cliente não confiável pode ser usado para restringir conexões de entrada.

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.

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.

Se você usar um servidor proxy não transparente, também deverá configurar as configurações de proxy para permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet. Consulte administrar StorageGRID para saber como configurar as configurações de proxy.

Para obter mais informações sobre redes de clientes não confiáveis, consulte as instruções para administrar o StorageGRID. Para obter mais informações sobre serviços de plataforma, consulte as instruções para usar contas de locatário. Para obter mais informações sobre Cloud Storage Pools, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Informações relacionadas

"Referência da porta de rede"

"Primário de grelha"

"Administrar o StorageGRID"

"Use uma conta de locatário"

"Gerenciar objetos com ILM"

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 nas instruções de instalação e manutenção do seu aparelho.

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

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 você quiser desativar a rede Admin ou a rede cliente, você pode remover a configuração deles durante o processo de aprovação do nó ou usar a ferramenta Change IP após a conclusão da instalação. Consulte as informações sobre os procedimentos de manutenção da rede nas instruções de recuperação e manutenção.

Informações relacionadas

"Manter recuperar"

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 seus endereços IP são alterados, o que pode causar interrupções se uma alteração de endereço 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. Consulte as informações sobre como configurar endereços IP nas instruções de recuperação e manutenção.
- 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.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Manter recuperar"

Referência da porta de rede

Você deve garantir que a infraestrutura de rede possa fornecer comunicação interna e externa entre nós dentro da grade e para clientes e serviços externos. Você pode precisar de acesso em firewalls internos e externos, sistemas de comutação e sistemas de roteamento.

Use os detalhes fornecidos para comunicações internas de nó de grade e comunicações externas para determinar como configurar cada porta necessária.

- "Comunicações internas do nó da grade"
- "Comunicações externas"

Comunicações internas do nó da grade

O firewall interno do StorageGRID só permite conexões de entrada para portas específicas na rede de Grade, com exceção das portas 22, 80, 123 e 443 (consulte as informações sobre comunicações externas). 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 (HA) estiverem configurados.

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 as instruções de instalação da sua plataforma Linux.

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, consulte as instruções de instalação do VMware.

Diretrizes para nós de storage do 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. Para obter mais informações sobre o mapeamento de portas para dispositivos, consulte as instruções de instalação do seu dispositivo de armazenamento.

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.
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.
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.
1509	TCP	Todos os nós	Nós de arquivamento	Tráfego interno do nó de arquivamento.
1511	TCP	Todos os nós	Nós de storage	Tráfego interno de metadados.
5353	UDP	Todos os nós	Todos os nós	Usado opcionalmente para alterações de IP de grade completa e para descoberta de nó de administrador principal durante a instalação, expansão e recuperação.
7001	TCP	Nós de storage	Nós de storage	Comunicação de cluster entre nós Cassandra TLS.
7443	TCP	Todos os nós	Nós de administração	Tráfego interno para procedimentos de manutenção e relatórios de erros.
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 mensagens AutoSupport do Gerenciador de sistemas SANtricity do e-Series para o nó de administração principal.
11139	TCP	Nós de arquivamento/storage	Nós de arquivamento/storage	Tráfego interno entre nós de storage e nós de arquivamento.
18000	TCP	Nós de administração/storage	Nós de storage com ADC	Tráfego interno do serviço de conta.
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.
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"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

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.

Se as políticas de rede empresarial restringirem o acesso a qualquer uma das portas, você poderá usar pontos de extremidade do balanceador de carga para permitir o acesso em portas definidas pelo usuário. O recurso redes de clientes não confiáveis pode ser usado para permitir o acesso apenas em portas de endpoint do balanceador de carga.

Para usar sistemas e protocolos como SMTP, DNS, SSH ou DHCP, você deve remapear portas ao implantar nós. No entanto, você não deve remapear os pontos de extremidade do balanceador. Para obter informações sobre o mapeamento de portas, consulte as instruções de instalação da sua plataforma.

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

Esta lista não inclui portas que podem ser configuradas como pontos de extremidade do balanceador de carga. Para obter mais informações, consulte as instruções para configurar 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 o sistema de nomes de domínio.
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.
80	TCP	HTTP	Navegador	Nós de administração	A porta 80 redireciona para a porta 443 para a interface de usuário do nó de administrador.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
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.
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.
137	UDP	NetBIOS	Cliente SMB	Nós de administração	Usado pela exportação de auditoria baseada em SMB para clientes que exigem suporte NetBIOS. **Nota:** esta porta é necessária apenas se a exportação de auditoria baseada em SMB estiver ativada.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
138	UDP	NetBIOS	Cliente SMB	Nós de administração	Usado pela exportação de auditoria baseada em SMB para clientes que exigem suporte NetBIOS. **Nota:** esta porta é necessária apenas se a exportação de auditoria baseada em SMB estiver ativada.
139	TCP	SMB	Cliente SMB	Nós de administração	Usado pela exportação de auditoria baseada em SMB para clientes que exigem suporte NetBIOS. **Nota:** esta porta é necessária apenas se a exportação de auditoria baseada em SMB estiver ativada.
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 e alarme. 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.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
162	TCP/UDP	Notificações 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.
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 arquivamento	Amazon S3	Usado para acessar o Amazon S3 a partir de nós de arquivamento.
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.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
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.
445	TCP	SMB	Cliente SMB	Nós de administração	Usado pela exportação de auditoria baseada em SMB. **Nota:** esta porta é necessária apenas se a exportação de auditoria baseada em SMB estiver ativada.
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.
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.

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.
8082	TCP	HTTPS	S3 clientes	Nós de gateway	Tráfego externo relacionado a S3 para nós de gateway (HTTPS).
8083	TCP	HTTPS	Clientes Swift	Nós de gateway	Tráfego externo relacionado ao Swift para os nós de gateway (HTTPS).
8084	TCP	HTTP	S3 clientes	Nós de gateway	Tráfego externo relacionado a S3 para nós de gateway (HTTP).
8085	TCP	HTTP	Clientes Swift	Nós de gateway	Tráfego externo relacionado ao Swift para os nós de gateway (HTTP).

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
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.
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.
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 externo relacionado a S3 para nós de storage (HTTPS).
18083	TCP	HTTPS	Clientes Swift	Nós de storage	Tráfego externo relacionado ao Swift para nós de storage (HTTPS).

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
18084	TCP	HTTP	S3 clientes	Nós de storage	Tráfego externo relacionado ao S3 para nós de storage (HTTP).
18085	TCP	HTTP	Clientes Swift	Nós de storage	Tráfego externo relacionado ao Swift para Storage Nodes (HTTP).

Informações relacionadas

"Comunicações internas do nó da grade"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

Instale e atualize o software

Instale o Red Hat Enterprise Linux ou CentOS

Saiba como instalar o software StorageGRID nas implantações do Red Hat Enterprise Linux ou CentOS.

- "Visão geral da instalação"
- "Planejamento e preparação"
- "Implantando nós de grade virtual"
- "Configurar a grelha e concluir a instalação"
- "Automatizando a instalação"
- "Visão geral da API REST de instalação"
- "Onde ir a seguir"
- "Solução de problemas de instalação"
- "Exemplo /etc/sysconfig/network-scripts"

Visão geral da instalação

A instalação de um sistema StorageGRID em um ambiente Linux Red Hat Enterprise (RHEL) ou CentOS Linux inclui três etapas principais.

1. **Preparação**: Durante o Planejamento e a preparação, você executa as seguintes tarefas:
    - Saiba mais sobre os requisitos de hardware e armazenamento do StorageGRID.
    - Saiba mais sobre os detalhes da rede StorageGRID para que você possa configurar sua rede adequadamente. Para obter mais informações, consulte as diretrizes de rede do StorageGRID.
    - Identifique e prepare os servidores físicos ou virtuais que você planeja usar para hospedar seus nós de grade do StorageGRID.
    - Nos servidores que você preparou:
        - Instale o Linux
        - Configure a rede host
        - Configurar o armazenamento do host
        - Instale o Docker
        - Instale os serviços de host do StorageGRID
2. **Implantação**: Implante nós de grade usando a interface de usuário apropriada. Quando você implementa nós de grade, eles são criados como parte do sistema StorageGRID e conetados a uma ou mais redes.
    a. Use os arquivos de configuração de nó e linha de comando do Linux para implantar nós de grade baseados em software nos hosts preparados na etapa 1.
    b. Use o Instalador de dispositivos StorageGRID para implantar nós de dispositivos StorageGRID.

> As instruções de instalação e integração específicas de hardware não estão incluídas no procedimento de instalação do StorageGRID. Para saber como instalar dispositivos StorageGRID, consulte as instruções de instalação e manutenção do seu aparelho.

3. **Configuração**: Quando todos os nós tiverem sido implantados, use o StorageGRIDGrid Manager para configurar a grade e concluir a instalação.

Essas instruções recomendam uma abordagem padrão para implantar e configurar um sistema StorageGRID. Consulte também as informações sobre as seguintes abordagens alternativas:

- Usar uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef, para instalar o RHEL ou CentOS, configurar rede e armazenamento, instalar o Docker e o serviço de host StorageGRID e implantar nós de grade virtual.
- Automatize a implantação e configuração do sistema StorageGRID usando um script de configuração Python (fornecido no arquivo de instalação).
- Automatize a implantação e a configuração dos nós de grade do dispositivo com um script de configuração Python (disponível no arquivo de instalação ou no instalador do dispositivo StorageGRID).
- Se você é um desenvolvedor avançado de implantações do StorageGRID, use as APIS REST de instalação para automatizar a instalação de nós de grade do StorageGRID.

Informações relacionadas

"Planejamento e preparação"

"Implantando nós de grade virtual"

"Configurar a grelha e concluir a instalação"

"Automatizando a instalação"

"Visão geral da API REST de instalação"

"Diretrizes de rede"

Planejamento e preparação

Antes de implantar nós de grade e configurar a grade StorageGRID, você deve estar familiarizado com as etapas e requisitos para concluir o procedimento.

Os procedimentos de implantação e configuração do StorageGRID presumem que você está familiarizado com a arquitetura e o funcionamento do sistema StorageGRID.

Você pode implantar um único local ou vários locais de uma só vez. No entanto, todos os locais precisam atender ao requisito mínimo de ter pelo menos três nós de storage.

Antes de iniciar uma instalação do StorageGRID, você deve:

- Entenda os requisitos de computação do StorageGRID, incluindo os requisitos mínimos de CPU e RAM para cada nó.
- Entenda como o StorageGRID oferece suporte a várias redes para separação de tráfego, segurança e conveniência administrativa e tenha um plano para quais redes você pretende anexar a cada nó do StorageGRID.

Consulte as diretrizes de rede do StorageGRID.

- Compreender os requisitos de storage e desempenho de cada tipo de nó 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.
- Entenda os requisitos para migração de nós, se você quiser realizar manutenção programada em hosts físicos sem qualquer interrupção do serviço.
- Reúna todas as informações de rede com antecedência. A menos que você esteja usando DHCP, reúna os endereços IP para atribuir a cada nó de grade e os endereços IP dos servidores DNS (Domain Name System) e NTP (Network Time Protocol) que serão usados.
- Instale, conete e configure todo o hardware necessário, incluindo quaisquer dispositivos StorageGRID, de acordo com as especificações.

> As instruções de instalação e integração específicas de hardware não estão incluídas no procedimento de instalação do StorageGRID. Para saber como instalar dispositivos StorageGRID, consulte as instruções de instalação e manutenção do seu aparelho.

- Decida qual das ferramentas de implantação e configuração disponíveis você deseja usar.

Informações relacionadas

"Diretrizes de rede"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

Materiais necessários

Antes de instalar o StorageGRID, você deve reunir e preparar os materiais necessários.

Item	Notas
Licença NetApp StorageGRID	Você deve ter uma licença NetApp válida e assinada digitalmente. **Nota**: Uma licença de não produção, que pode ser usada para testes e grades de prova de conceito, está incluída no arquivo de instalação do StorageGRID.
Arquivo de instalação do StorageGRID	Você deve baixar o arquivo de instalação do StorageGRID e extrair os arquivos.

Item	Notas
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 versão • Instruções para administrar o StorageGRID

Informações relacionadas

"Transferir e extrair os ficheiros de instalação do StorageGRID"

"Requisitos do navegador da Web"

"Administrar o StorageGRID"

"Notas de lançamento"

Transferir e extrair os ficheiros de instalação do StorageGRID

Você deve baixar o arquivo de instalação do StorageGRID e extrair os arquivos necessários.

Passos

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

   "NetApp Downloads: 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 aparecer uma instrução Caution/MustRead, leia-a e marque a caixa de seleção.

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

5. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.
6. Na coluna **Instalar StorageGRID**, selecione o software apropriado.

   Transfira o `.tgz` ficheiro de arquivo ou `.zip` para a sua plataforma.

   Os arquivos compatados contêm os arquivos RPM e scripts para Red Hat Enterprise Linux ou CentOS.

   Use o `.zip` arquivo se você estiver executando o Windows no laptop de serviço.

7. Salve e extraia o arquivo de arquivo.
8. Escolha os arquivos que você precisa na lista a seguir.

   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 ou CentOS.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL ou CentOS.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.
	Um arquivo de configuração de exemplo 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.
	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 RHEL ou CentOS para implantação de contêineres do StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.

Informações relacionadas

"Manter recuperar"

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.

Para obter informações sobre servidores suportados, consulte a Matriz de interoperabilidade.

Cada nó do StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Pelo menos 24 GB por nó e 2 a 16 GB menos do que a RAM total do sistema, dependendo do total de RAM disponível e da quantidade de software que não seja StorageGRID executado no sistema

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), considere 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 de administração, monitoramento e atualização do 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 as informações sobre os requisitos de armazenamento.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Requisitos de storage e desempenho"

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

"Atualizar o software"

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 capacidade de migração de nós do StorageGRID, você deve armazenar dados de sistema e dados de objetos em armazenamento compartilhado.

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 AFF

Se o nó StorageGRID usar o storage atribuído a partir de um sistema NetApp AFF, 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 Docker	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.	4.000 GB consulte Requisitos de storage para nós de storage para obter mais informações.
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 a 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 de administração. Como regra geral, 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.

> Os snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte os procedimentos de recuperação e manutenção 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*
Nó de arquivo	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	4.000 GB
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

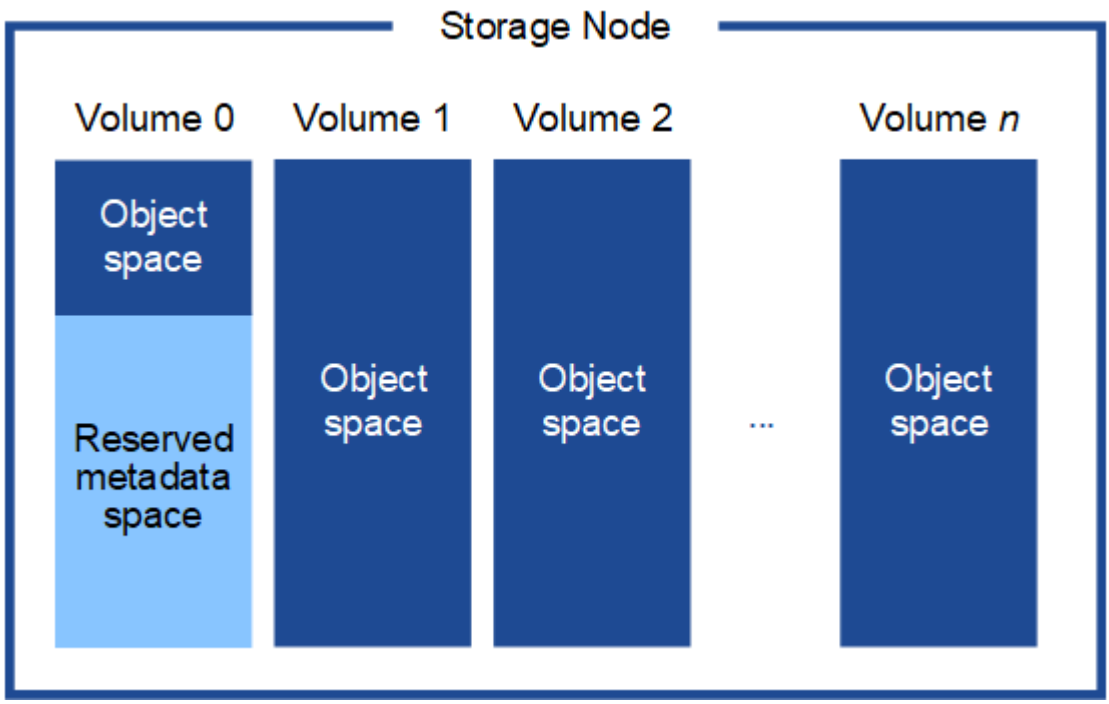
Tipo de nó	Finalidade do LUN	Número de LUNs	Tamanho da LUN
Total		**9**	• Conjunto de contentores: * 300 GB **Dados do sistema:** 670 GB **Dados do objeto:** 12.000 GB

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 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 Storage Read-Only (somente leitura de armazenamento) na inicialização e armazenar somente metadados de objetos.

- Se você estiver instalando um novo sistema StorageGRID 11,5 e cada nó de armazenamento tiver 128 GB ou mais de RAM, deverá atribuir 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 detalhes, vá para as instruções de administração do StorageGRID e procure "armazenamento de metadados de objetos".

"Administrar o StorageGRID"

Informações relacionadas

"Requisitos de migração de contêiner de nós"

"Manter recuperar"

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. Basta mover 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 migração de VM, talvez queira usar essa capacidade em vez do recurso de migração de nós do 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 de recuperação e manutenção para desligar um nó de grade.

Migração do VMware Live não suportada

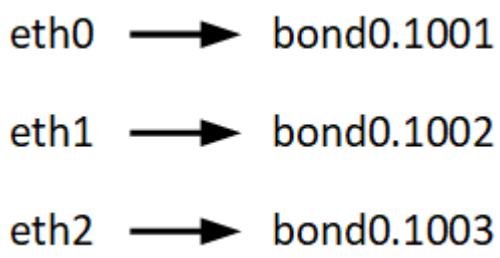
O OpenStack Live Migration e o VMware Live vMotion fazem com que a hora do relógio da máquina virtual salte e não seja compatível com nós de grade de qualquer tipo. Embora raros, tempos de clock incorretos podem resultar em perda de dados ou atualizações de configuração.

A migração fria é suportada. Na migração fria, você desliga os nós do StorageGRID antes de migrá-los entre hosts. Consulte o procedimento para desligar um nó de grade nas instruções de recuperação e manutenção.

Nomes de interface de rede consistentes

Para mover um nó de um host para outro, o serviço de host do 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; consulte ""Configurando a rede de host"" para alguns exemplos.

Armazenamento compartilhado

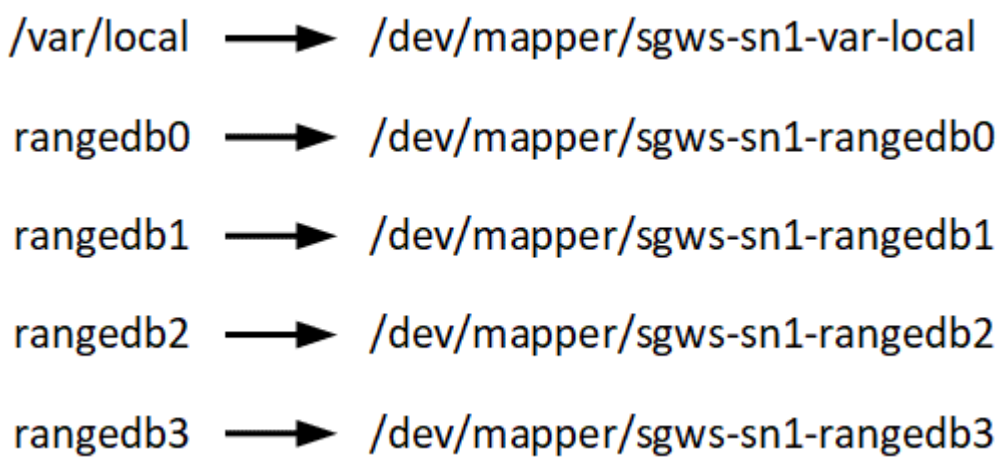
Para conseguir migrações de nós rápidas e de baixa sobrecarga, o recurso de migração de nós do StorageGRID não move fisicamente os dados dos nós. Em vez disso, a migração de nós é realizada como um par de operações de exportação e importação, da seguinte forma:

1. Durante a operação de exportação de nós, 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 nós, 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.



Informações relacionadas

"Configurando a rede host"

"Manter recuperar"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Ferramentas de implantação

Você pode se beneficiar da automação de toda ou parte da instalação do StorageGRID.

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.

Se você estiver interessado em automatizar toda ou parte da implantação do StorageGRID, revise ""Automatizar a instalação"" antes de iniciar o processo de instalação.

Informações relacionadas

"Visão geral da API REST de instalação"

"Automatizando a instalação"

Preparando os anfitriões

Você deve concluir as etapas a seguir para preparar seus hosts físicos ou virtuais para o StorageGRID. Observe que você pode automatizar muitas ou todas essas etapas usando estruturas de configuração de servidor padrão, como Ansible, Puppet ou Chef.

Informações relacionadas

"Automatizando a instalação e a configuração do serviço de host StorageGRID"

Instalando o Linux

É necessário instalar o Red Hat Enterprise Linux ou CentOS Linux em todos os hosts de grade. Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

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, o NetApp recomenda selecionar 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.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Configurando a rede host

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.

O que você vai precisar

- Você revisou as diretrizes de rede do StorageGRID.

  "Diretrizes de rede"

- Você analisou as informações sobre os requisitos de migração de contêineres do nó.

  "Requisitos de migração de contêiner de nós"

- Se você estiver usando hosts virtuais, leia as considerações e recomendações sobre a clonagem de endereços MAC antes de configurar a rede host.

  "Considerações e recomendações para clonagem de endereços MAC"

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 são máquinas virtuais e você está implantando um ou dois nós de StorageGRID para cada host, você pode simplesmente 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

"Diretrizes de rede"

"Requisitos de migração de contêiner de nós"

"Criando arquivos de configuração de nó"

Considerações e recomendações para clonagem de endereços MAC

A clonagem de endereços MAC faz com que o contentor Docker 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. Fazer com que o contentor Docker use o endereço MAC da NIC dedicada no host permite evitar o uso de configurações de rede de modo promíscuo.

> 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 Docker 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

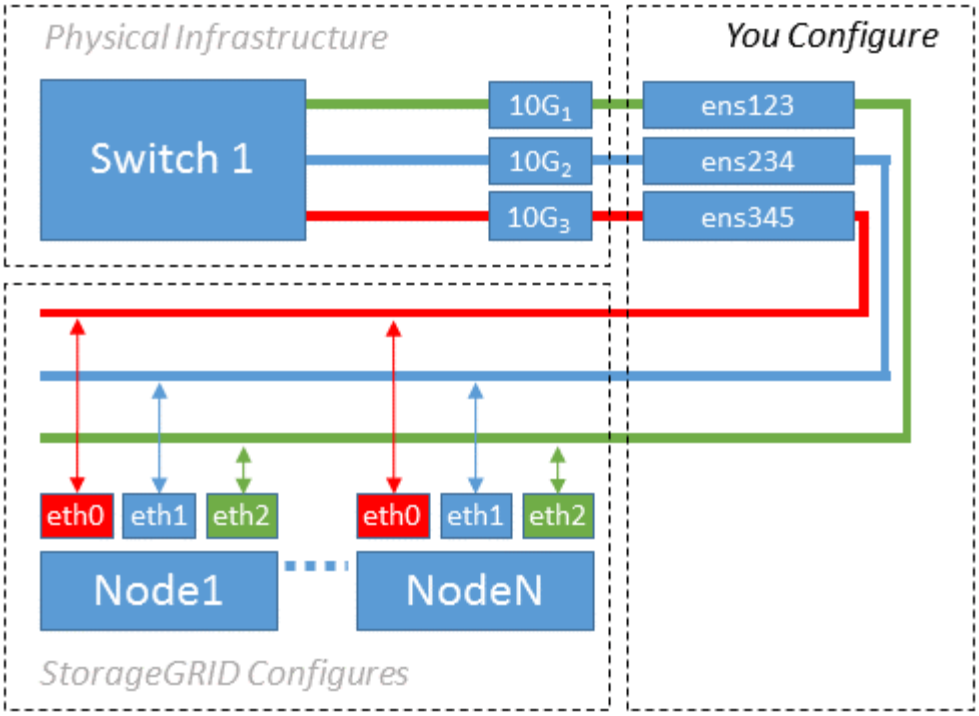
Exemplo de clonagem MAC ativada com um host com endereço MAC de 11:22:33:44:55:66 para a interface ens256 e as seguintes chaves no arquivo de configuração do nó:

- `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.

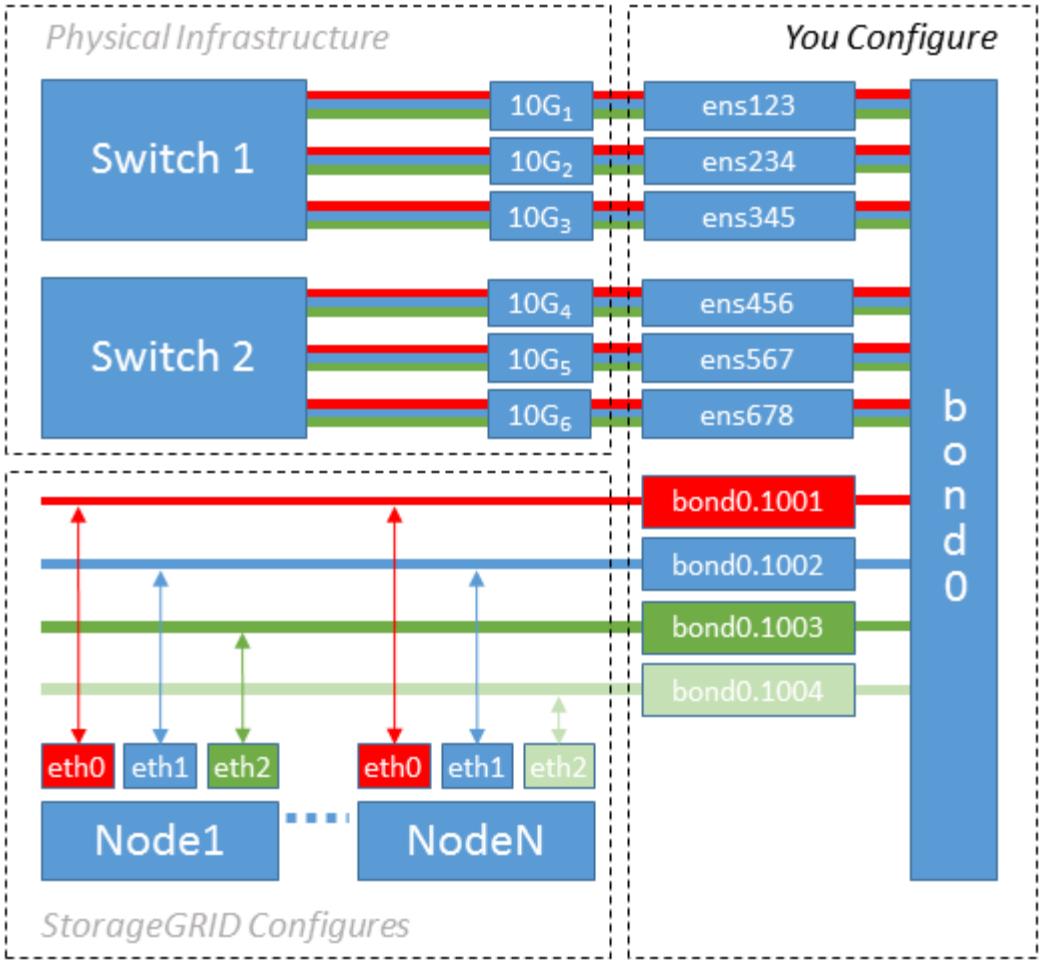
Exemplo 2: VLANs de transporte de ligação LACP

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 a ligação em cada host, por exemplo, bond0.

2. Crie interfaces VLAN que usam essa ligação como seu "'dispositivo físico associado," `using the standard VLAN interface naming convention `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"

Configuração do storage de host

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

O que você vai precisar

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 volumes de armazenamento de bloco (LUNs) 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.

Evite usar arquivos de dispositivo especiais "'RAW'" (`/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 LUNs iSCSI e multipathing de mapeamento de dispositivos, considere usar aliases 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
     }
     …
```

Isso fará com que os aliases apareçam como dispositivos de bloco `/dev/mapper` no diretório no 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 oferecer suporte à migração de nós do StorageGRID e usando multipathing de mapeamento de dispositivos, você poderá criar e instalar um comum `/etc/multipath.conf` em todos os hosts colocalizados. 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.

Informações relacionadas

"Instalando o Docker"

Configurando o volume de armazenamento do Docker

Antes de instalar o Docker, talvez seja necessário formatar o volume de armazenamento do Docker e montá-lo `/var/lib/docker` no .

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.

Instalando o Docker

O sistema StorageGRID é executado no Red Hat Enterprise Linux ou CentOS como uma coleção de contentores Docker. Antes de poder instalar o StorageGRID, você deve instalar o Docker.

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 1.10.3 ou posterior.

```
Client:
  Version: 1.10.3
  API version: 1.22
  Package version: docker-common-1.10.3-46.el7.14.x86_64
  Go version: go1.6.2
  Git commit: 5206701-unsupported
  Built: Mon Aug 29 14:00:01 2016
  OS/Arch: linux/amd64

Server:
  Version: 1.10.3
  API version: 1.22
  Package version: docker-common-1.10.3-46.el7.14.x86_64
  Go version: go1.6.2
  Git commit: 5206701-unsupported
  Built: Mon Aug 29 14:00:01 2016
  OS/Arch: linux/amd64
```

Informações relacionadas

"Configuração do storage de host"

Instalação dos 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 Yum incluídos no arquivo de instalação para instalar os pacotes RPM remotamente. Veja as instruções do repositório Yum 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 yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
```

```
sudo yum --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.

Implantando nós de grade virtual

Para implantar nós de grade virtual em hosts do Red Hat Enterprise Linux ou CentOS, você cria arquivos de configuração de nós para todos os nós, valida os arquivos e inicia o serviço de host do StorageGRID, que inicia os nós. Se você precisar implantar qualquer nó de storage do dispositivo StorageGRID, consulte as instruções de instalação e manutenção do dispositivo depois de implantar todos os nós virtuais.

- "Criando arquivos de configuração de nó"
- "Validar a configuração do StorageGRID"
- "Iniciando o serviço de host do StorageGRID"

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

"SG5600 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG6000 dispositivos de armazenamento"

Criando arquivos de configuração de nó

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.

Onde coloco os arquivos de configuração do nó?

Você deve colocar 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.

O que nomeo os arquivos de configuração do 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.

O que está em um arquivo de configuração de nó?

Os arquivos de configuração contêm pares chave/valor, com uma chave e um valor por linha. Para cada par chave/valor, você deve seguir 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.

Algumas chaves são necessárias para cada nó, enquanto outras são opcionais ou apenas necessárias para

determinados tipos de nó.

A tabela define os valores aceitáveis para todas as chaves suportadas. Na coluna do meio:

R: Necessário e BP: Melhor prática e o: Opcional

Chave	R, BP OU O?	Valor
ADMIN_IP	BP	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. Veja como os nós de grade descobrem o nó de administrador principal." **Nota**: Este valor é ignorado, e pode ser proibido, no nó Admin principal.
ADMIN_NETWORK_CONFIG	O	DHCP, ESTÁTICO OU DESATIVADO
ADMIN_NETWORK_ESL	O	Lista de sub-redes separadas por vírgulas na notação CIDR à qual esse nó deve se comunicar através do gateway Admin Network. Exemplo: 172.16.0.0/21,172.17.0.0/21

Chave	R, BP OU O?	Valor
ADMIN_NETWORK_GATEWAY	O (**R**)	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. **Nota**: Este parâmetro é necessário se ADMIN_NETWORK_ESL for especificado. Exemplos: • 1.1.1.1 • 10.224.4.81
ADMIN_NETWORK_IP	O	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
ADMIN_NETWORK_MAC	O	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

Chave	R, BP OU O?	Valor
ADMIN_NETWORK_MASK	O	IPv4 máscara de rede para este nó, na rede Admin. Esta chave só é necessária quando ADMIN_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores. Exemplos: • 255.255.255.0 • 255.255.248.0
ADMIN_NETWORK_MTU	O	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

Chave	R, BP OU O?	Valor
ADMIN_NETWORK_TARGET	BP	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
ADMIN_NETWORK_TARGET_TYPE	O	Interface (Este é o único valor suportado.)

Chave	R, BP OU O?	Valor
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	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, consulte as considerações e recomendações para clonagem de endereços MAC. "Considerações e recomendações para clonagem de endereços MAC"
ADMIN_ROLE	**R**	Primário ou não primário Esta chave só é necessária quando NODE_TYPE: VM_Admin_Node; não a especifique para outros tipos de nó.

Chave	R, BP OU O?	Valor
BLOCK_DEVICE_AUDIT_LOGS	**R**	Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento persistente de logs de auditoria. 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-audit-logs`

Chave	R, BP OU O?	Valor
BLOCK_DEVICE_RANGEDB_00 BLOCK_DEVICE_RANGEDB_01 BLOCK_DEVICE_RANGEDB_02 BLOCK_DEVICE_RANGEDB_03 BLOCK_DEVICE_RANGEDB_04 BLOCK_DEVICE_RANGEDB_05 BLOCK_DEVICE_RANGEDB_06 BLOCK_DEVICE_RANGEDB_07 BLOCK_DEVICE_RANGEDB_08 BLOCK_DEVICE_RANGEDB_09 BLOCK_DEVICE_RANGEDB_10 BLOCK_DEVICE_RANGEDB_11 BLOCK_DEVICE_RANGEDB_12 BLOCK_DEVICE_RANGEDB_13 BLOCK_DEVICE_RANGEDB_14 BLOCK_DEVICE_RANGEDB_15	**R**	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 NÓ_TIPO: VM_Storage_Node; não a especifique para outros tipos de nó. Somente block_DEVICE_RANGEDB_00 é necessário; o resto é opcional. O dispositivo de bloco especificado para block_DEVICE_RANGEDB_00 deve ter pelo menos 4 TB; os outros podem ser menores. **Nota**: Não deixe lacunas. Se você especificar block_DEVICE_RANGEDB_05, você também deve especificar BLOCK_DEVICE_RANGEDB_04. 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-0`

Chave	R, BP OU O?	Valor
BLOCK_DEVICE_TABLES	**R**	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`
BLOCK_DEVICE_VAR_LOCAL	**R**	Caminho e nome do arquivo especial do dispositivo de bloco este nó usará para seu armazenamento persistente /var/local. 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`
CLIENT_NETWORK_CONFIG	O	DHCP, ESTÁTICO OU DESATIVADO

Chave	R, BP OU O?	Valor
CLIENT_NETWORK_GATEWAY	O	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
CLIENT_NETWORK_IP	O	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
CLIENT_NETWORK_MAC	O	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
CLIENT_NETWORK_MASK	O	IPv4 máscara de rede para este nó na rede do cliente. Esta chave só é necessária quando CLIENT_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores. Exemplos: • 255.255.255.0 • 255.255.248.0

Chave	R, BP OU O?	Valor
CLIENT_NETWORK_MTU	O	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

Chave	R, BP OU O?	Valor
CLIENT_NETWORK_TARGET	BP	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
CLIENT_NETWORK_TARGET_TYPE	O	Interface (Este é apenas o valor suportado.)

Chave	R, BP OU O?	Valor
CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	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, consulte as considerações e recomendações para clonagem de endereços MAC. "Considerações e recomendações para clonagem de endereços MAC"
GRID_NETWORK_CONFIG	BP	ESTÁTICO ou DHCP (O padrão é ESTÁTICO se não for especificado.)
GRID_NETWORK_GATEWAY	**R**	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.

Chave	R, BP OU O?	Valor
GRID_NETWORK_IP	**R**	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
GRID_NETWORK_MAC	O	O endereço MAC da interface Grid Network 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:C2:27:30
GRID_NETWORK_MASK	O	IPv4 máscara de rede para este nó na rede de Grade. Esta chave só é necessária quando GRID_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores. Exemplos: • 255.255.255.0 • 255.255.248.0

Chave	R, BP OU O?	Valor
GRID_NETWORK_MTU	O	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

Chave	R, BP OU O?	Valor
GRID_NETWORK_TARGET	**R**	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
GRID_NETWORK_TARGET_TYPE	O	Interface (Este é o único valor suportado.)
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	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, consulte as considerações e recomendações para clonagem de endereços MAC. "Considerações e recomendações para clonagem de endereços MAC"

Chave	R, BP OU O?	Valor
MÁXIMO_RAM	O	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 as instruções para administrar o StorageGRID para obter uma descrição do que é o espaço reservado de metadados. O formato deste campo é `<number><unit>`, onde `<unit>` pode ser `b`, `k`, , `m` `g` ou . Exemplos: 13 24 g 38654705664b **Nota**: Se você quiser usar essa opção, você deve habilitar o suporte do kernel para cgroups de memória.
NODE_TYPE (TIPO DE NÓ)	**R**	Tipo de nó: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway

Chave	R, BP OU O?	Valor
PORT_REMAP	O	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 de nó de grade"" ou ""Comunicações externas"". **IMPORTANTE**: Não remapear 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 o protocolo é tcp ou udp. Por exemplo: `PORT_REMAP = client/tcp/18082/443`

Chave	R, BP OU O?	Valor
PORT_REMAP_INBOUND	O	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 remapear 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 o protocolo é tcp ou udp. Por exemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Informações relacionadas

"Como os nós de grade descobrem o nó de administração principal"

"Diretrizes de rede"

"Administrar o StorageGRID"

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 de 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
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 nó de arquivo

- Exemplo de nome do arquivo:* `/etc/storagegrid/nodes/dc1-arc1.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
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
```

Validar 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.

```
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
```

Iniciando 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
```

Para qualquer nó que retorna um status de "'Not-Running'" ou "'stopped'", execute o seguinte comando:

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

3. Se você já ativou e iniciou o serviço de host StorageGRID (ou se não tiver certeza se o serviço foi ativado e iniciado), execute também o seguinte comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configurar a grelha e concluir a instalação

Você conclui a instalação configurando o sistema StorageGRID a partir do Gerenciador de Grade no nó Admin principal.

- "Navegando para o Gerenciador de Grade"
- "Especificando as informações da licença do StorageGRID"
- "Adicionar sites"
- "Especificando sub-redes de rede de Grade"
- "Aprovando nós de grade pendentes"
- "Especificando informações do servidor Network Time Protocol"
- "Especificando informações do servidor do sistema de nomes de domínio"
- "Especificando as senhas do sistema StorageGRID"
- "Rever a sua configuração e concluir a instalação"
- "Diretrizes de pós-instalação"

Navegando para o Gerenciador de Grade

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

O que você vai precisar

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 um dos seguintes endereços:

```
https://primary_admin_node_ip

client_network_ip
```

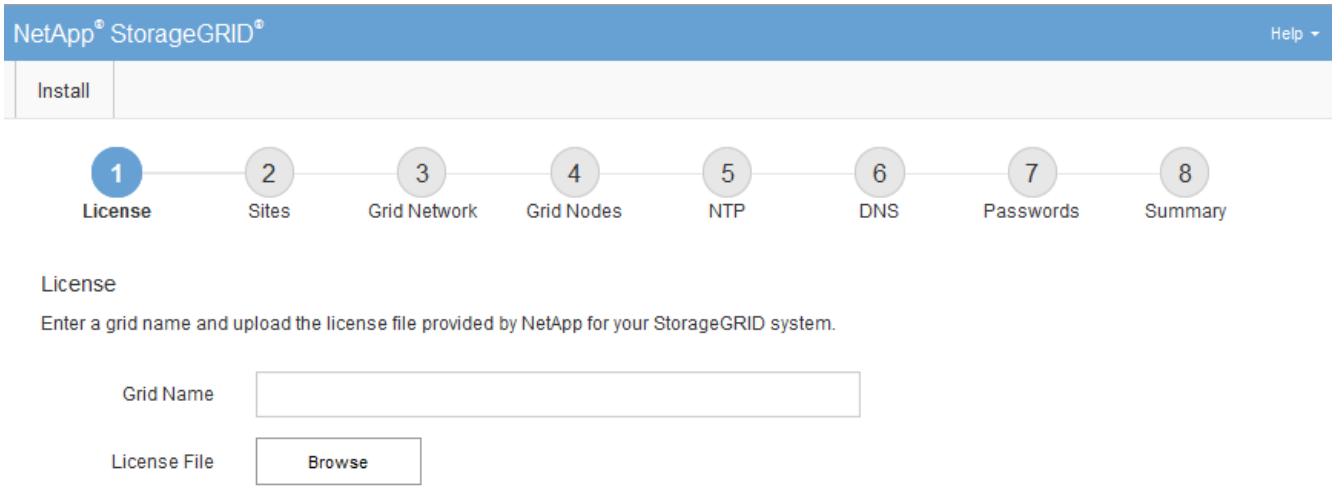
Como alternativa, você pode acessar o Gerenciador de Grade na porta 8443:

`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. Clique em **Instalar um sistema StorageGRID**.

   É apresentada a página utilizada para configurar um sistema StorageGRID.



Especificando 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

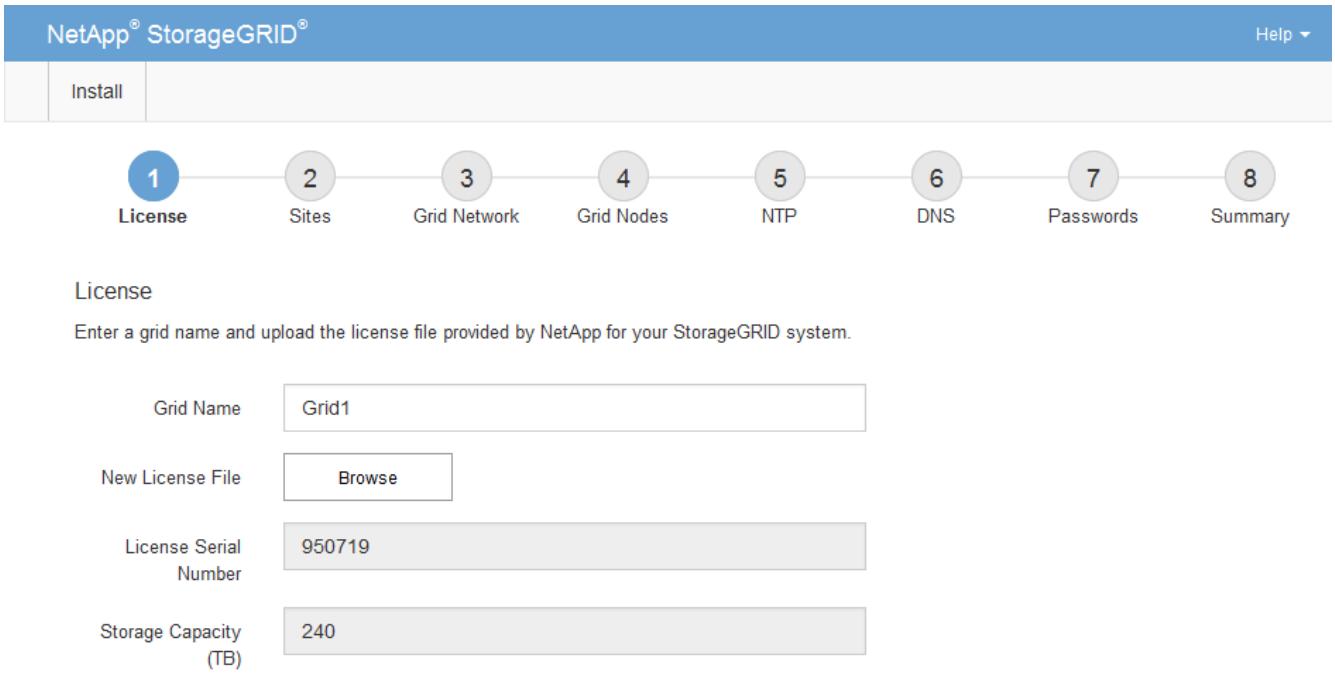
1. Na página Licença, insira um nome significativo para o seu sistema StorageGRID em **Nome da Grade**.

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

2. Clique em **Procurar**, localize o ficheiro de licença do NetApp (`NLFunique_id.txt`) e clique em **abrir**.

   O arquivo de licença é validado e o número de série e a capacidade de armazenamento licenciada são exibidos.

> 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. Clique em **seguinte**.

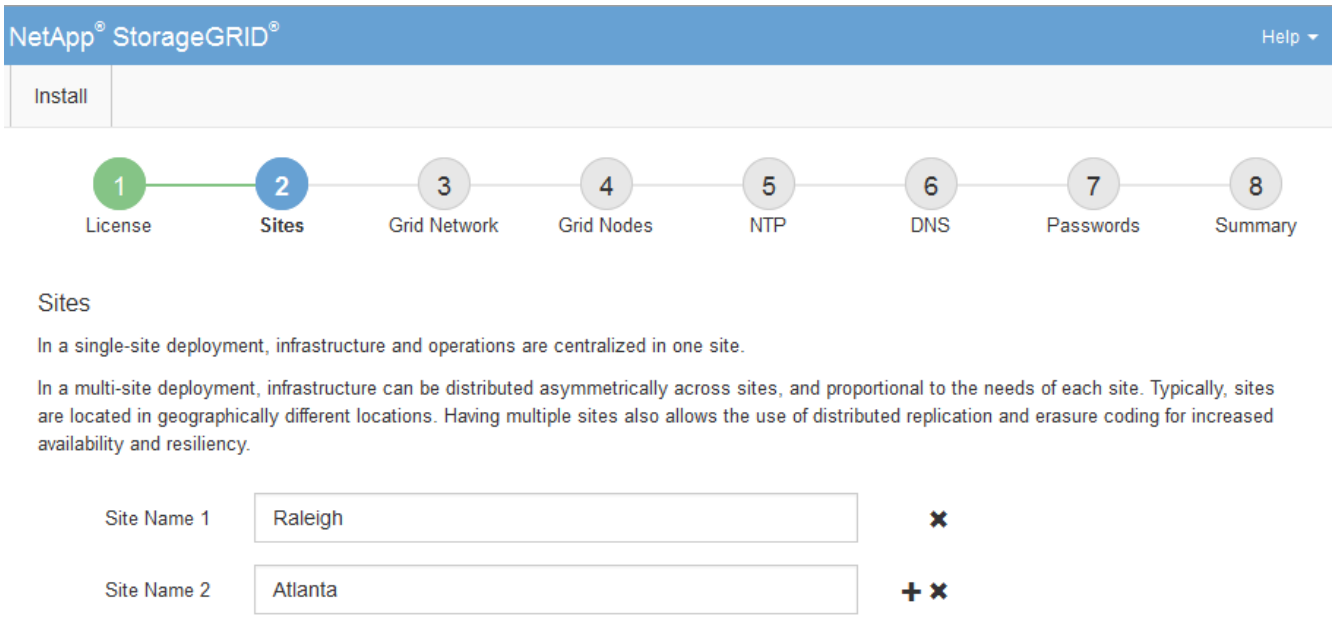
Adicionar sites

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**.

Especificando sub-redes de rede de Grade

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

Sobre esta tarefa

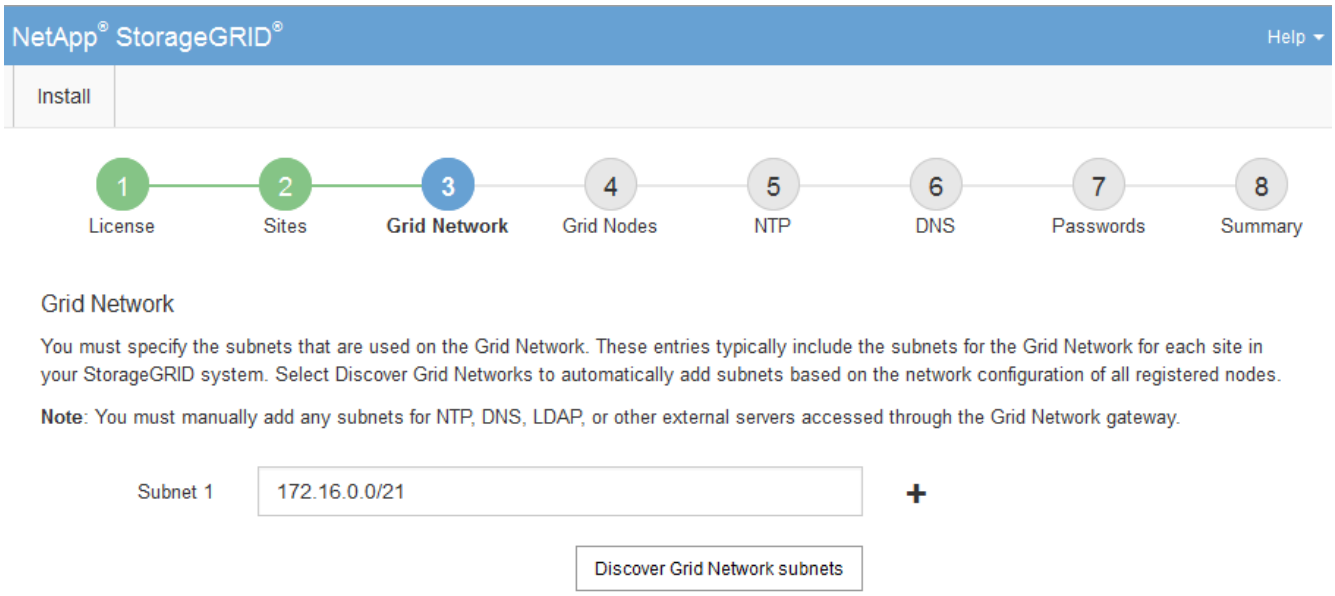
As entradas de sub-rede incluem as sub-redes para a rede de Grade para cada site no seu sistema StorageGRID, juntamente com quaisquer sub-redes que precisam ser acessíveis através da rede de Grade.

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.

   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.



3. Clique em **seguinte**.

Aprovando nós de grade pendentes

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

O que você vai precisar

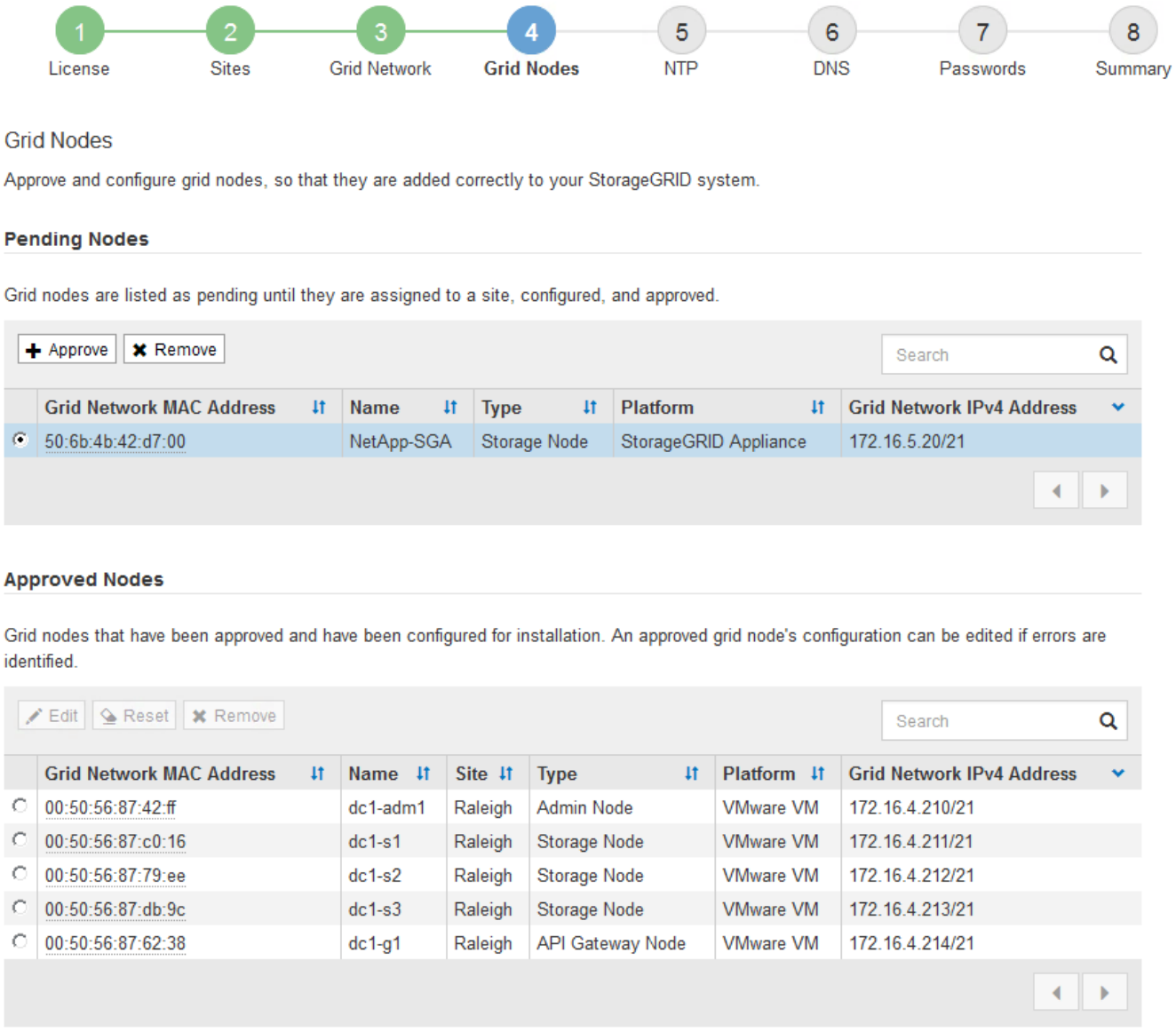
Todos os nós de grade de dispositivos virtuais e StorageGRID devem ter sido implantados.

Passos

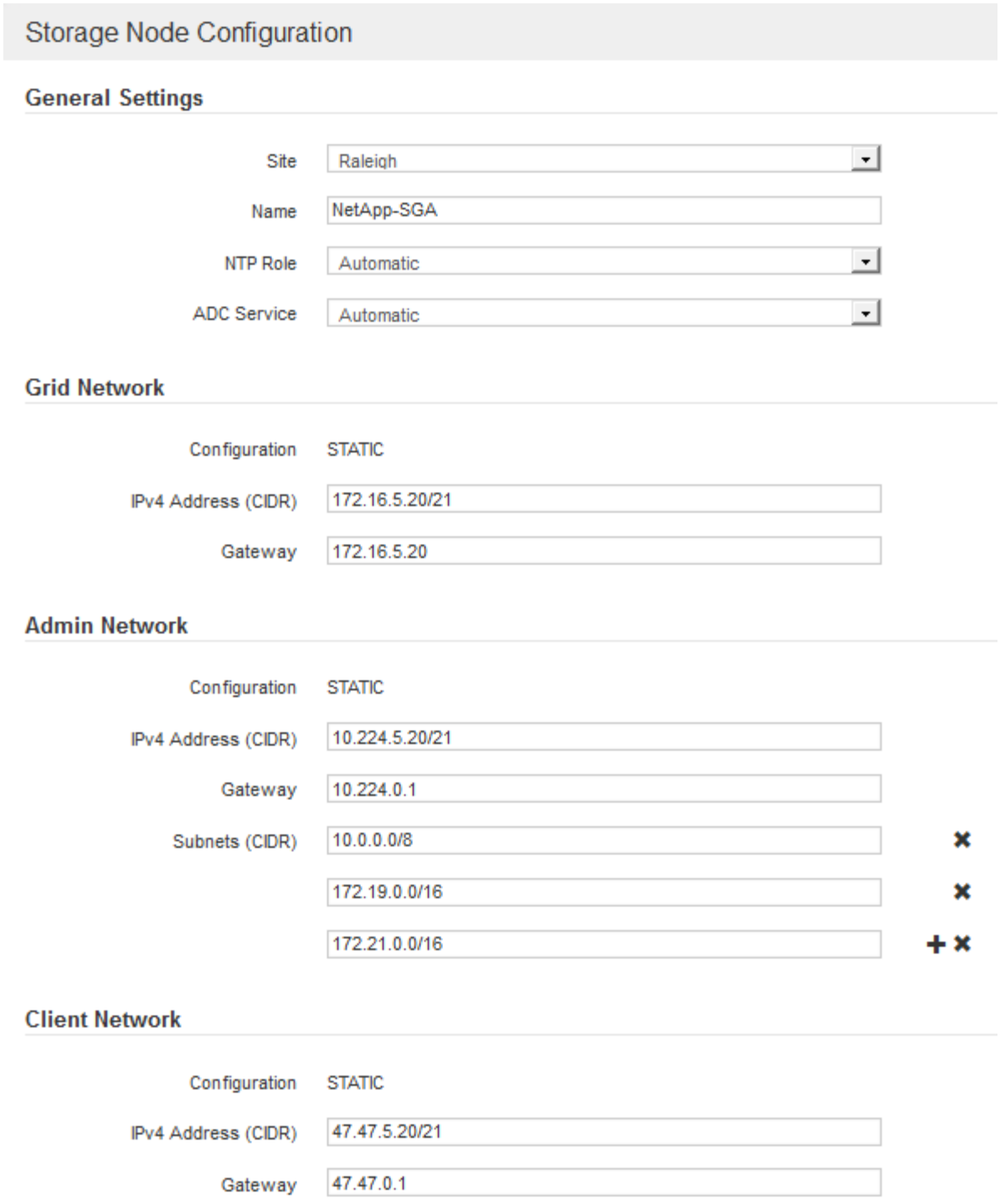
1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade implantados.

   Se um nó de grade estiver ausente, confirme que ele foi implantado com sucesso.

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 site com o qual este nó de grade será associado.
- **Nome**: O nome que será atribuído ao nó e o nome que será exibido no Gerenciador de Grade. O nome padrão é o nome que você especificou quando configurou o nó. Durante esta etapa do processo de instalação, você pode alterar o nome conforme necessário.

> Depois de concluir a instalação, não é possível alterar o nome do nó.

> 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.

- **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. Você não pode 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 garantir que o endereço IP resultante não esteja 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 garantir que o endereço IP resultante não esteja 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 **Configurar rede Configuração de ligação** 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, redefina 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.

   Para obter informações adicionais, consulte as instruções de instalação e manutenção 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 garantir que o endereço IP resultante não esteja 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 **Configurar rede Configuração de ligação** 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, redefina o nó.

   f. Remova o nó da tabela nós pendentes.

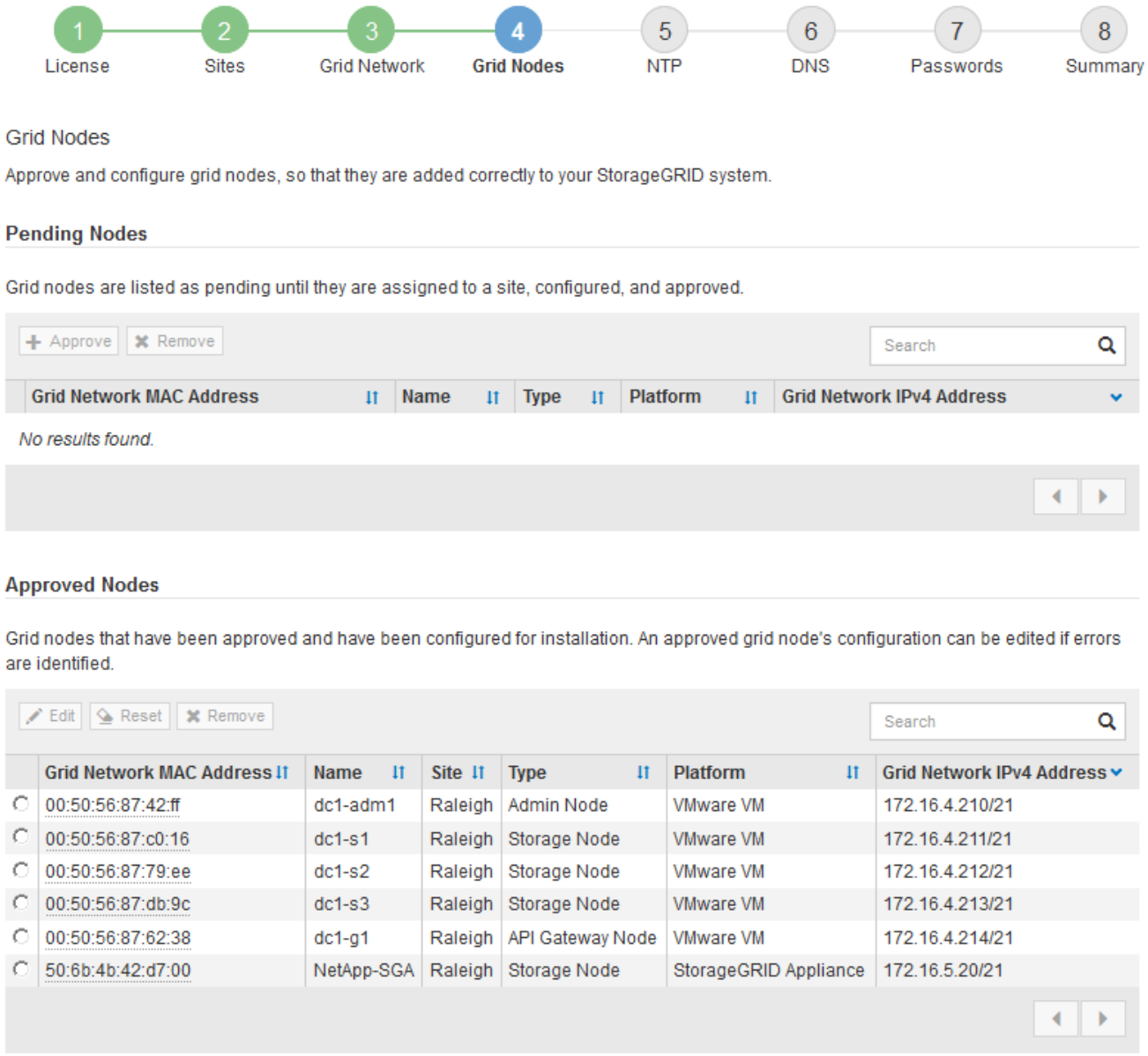
   g. Aguarde que o nó reapareça na lista de nós pendentes.

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

      Para obter informações adicionais, consulte as instruções de instalação e manutenção 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**.

Especificando 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.

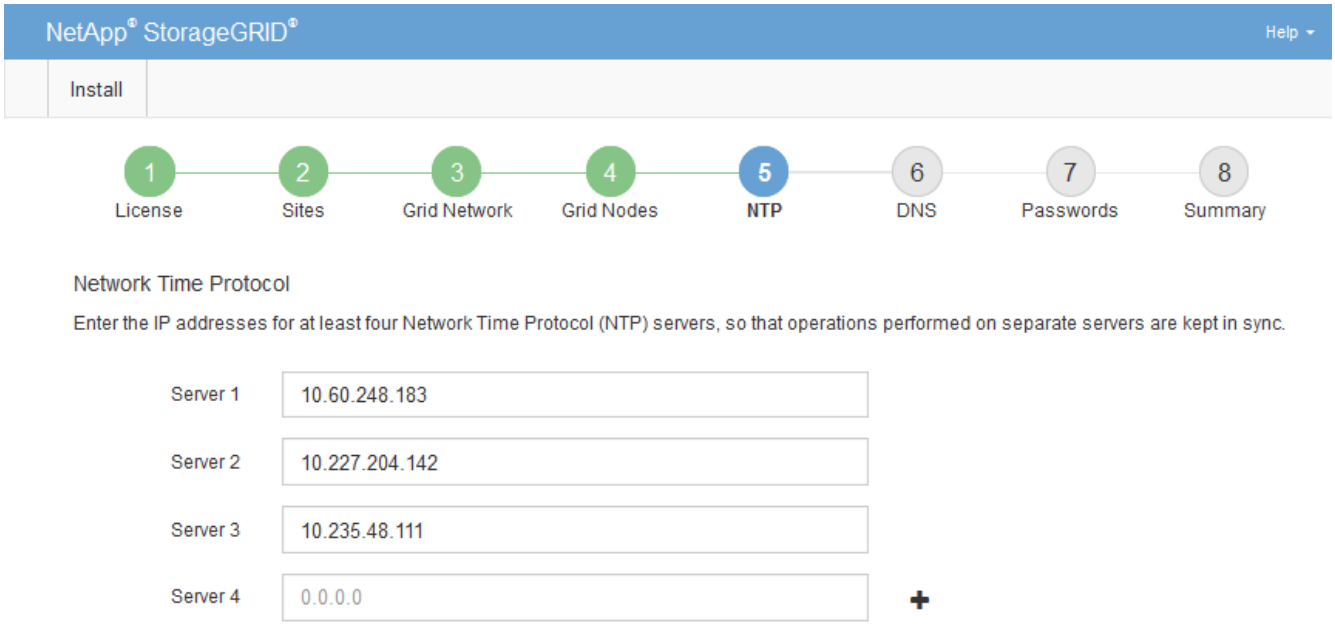
> Ao especificar a fonte NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft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

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**.

Especificando informações do servidor do sistema de nomes de domínio

Você deve especificar informações do sistema de nomes de domínio (DNS) para o seu sistema StorageGRID, para que você possa acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

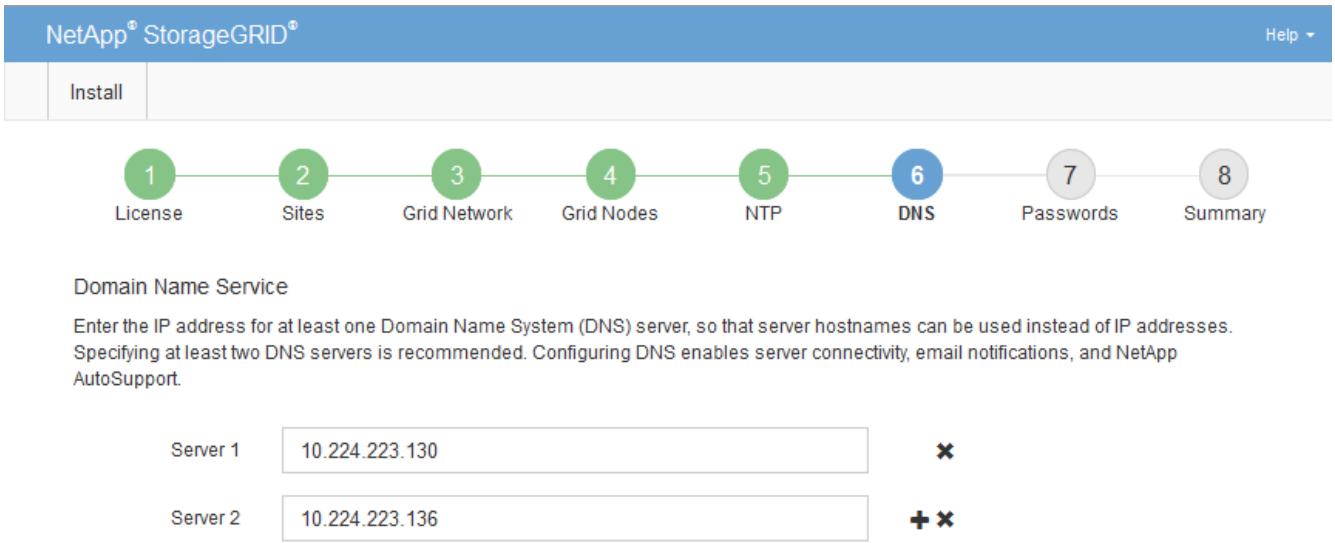
Especificar informações do servidor DNS permite que você use nomes de host de nome de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações de e-mail e AutoSupport. É recomendável especificar pelo menos dois servidores DNS.

> Forneça dois a seis endereços IPv4 para servidores DNS. Você deve selecionar servidores DNS que cada site pode acessar localmente no caso de rede ser aterrissada. Isso é para garantir que um site islanded continua a ter acesso ao serviço DNS. Depois de configurar a lista de servidores DNS em toda a grade, você pode personalizar ainda mais a lista de servidores DNS para cada nó. Para obter detalhes, consulte as informações sobre como modificar a configuração DNS nas instruções de recuperação e manutenção.

Se as informações do servidor DNS forem omitidas ou configuradas incorretamente, um alarme DNST será acionado no serviço SSM de cada nó da grade. O alarme é apagado quando o DNS está configurado corretamente e as novas informações do servidor atingiram todos os nós da grade.

Passos

1. 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**.

Especificando 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 arquivo Passwords.txt 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.

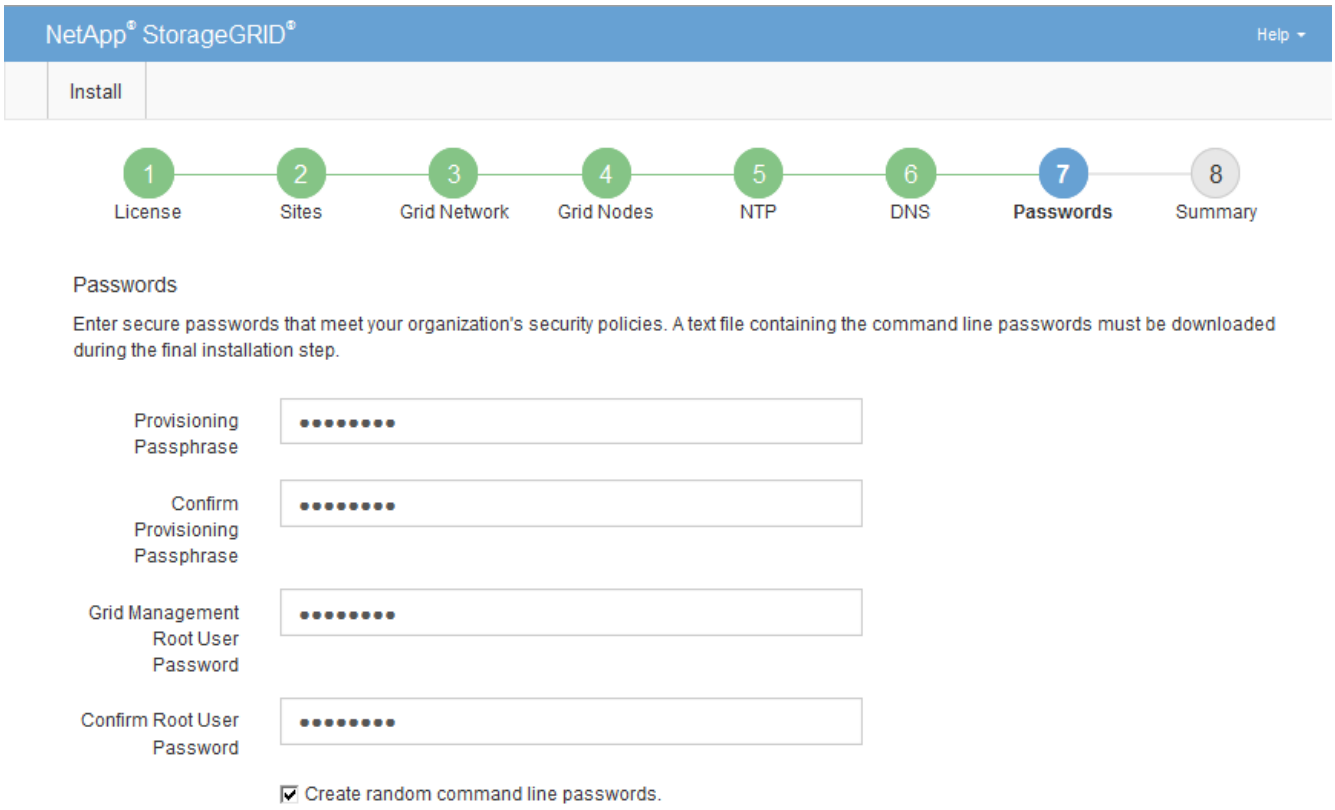
   Armazene a senha de provisionamento em um local seguro.

   > Se após a conclusão da instalação e você quiser alterar a senha de provisionamento mais tarde, você pode usar o Gerenciador de Grade. Selecione **Configuração Controle de Acesso senhas de Grade**.

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 opcionalmente 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. Desmarque **criar senhas de linha de comando aleatórias** apenas para grades de demonstração se você quiser usar senhas padrão para acessar os 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. Tem de transferir este ficheiro para concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas `Passwords.txt` no arquivo, contido no arquivo Pacote de recuperação.

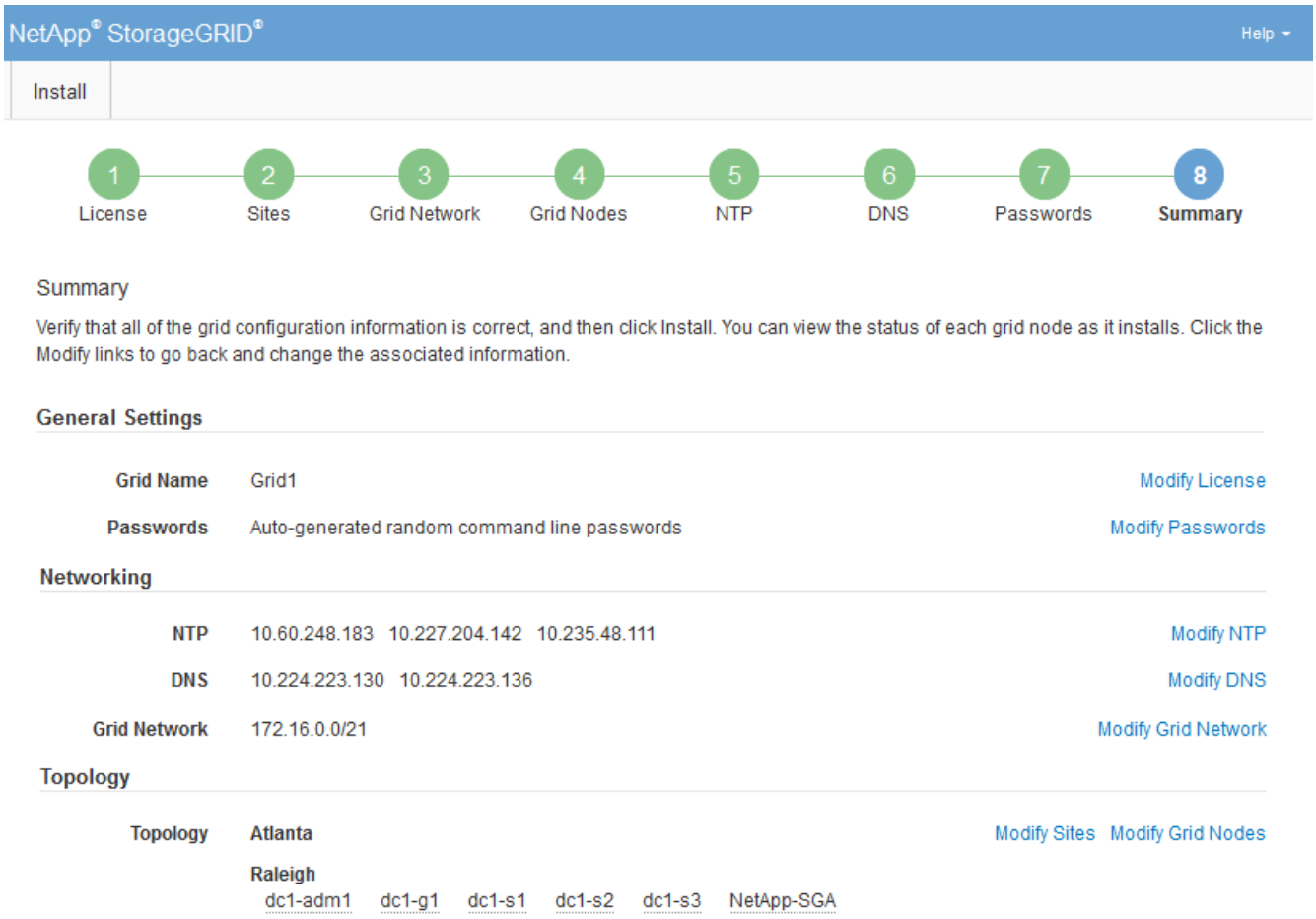
6. Clique em **seguinte**.

Rever a sua configuração e concluir 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.

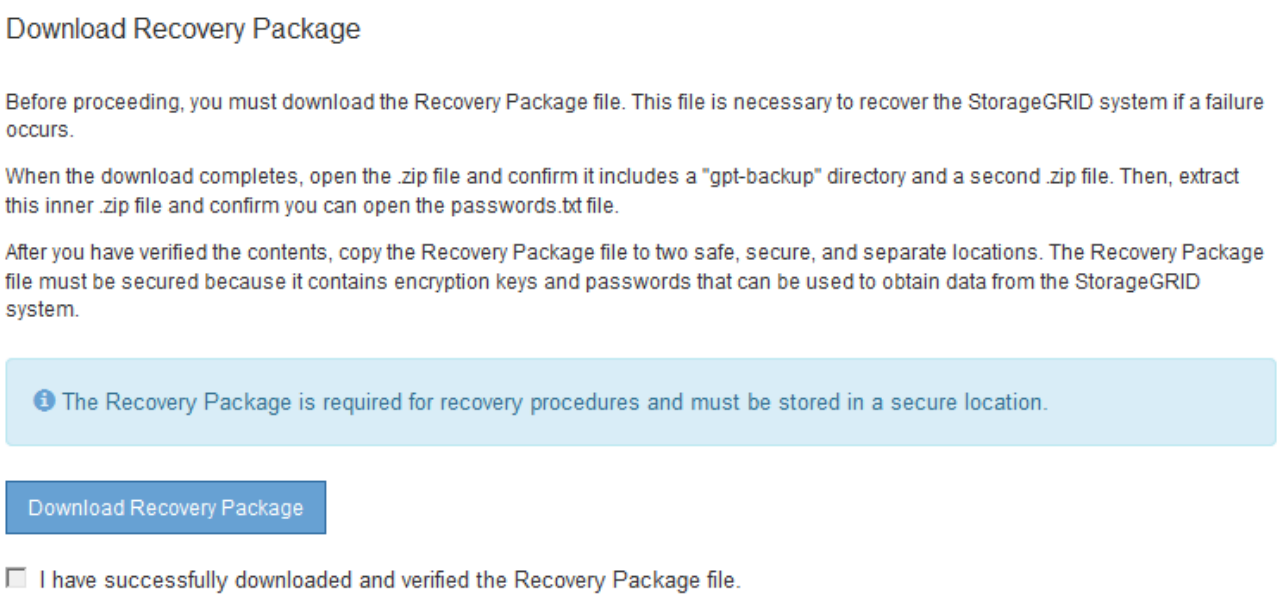
4. Clique em **Download Recovery Package**.

   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 não é possível concluir a instalação e aceder ao sistema StorageGRID até transferir e verificar este ficheiro.

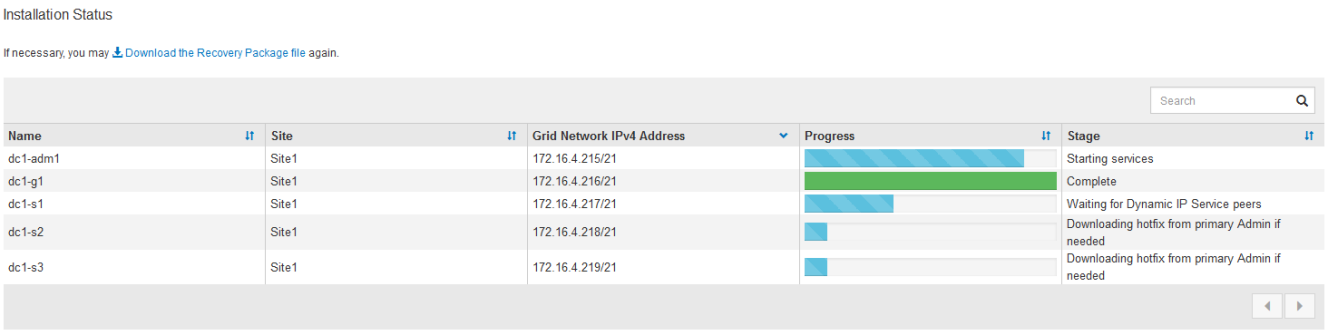
5. Verifique se você pode extrair o conteúdo do `.zip` arquivo e salvá-lo em dois locais seguros, seguros e separados.

> 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 seus endereços IP são alterados, o que pode causar interrupções se uma alteração de endereço 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. Consulte as informações sobre como configurar endereços IP nas instruções de recuperação e manutenção.
- 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.

Automatizando a instalação

É possível 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.

Se você estiver interessado em automatizar toda ou parte da implantação do StorageGRID, revise ""Automatizar a instalação"" antes de iniciar o processo de instalação.

Automatizando 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 RHEL ou CentOS, adicionar StorageGRID aos seus playbooks ou receitas deve ser simples.

Um exemplo de função e manual do Ansible são fornecidos com o arquivo de instalação na `/extras` pasta. 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.

Automatizando a configuração do StorageGRID

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

O que você vai precisar

- 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 amostra (`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, você precisa extrair o `Passwords.txt` arquivo e procurar 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

"Configurar a grelha e concluir a instalação"

"Visão geral da API REST de instalação"

Visão geral da 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 (JavaScript Object Notation).

Todas as operações de API que você executa usando a página da Web do API Docs 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 seu sistema StorageGRID e, caso precise 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.

Onde ir a seguir

Depois de concluir uma instalação, você deve executar uma série de etapas de integração e configuração. Alguns passos são necessários; outros são opcionais.

Tarefas necessárias

- Crie uma conta de locatário para cada protocolo de cliente (Swift ou S3) que será usado para armazenar objetos em seu sistema StorageGRID.
- Controle o acesso ao sistema configurando grupos e contas de usuário. Opcionalmente, você pode configurar uma fonte de identidade federada (como ative Directory ou OpenLDAP), para que você possa importar grupos de administração e usuários. Ou, você pode criar grupos e usuários locais.
- Integre e teste os aplicativos cliente API S3 ou Swift que você usará para fazer upload de objetos para seu sistema StorageGRID.
- Quando estiver pronto, configure as regras de gerenciamento do ciclo de vida das informações (ILM) e a

política de ILM que você deseja usar para proteger os dados do objeto.

> Quando você instala o StorageGRID, a política ILM padrão, Diretiva de cópias de linha de base 2, está ativa. Esta política inclui a regra ILM (fazer 2 cópias) e aplica-se se nenhuma outra política tiver sido ativada.

- Se a instalação incluir nós de storage do dispositivo, use o software SANtricity para concluir as seguintes tarefas:
  - Ligue a cada dispositivo StorageGRID.
  - Verifique a receção dos dados do AutoSupport.
- Se o seu sistema StorageGRID incluir quaisquer nós de arquivamento, configure a conexão do nó de arquivamento ao sistema de storage de arquivamento externo de destino.

> Se algum nó de arquivamento usar o Tivoli Storage Manager como o sistema de armazenamento de arquivamento externo, você também deve configurar o Tivoli Storage Manager.

- Revise e siga as diretrizes de fortalecimento do sistema StorageGRID para eliminar os riscos de segurança.
- Configurar notificações por e-mail para alertas do sistema.

Tarefas opcionais

- Se você quiser receber notificações do sistema de alarme (legado), configure listas de e-mail e notificações por e-mail para alarmes.
- Atualize os endereços IP do nó da grade se eles tiverem sido alterados desde que você planejou sua implantação e gerou o Pacote de recuperação. Consulte as informações sobre como alterar endereços IP nas instruções de recuperação e manutenção.
- Configure a criptografia de armazenamento, se necessário.
- Configure a compactação de armazenamento para reduzir o tamanho dos objetos armazenados, se necessário.
- Configurar acesso de cliente de auditoria. Você pode configurar o acesso ao sistema para fins de auditoria por meio de um compartilhamento de arquivos NFS ou CIFS. Consulte as instruções para administrar o StorageGRID.

> A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

Solução de 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, consulte as instruções para monitoramento e solução de problemas do StorageGRID. Para obter ajuda para solucionar problemas de instalação do aparelho, consulte as instruções de instalação e manutenção dos seus aparelhos. Se precisar de ajuda adicional, entre em Contato com o suporte técnico.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Suporte à NetApp"

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 VLAN que subtendem a ligação para uso como interfaces de rede StorageGRID, Admin e 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 Ubuntu ou Debian

Saiba como instalar o software StorageGRID em implantações Ubuntu ou Debian.

- "Visão geral da instalação"
- "Planejamento e preparação"
- "Implantando nós de grade virtual"
- "Configurar a grelha e concluir a instalação"

- "Automatizando a instalação"
- "Visão geral da API REST de instalação"
- "Onde ir a seguir"
- "Solução de problemas de instalação"
- "Exemplo /etc/network/interfaces"

Visão geral da instalação

Instalar um sistema StorageGRID em um ambiente Ubuntu ou Debian inclui três etapas principais.

1. **Preparação**: Durante o Planejamento e a preparação, você executa as seguintes tarefas:
   - Saiba mais sobre os requisitos de hardware e armazenamento do StorageGRID.
   - Saiba mais sobre os detalhes da rede StorageGRID para que você possa configurar sua rede adequadamente. Para obter mais informações, consulte as diretrizes de rede do StorageGRID.
   - Identifique e prepare os servidores físicos ou virtuais que você planeja usar para hospedar seus nós de grade do StorageGRID.
   - Nos servidores que você preparou:
     - Instale Ubuntu ou Debian
     - Configure a rede host
     - Configurar o armazenamento do host
     - Instale o Docker
     - Instale os serviços de host do StorageGRID
2. **Implantação**: Implante nós de grade usando a interface de usuário apropriada. Quando você implementa nós de grade, eles são criados como parte do sistema StorageGRID e conetados a uma ou mais redes.
   a. Use os arquivos de configuração de nó e linha de comando Ubuntu ou Debian para implantar nós de grade virtual nos hosts que você preparou na etapa 1.
   b. Use o Instalador de dispositivos StorageGRID para implantar nós de dispositivos StorageGRID.

   > As instruções de instalação e integração específicas de hardware não estão incluídas no procedimento de instalação do StorageGRID. Para saber como instalar dispositivos StorageGRID, consulte as instruções de instalação e manutenção do seu aparelho.
3. **Configuração**: Quando todos os nós tiverem sido implantados, use o Gerenciador de Grade para configurar a grade e concluir a instalação.

Estas instruções recomendam uma abordagem padrão para implantar e configurar um sistema StorageGRID em um ambiente Ubuntu ou Debian. Consulte também as informações sobre as seguintes abordagens alternativas:

- Use uma estrutura de orquestração padrão como Ansible, Puppet ou Chef para instalar o Ubuntu ou Debian, configurar rede e armazenamento, instalar o Docker e o serviço de host StorageGRID e implantar nós de grade virtual.
- Automatize a implantação e configuração do sistema StorageGRID usando um script de configuração Python (fornecido no arquivo de instalação).

- Automatize a implantação e a configuração dos nós de grade do dispositivo com um script de configuração Python (disponível no arquivo de instalação ou no instalador do dispositivo StorageGRID).
- Se você é um desenvolvedor avançado de implantações do StorageGRID, use as APIS REST de instalação para automatizar a instalação de nós de grade do StorageGRID.

Informações relacionadas

"Planejamento e preparação"

"Implantando nós de grade virtual"

"Configurar a grelha e concluir a instalação"

"Automatizando a instalação e a configuração do serviço de host StorageGRID"

"Visão geral da API REST de instalação"

"Diretrizes de rede"

Planejamento e preparação

Antes de implantar nós de grade e configurar a grade StorageGRID, você deve estar familiarizado com as etapas e requisitos para concluir o procedimento.

Os procedimentos de implantação e configuração do StorageGRID presumem que você está familiarizado com a arquitetura e o funcionamento do sistema StorageGRID.

Você pode implantar um único local ou vários locais de uma só vez. No entanto, todos os locais precisam atender ao requisito mínimo de ter pelo menos três nós de storage.

Antes de iniciar uma instalação do StorageGRID, você deve:

- Entenda os requisitos de computação do StorageGRID, incluindo os requisitos mínimos de CPU e RAM para cada nó.
- Entenda como o StorageGRID oferece suporte a várias redes para separação de tráfego, segurança e conveniência administrativa e tenha um plano para quais redes você pretende anexar a cada nó do StorageGRID.

  Consulte as diretrizes de rede do StorageGRID.

- Compreender os requisitos de storage e desempenho de cada tipo de nó 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.
- Entenda os requisitos para migração de nós, se você quiser realizar manutenção programada em hosts físicos sem qualquer interrupção do serviço.
- Reúna todas as informações de rede com antecedência. A menos que você esteja usando DHCP, reúna os endereços IP para atribuir a cada nó de grade e os endereços IP dos servidores DNS (Domain Name System) e NTP (Network Time Protocol) que serão usados.
- Instale, conete e configure todo o hardware necessário, incluindo quaisquer dispositivos StorageGRID, de acordo com as especificações.

As instruções de instalação e integração específicas de hardware não estão incluídas no procedimento de instalação do StorageGRID. Para saber como instalar dispositivos StorageGRID, consulte as instruções de instalação e manutenção do seu aparelho.

- Decida qual das ferramentas de implantação e configuração disponíveis você deseja usar.

Informações relacionadas

"Diretrizes de rede"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Requisitos de migração de contêiner de nós"

Materiais necessários

Antes de instalar o StorageGRID, você deve reunir e preparar os materiais necessários.

Item	Notas
Licença NetApp StorageGRID	Você deve ter uma licença NetApp válida e assinada digitalmente. **Nota**: Uma licença de não produção, que pode ser usada para testes e grades de prova de conceito, está incluída no arquivo de instalação do StorageGRID.
Arquivo de instalação do StorageGRID	Você deve baixar o arquivo de instalação do StorageGRID e extrair 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

Informações relacionadas

"Transferir e extrair os ficheiros de instalação do StorageGRID"

"Requisitos do navegador da Web"

"Administrar o StorageGRID"

"Notas de lançamento"

Transferir e extrair os ficheiros de instalação do StorageGRID

Você deve baixar o arquivo de instalação do StorageGRID e extrair os arquivos necessários.

Passos

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

   "NetApp Downloads: 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 aparecer uma instrução Caution/MustRead, leia-a e marque a caixa de seleção.

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

5. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.

   É apresentada a página de transferências para a versão selecionada. A página contém três colunas:

6. Na coluna **Instalar StorageGRID**, selecione o software apropriado.

   Selecione o `.tgz` arquivo ou `.zip` archive para sua plataforma.

   - `StorageGRID-Webscale-version-DEB-uniqueID.zip`
   - `StorageGRID-Webscale-version-DEB-uniqueID.tgz`

     Os arquivos compatados contêm os arquivos DEB e scripts para Ubuntu ou Debian.

   > Use o `.zip` arquivo se você estiver executando o Windows no laptop de serviço.

7. Salve e extraia o arquivo de arquivo.
8. Escolha os arquivos que você precisa na lista a seguir.

   O conjunto de arquivos de que você precisa depende da topologia de grade planejada e de como você implantará sua grade 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.
	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.
	Um arquivo de configuração de exemplo 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.

Informações relacionadas

"Manter recuperar"

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.

Para obter informações sobre servidores suportados, consulte a Matriz de interoperabilidade.

Cada nó do StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Pelo menos 24 GB por nó e 2 a 16 GB menos do que a RAM total do sistema, dependendo do total de RAM disponível e da quantidade de software que não seja StorageGRID executado no sistema

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), considere 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 de administração, monitoramento e atualização do 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 as informações sobre os requisitos de armazenamento.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Requisitos de storage e desempenho"

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

"Atualizar o software"

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 capacidade de migração de nós do StorageGRID, você deve armazenar dados de sistema e dados de objetos em armazenamento compartilhado.

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 AFF

Se o nó StorageGRID usar o storage atribuído a partir de um sistema NetApp AFF, 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 Docker	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.	4.000 GB consulte requisitos de storage para nós de storage para obter mais informações.
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 a 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 de administração. Como regra geral, 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.

Os snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte os procedimentos de recuperação e manutenção 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*
Nó de arquivo	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	4.000 GB
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

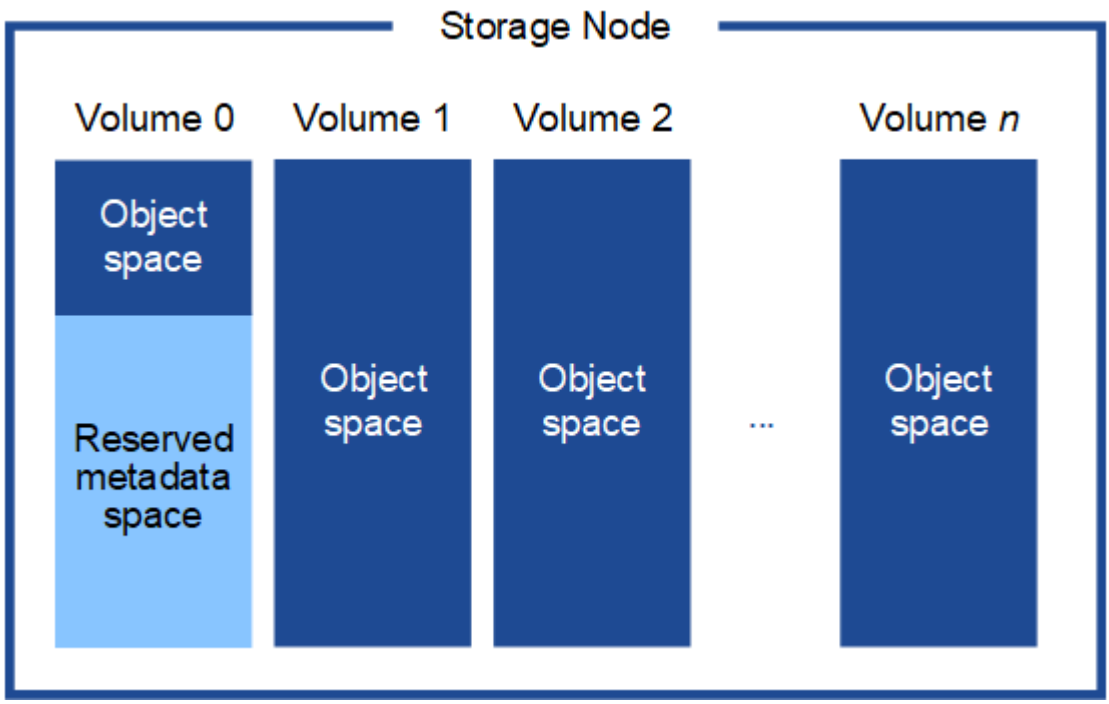
Requisitos de storage para nós de storage

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 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 Storage Read-Only (somente leitura de armazenamento) na inicialização e armazenar somente metadados de objetos.

- Se você estiver instalando um novo sistema StorageGRID 11,5 e cada nó de armazenamento tiver 128 GB ou mais de RAM, deverá atribuir 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 detalhes, vá para as instruções de administração do StorageGRID e procure "armazenamento de metadados de objetos".

"Administrar o StorageGRID"

Informações relacionadas

"Requisitos de migração de contêiner de nós"

"Manter recuperar"

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. Basta mover 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 migração de VM, talvez queira usar essa capacidade em vez do recurso de migração de nós do 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 de recuperação e manutenção para desligar um nó de grade.

Migração do VMware Live não suportada

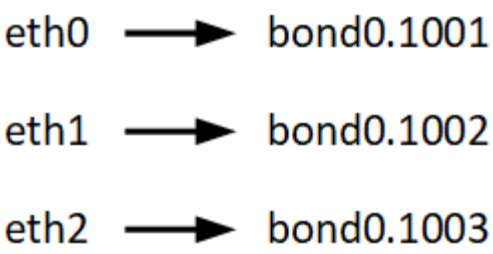
O OpenStack Live Migration e o VMware Live vMotion fazem com que a hora do relógio da máquina virtual salte e não seja compatível com nós de grade de qualquer tipo. Embora raros, tempos de clock incorretos podem resultar em perda de dados ou atualizações de configuração.

A migração fria é suportada. Na migração fria, você desliga os nós do StorageGRID antes de migrá-los entre hosts. Consulte o procedimento para desligar um nó de grade nas instruções de recuperação e manutenção.

Nomes de interface de rede consistentes

Para mover um nó de um host para outro, o serviço de host do 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; consulte ""Configurando a rede de host"" para alguns exemplos.

Armazenamento compartilhado

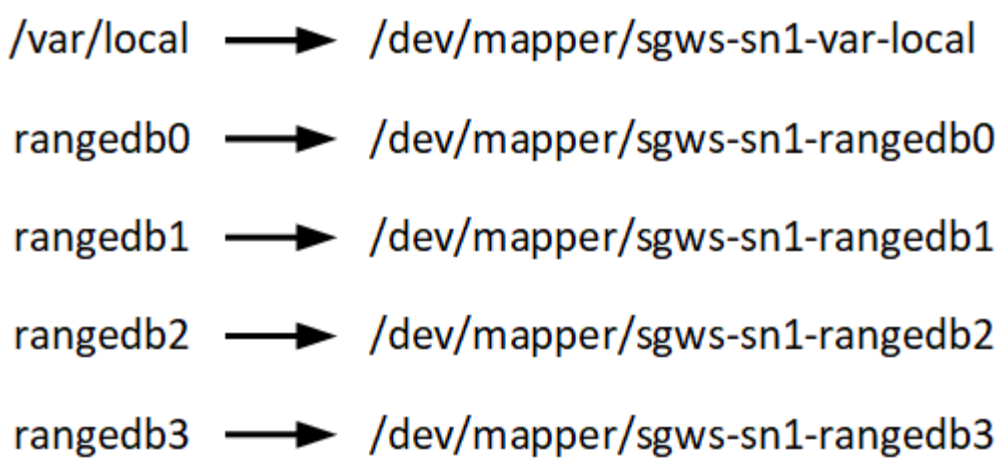
Para conseguir migrações de nós rápidas e de baixa sobrecarga, o recurso de migração de nós do StorageGRID não move fisicamente os dados dos nós. Em vez disso, a migração de nós é realizada como um par de operações de exportação e importação, da seguinte forma:

Passos

1. Durante a operação de exportação de nós, 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 nós, 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.



Informações relacionadas

"Configurando a rede host"

"Manter recuperar"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Ferramentas de implantação

Você pode se beneficiar da automação de toda ou parte da instalação do StorageGRID.

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.

Se você estiver interessado em automatizar toda ou parte da implantação do StorageGRID, revise ""Automatizar a instalação"" antes de iniciar o processo de instalação.

Informações relacionadas

"Automatizando a instalação"

Preparando os anfitriões

Você deve concluir as etapas a seguir para preparar seus hosts físicos ou virtuais para o StorageGRID. Observe que você pode automatizar muitas ou todas essas etapas usando estruturas de configuração de servidor padrão, como Ansible, Puppet ou Chef.

Informações relacionadas

"Automatizando a instalação e a configuração do serviço de host StorageGRID"

Instalando o Linux

Você deve instalar Ubuntu ou Debian em todos os hosts de grade. Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

Passos

1. Instale o Ubuntu ou Debian 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 não selecionadas.

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.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Entendendo 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".

  Depois de desativar o AppArmor, nenhuma entrada indicando que o AppArmor está habilitado aparecerá nos arquivos de log do StorageGRID.

Configurando a rede host

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.

O que você vai precisar

- Você revisou as diretrizes de rede do StorageGRID.

  "Diretrizes de rede"

- Você analisou as informações sobre os requisitos de migração de contêineres do nó.

  "Requisitos de migração de contêiner de nós"

- Se você estiver usando hosts virtuais, leia as considerações e recomendações sobre a clonagem de endereços MAC antes de configurar a rede host.

  "Considerações e recomendações para clonagem de endereços MAC"

> 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 são máquinas virtuais e você está implantando um ou dois nós de StorageGRID para cada host, você pode simplesmente 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 Docker 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. Fazer com que o

contentor Docker use o endereço MAC da NIC dedicada no host permite evitar o uso de configurações de rede de modo promíscuo.

> 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 Docker 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 as instruções para criar arquivos de configuração de nós.

"Criando arquivos de configuração de nó"

Exemplo de clonagem DE MAC

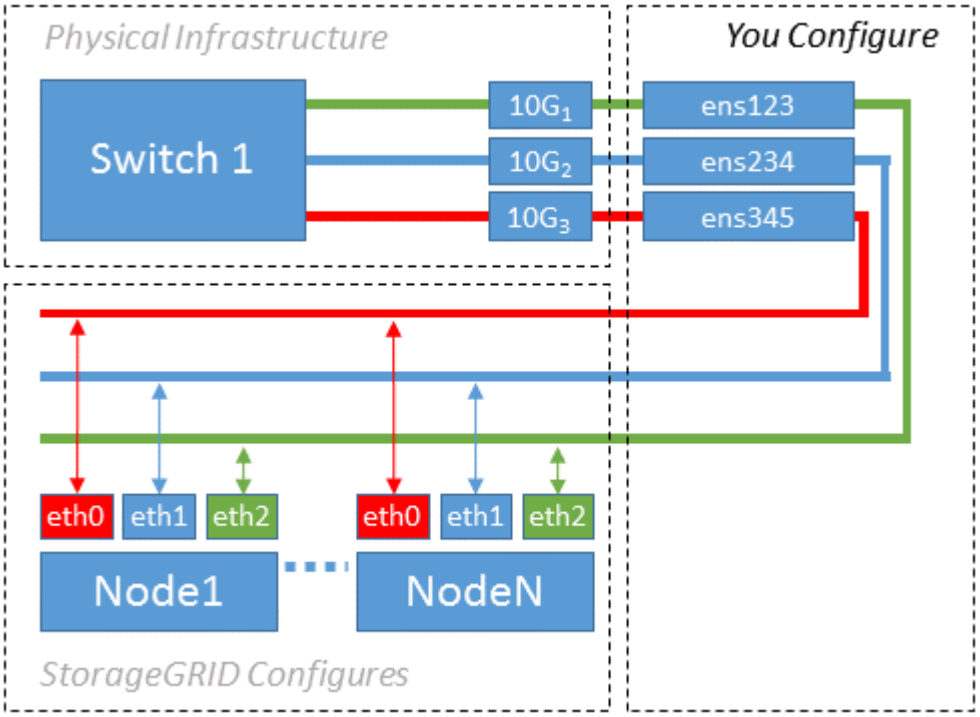
Exemplo de clonagem MAC ativada com um host com endereço MAC de 11:22:33:44:55:66 para a interface ens256 e as seguintes chaves no arquivo de configuração do nó:

- `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

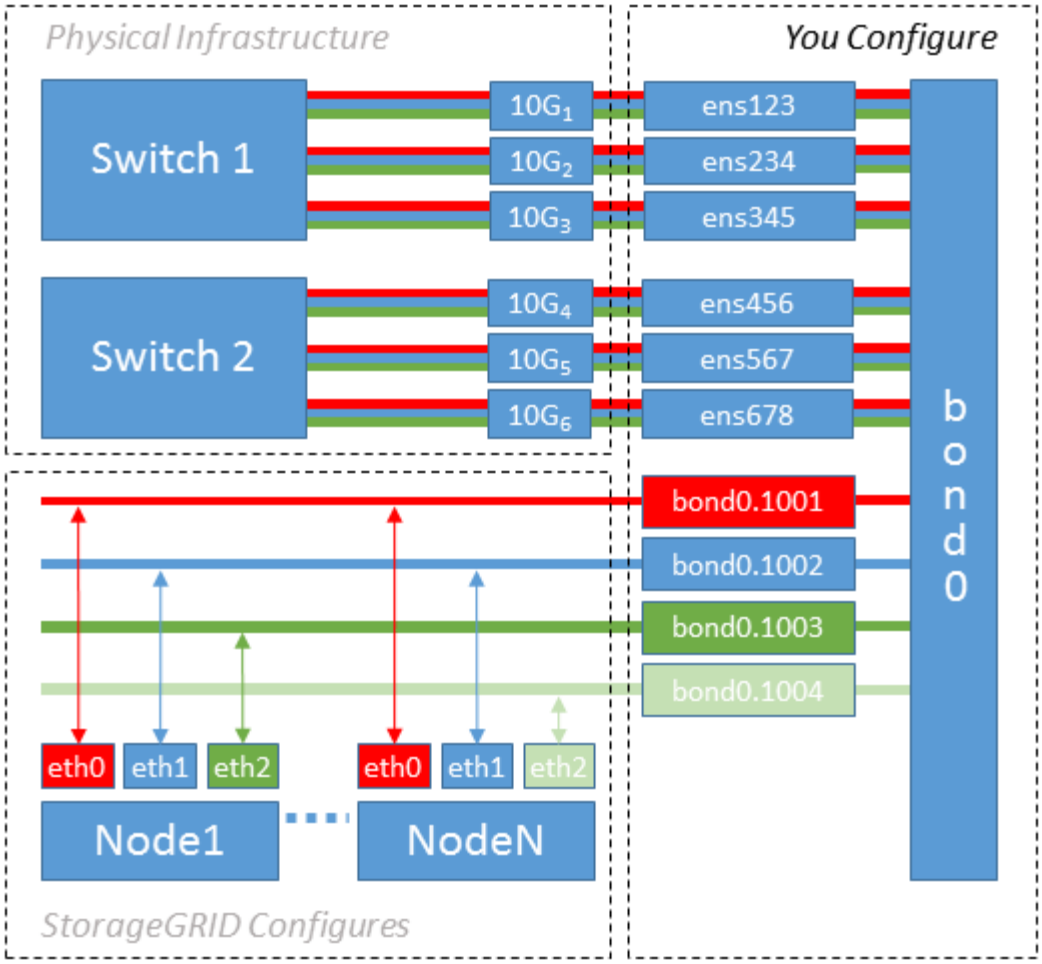
O exemplo 2 assume que você está familiarizado com a ligação de interfaces de rede e com a criação de interfaces VLAN na distribuição Linux que você está usando.

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," `using the standard VLAN interface naming convention `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/network/interfaces"

Configuração do storage de host

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

O que você vai precisar

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 volumes de armazenamento de bloco (LUNs) 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.

Evite usar arquivos de dispositivo especiais "'RAW'" (`/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 LUNs iSCSI e multipathing de mapeamento de dispositivos, considere usar aliases 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
     }
     …
```

Isso fará com que os aliases apareçam como dispositivos de bloco `/dev/mapper` no diretório no 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 oferecer suporte à migração de nós do StorageGRID e usando multipathing de mapeamento de dispositivos, você poderá criar e instalar um comum `/etc/multipath.conf` em todos os hosts colocalizados. 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.

Informações relacionadas

"Requisitos de storage e desempenho"

"Requisitos de migração de contêiner de nós"

Configurando o volume de armazenamento do Docker

Antes de instalar o Docker, talvez seja necessário formatar o volume de armazenamento do Docker e montá-lo `/var/lib/docker` no .

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.

Instalando 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.

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 1.10.3 ou posterior.

```
Client:
  Version:      1.10.3
  API version:  1.22
  Go version:   go1.6.1
  Git commit:   20f81dd
  Built:        Wed, 20 Apr 2016 14:19:16 -0700
  OS/Arch:      linux/amd64

Server:
  Version:      1.10.3
  API version:  1.22
  Go version:   go1.6.1
  Git commit:   20f81dd
  Built:        Wed, 20 Apr 2016 14:19:16 -0700
  OS/Arch:      linux/amd64
```

Informações relacionadas

"Configuração do storage de host"

Instalação dos 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.

Implantando nós de grade virtual

Ao implantar nós de grade em um ambiente Ubuntu ou Debian, você cria arquivos de configuração de nós para todos os nós, valida os arquivos e inicia o serviço de host StorageGRID, que inicia os nós. Se você precisar implantar qualquer nó de storage do dispositivo StorageGRID, consulte as instruções de instalação e manutenção do dispositivo depois de implantar todos os nós virtuais.

- "Criando arquivos de configuração de nó"
- "Validar a configuração do StorageGRID"
- "Iniciando o serviço de host do StorageGRID"

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

"SG5600 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG6000 dispositivos de armazenamento"

Criando arquivos de configuração de nó

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.

Onde coloco os arquivos de configuração do nó?

Você deve colocar 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.

O que nomeo os arquivos de configuração do 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>-<node type>-<node number>.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.

O que está em um arquivo de configuração de nó?

Os arquivos de configuração contêm pares chave/valor, com uma chave e um valor por linha. Para cada par chave/valor, você deve seguir 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.

Algumas chaves são necessárias para cada nó, enquanto outras são opcionais ou apenas necessárias para

determinados tipos de nó.

A tabela define os valores aceitáveis para todas as chaves suportadas. Na coluna do meio:

R: Necessário e BP: Melhor prática e o: Opcional

Chave	R, BP OU O?	Valor
ADMIN_IP	BP	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. Veja como os nós de grade descobrem o nó de administrador principal." **Nota**: Este valor é ignorado, e pode ser proibido, no nó Admin principal.
ADMIN_NETWORK_CONFIG	O	DHCP, ESTÁTICO OU DESATIVADO
ADMIN_NETWORK_ESL	O	Lista de sub-redes separadas por vírgulas na notação CIDR à qual esse nó deve se comunicar através do gateway Admin Network. Exemplo: 172.16.0.0/21,172.17.0.0/21

Chave	R, BP OU O?	Valor
ADMIN_NETWORK_GATEWAY	O (**R**)	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. **Nota**: Este parâmetro é necessário se ADMIN_NETWORK_ESL for especificado. Exemplos: • 1.1.1.1 • 10.224.4.81
ADMIN_NETWORK_IP	O	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
ADMIN_NETWORK_MAC	O	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

Chave	R, BP OU O?	Valor
ADMIN_NETWORK_MASK	O	IPv4 máscara de rede para este nó, na rede Admin. Esta chave só é necessária quando ADMIN_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores. Exemplos: • 255.255.255.0 • 255.255.248.0
ADMIN_NETWORK_MTU	O	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

Chave	R, BP OU O?	Valor
ADMIN_NETWORK_TARGET	BP	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
ADMIN_NETWORK_TARGET_TYPE	O	Interface (Este é o único valor suportado.)

Chave	R, BP OU O?	Valor
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	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, consulte as considerações e recomendações para clonagem de endereços MAC. "Considerações e recomendações para clonagem de endereços MAC"
ADMIN_ROLE	**R**	Primário ou não primário Esta chave só é necessária quando NODE_TYPE: VM_Admin_Node; não a especifique para outros tipos de nó.

Chave	R, BP OU O?	Valor
BLOCK_DEVICE_AUDIT_LOGS	**R**	Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento persistente de logs de auditoria. 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-audit-logs`

Chave	R, BP OU O?	Valor
BLOCK_DEVICE_RANGEDB_00 BLOCK_DEVICE_RANGEDB_01 BLOCK_DEVICE_RANGEDB_02 BLOCK_DEVICE_RANGEDB_03 BLOCK_DEVICE_RANGEDB_04 BLOCK_DEVICE_RANGEDB_05 BLOCK_DEVICE_RANGEDB_06 BLOCK_DEVICE_RANGEDB_07 BLOCK_DEVICE_RANGEDB_08 BLOCK_DEVICE_RANGEDB_09 BLOCK_DEVICE_RANGEDB_10 BLOCK_DEVICE_RANGEDB_11 BLOCK_DEVICE_RANGEDB_12 BLOCK_DEVICE_RANGEDB_13 BLOCK_DEVICE_RANGEDB_14 BLOCK_DEVICE_RANGEDB_15	**R**	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 NÓ_TIPO: VM_Storage_Node; não a especifique para outros tipos de nó. Somente block_DEVICE_RANGEDB_00 é necessário; o resto é opcional. O dispositivo de bloco especificado para block_DEVICE_RANGEDB_00 deve ter pelo menos 4 TB; os outros podem ser menores. **Nota**: Não deixe lacunas. Se você especificar block_DEVICE_RANGEDB_05, você também deve especificar BLOCK_DEVICE_RANGEDB_04. 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-0`

Chave	R, BP OU O?	Valor
BLOCK_DEVICE_TABLES	**R**	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`
BLOCK_DEVICE_VAR_LOCAL	**R**	Caminho e nome do arquivo especial do dispositivo de bloco este nó usará para seu armazenamento persistente /var/local. 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`
CLIENT_NETWORK_CONFIG	O	DHCP, ESTÁTICO OU DESATIVADO

Chave	R, BP OU O?	Valor
CLIENT_NETWORK_GATEWAY	O	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
CLIENT_NETWORK_IP	O	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
CLIENT_NETWORK_MAC	O	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
CLIENT_NETWORK_MASK	O	IPv4 máscara de rede para este nó na rede do cliente. Esta chave só é necessária quando CLIENT_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores. Exemplos: • 255.255.255.0 • 255.255.248.0

Chave	R, BP OU O?	Valor
CLIENT_NETWORK_MTU	O	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

Chave	R, BP OU O?	Valor
CLIENT_NETWORK_TARGET	BP	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
CLIENT_NETWORK_TARGET_TYPE	O	Interface (Este é apenas o valor suportado.)

Chave	R, BP OU O?	Valor
CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	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, consulte as considerações e recomendações para clonagem de endereços MAC. "Considerações e recomendações para clonagem de endereços MAC"
GRID_NETWORK_CONFIG	BP	ESTÁTICO ou DHCP (O padrão é ESTÁTICO se não for especificado.)
GRID_NETWORK_GATEWAY	**R**	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.

Chave	R, BP OU O?	Valor
GRID_NETWORK_IP	**R**	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
GRID_NETWORK_MAC	O	O endereço MAC da interface Grid Network 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:C2:27:30
GRID_NETWORK_MASK	O	IPv4 máscara de rede para este nó na rede de Grade. Esta chave só é necessária quando GRID_NETWORK_CONFIG é ESTÁTICA; não a especifique para outros valores. Exemplos: • 255.255.255.0 • 255.255.248.0

Chave	R, BP OU O?	Valor
GRID_NETWORK_MTU	O	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

Chave	R, BP OU O?	Valor
GRID_NETWORK_TARGET	**R**	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
GRID_NETWORK_TARGET_TYPE	O	Interface (Este é o único valor suportado.)
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	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, consulte as considerações e recomendações para clonagem de endereços MAC. "Considerações e recomendações para clonagem de endereços MAC"

Chave	R, BP OU O?	Valor
MÁXIMO_RAM	O	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 as instruções para administrar o StorageGRID para obter uma descrição do que é o espaço reservado de metadados. O formato deste campo é `<number><unit>`, onde `<unit>` pode ser `b`, `k`, , `m` `g` ou . Exemplos: 13 24 g 38654705664b **Nota**: Se você quiser usar essa opção, você deve habilitar o suporte do kernel para cgroups de memória.
NODE_TYPE (TIPO DE NÓ)	**R**	Tipo de nó: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway

Chave	R, BP OU O?	Valor
PORT_REMAP	O	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 de nó de grade"" ou ""Comunicações externas"". **IMPORTANTE**: Não remapear 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 o tipo de rede é grade, admin ou cliente e o protocolo é tcp ou udp. Por exemplo: `PORT_REMAP = client/tcp/18082/443`

Chave	R, BP OU O?	Valor
PORT_REMAP_INBOUND	O	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 remapear 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 o tipo de rede é grade, admin ou cliente e o protocolo é tcp ou udp. Por exemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Informações relacionadas

"Como os nós de grade descobrem o nó de administração principal"

"Diretrizes de rede"

"Administrar o StorageGRID"

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 de 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
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 nó de arquivo

- Exemplo de nome do arquivo:* `/etc/storagegrid/nodes/dc1-arc1.conf`
- Exemplo de conteúdo do arquivo:*

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
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
```

Validar 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.

```
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
```

Iniciando 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
```

Para qualquer nó que retorna um status de "'Not Running'" ou "'stopped'", execute o seguinte comando:

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

3. Se você já ativou e iniciou o serviço de host StorageGRID (ou se não tiver certeza se o serviço foi ativado e iniciado), execute também o seguinte comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configurar a grelha e concluir a instalação

Você conclui a instalação configurando o sistema StorageGRID a partir do Gerenciador de Grade no nó Admin principal.

- "Navegando para o Gerenciador de Grade"
- "Especificando as informações da licença do StorageGRID"
- "Adicionar sites"
- "Especificando sub-redes de rede de Grade"
- "Aprovando nós de grade pendentes"
- "Especificando informações do servidor Network Time Protocol"
- "Especificando informações do servidor do sistema de nomes de domínio"
- "Especificando as senhas do sistema StorageGRID"
- "Rever a sua configuração e concluir a instalação"
- "Diretrizes de pós-instalação"

Navegando para o Gerenciador de Grade

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

O que você vai precisar

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 um dos seguintes endereços:

```
https://primary_admin_node_ip

client_network_ip
```

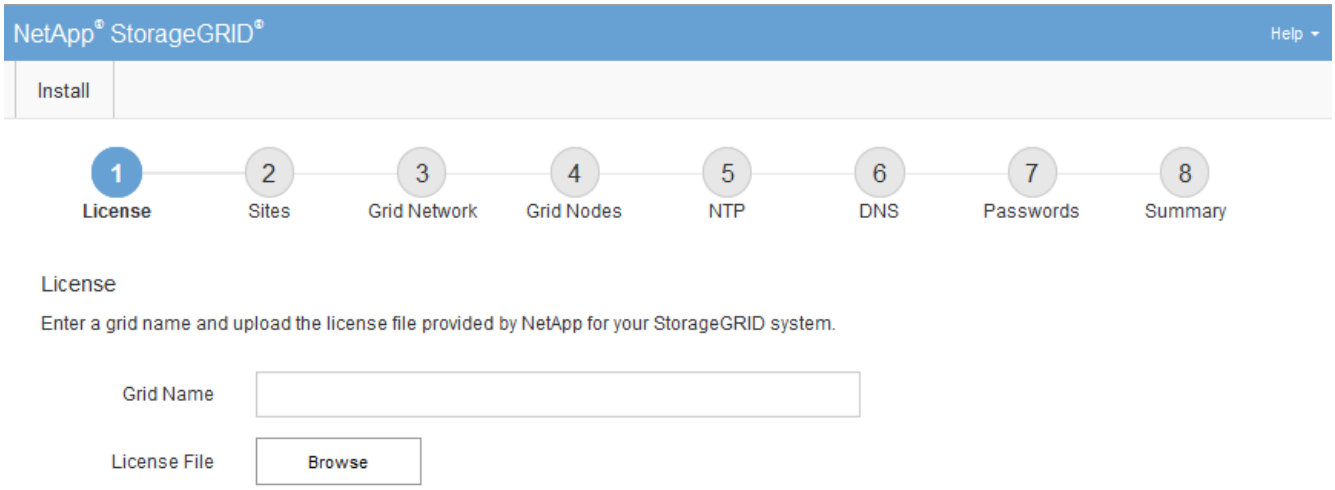
Como alternativa, você pode acessar o Gerenciador de Grade na porta 8443:

```
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.

1. Clique em **Instalar um sistema StorageGRID**.

   A página usada para configurar uma grade StorageGRID é exibida.



Especificando 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

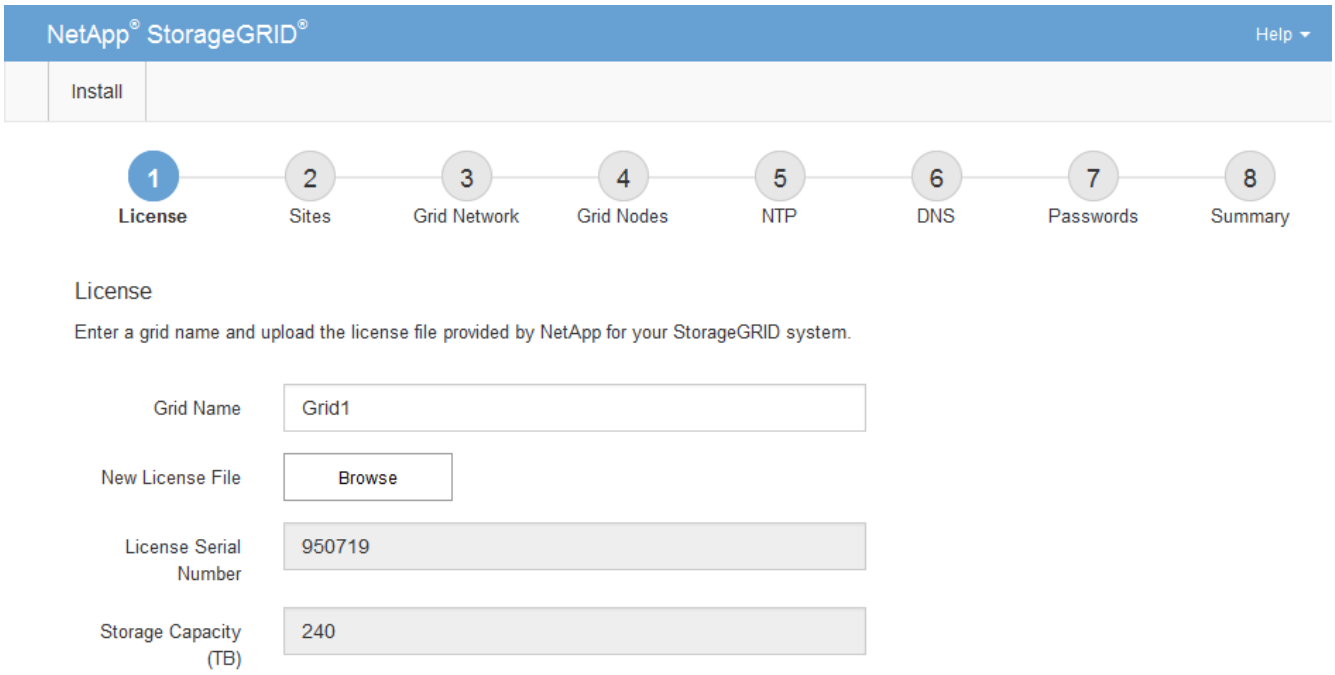
1. Na página Licença, insira um nome significativo para o seu sistema StorageGRID em **Nome da Grade**.

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

2. Clique em **Procurar**, localize o ficheiro de licença do NetApp (`NLFunique_id.txt`) e clique em **abrir**.

   O arquivo de licença é validado e o número de série e a capacidade de armazenamento licenciada são exibidos.

> 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.



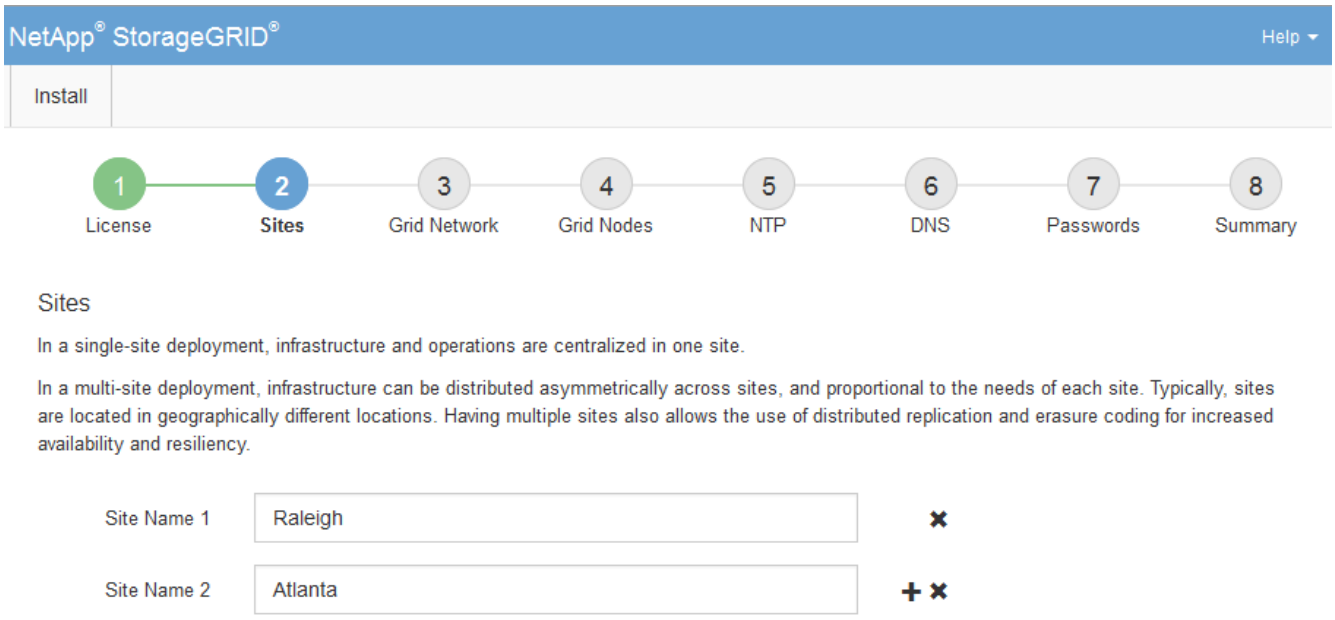
3. Clique em **seguinte**.

Adicionar 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.

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**.

Especificando sub-redes de rede de Grade

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

Sobre esta tarefa

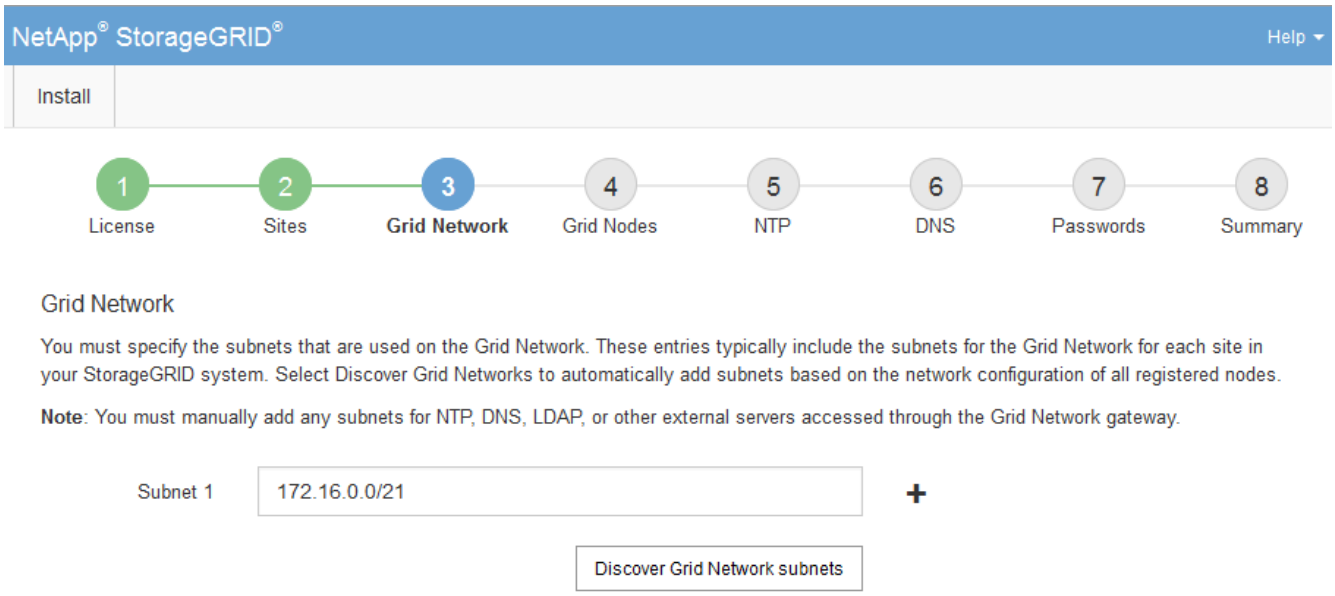
As entradas de sub-rede incluem as sub-redes para a rede de Grade para cada site no seu sistema StorageGRID, juntamente com quaisquer sub-redes que precisam ser acessíveis através da rede de Grade.

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.

   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.



3. Clique em **seguinte**.

Aprovando nós de grade pendentes

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

O que você vai precisar

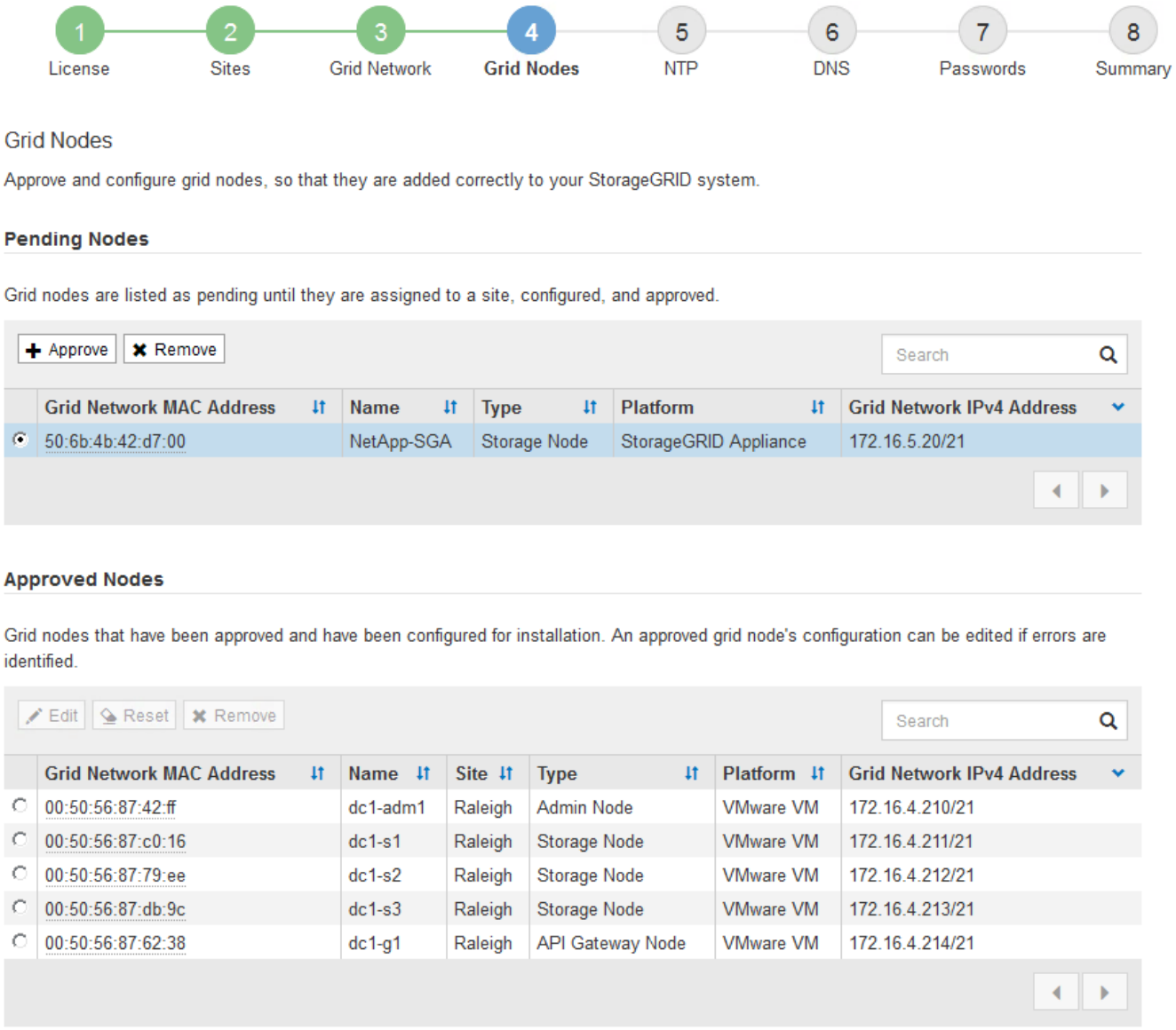
Todos os nós de grade de dispositivos virtuais e StorageGRID devem ter sido implantados.

Passos

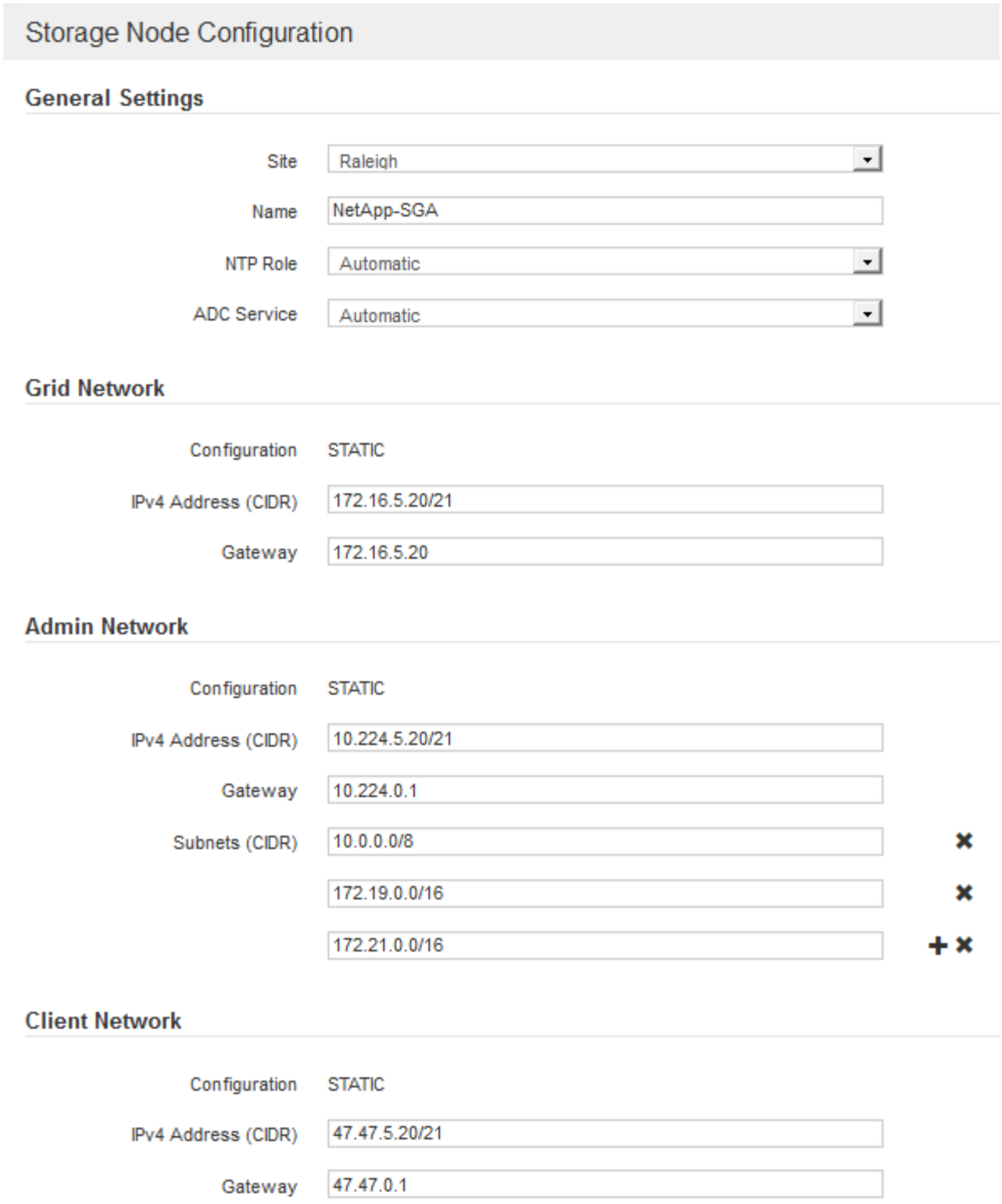
1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade implantados.

   Se um nó de grade estiver ausente, confirme que ele foi implantado com sucesso.

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 site com o qual este nó de grade será associado.
- **Nome**: O nome que será atribuído ao nó e o nome que será exibido no Gerenciador de Grade. O nome padrão é o nome que você especificou quando configurou o nó. Durante esta etapa do processo de instalação, você pode alterar o nome conforme necessário.

> Depois de concluir a instalação, não é possível alterar o nome do nó.

> 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.

- **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. Você não pode 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 garantir que o endereço IP resultante não esteja 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 garantir que o endereço IP resultante não esteja 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 **Configurar rede Configuração de ligação** 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, redefina 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.

   Para obter informações adicionais, consulte as instruções de instalação e manutenção 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 garantir que o endereço IP resultante não esteja 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 **Configurar rede Configuração de ligação** 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, redefina o nó.

   f. Remova o nó da tabela nós pendentes.

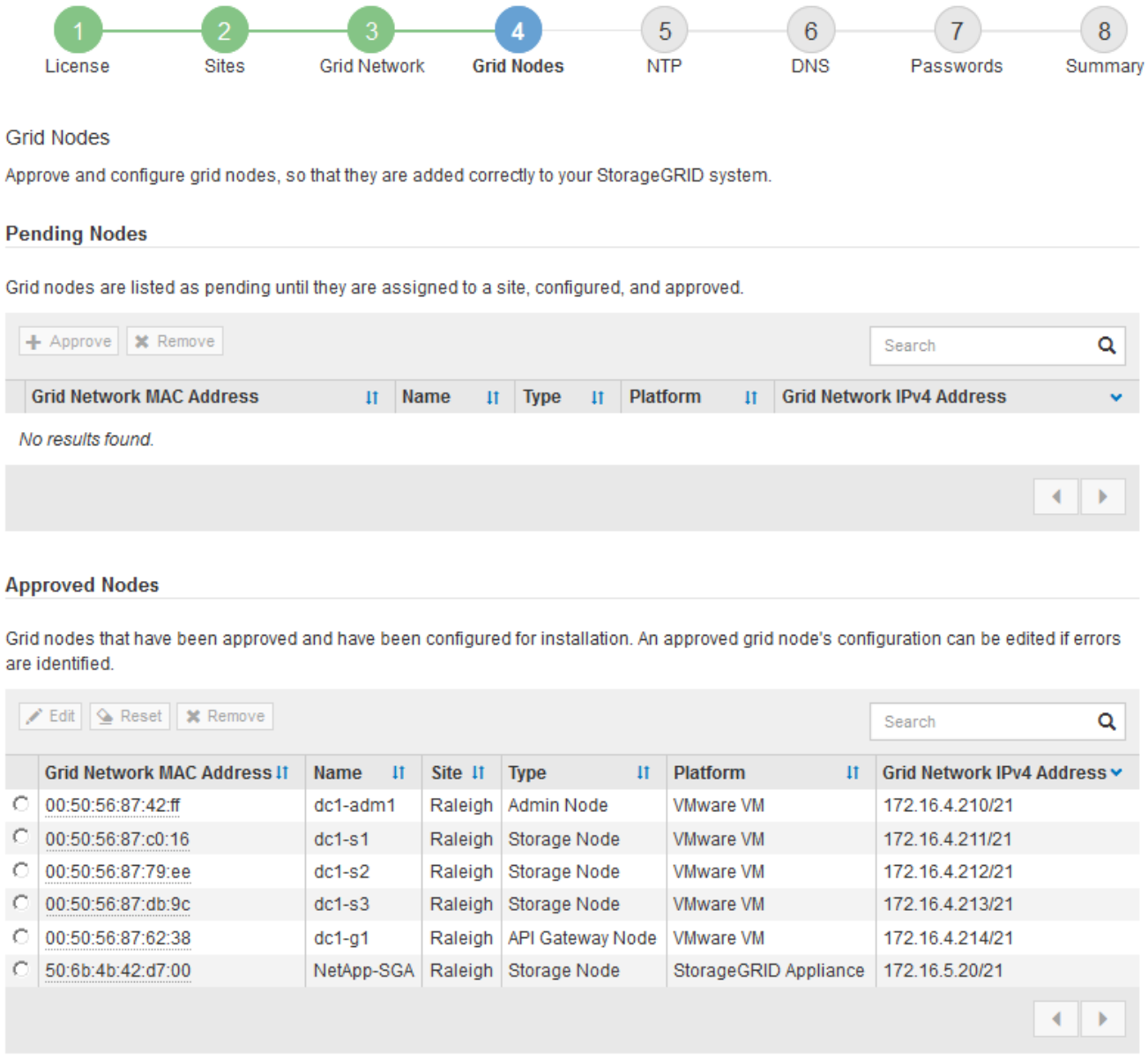
   g. Aguarde que o nó reapareça na lista de nós pendentes.

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

      Para obter informações adicionais, consulte as instruções de instalação e manutenção 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**.

Especificando 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.

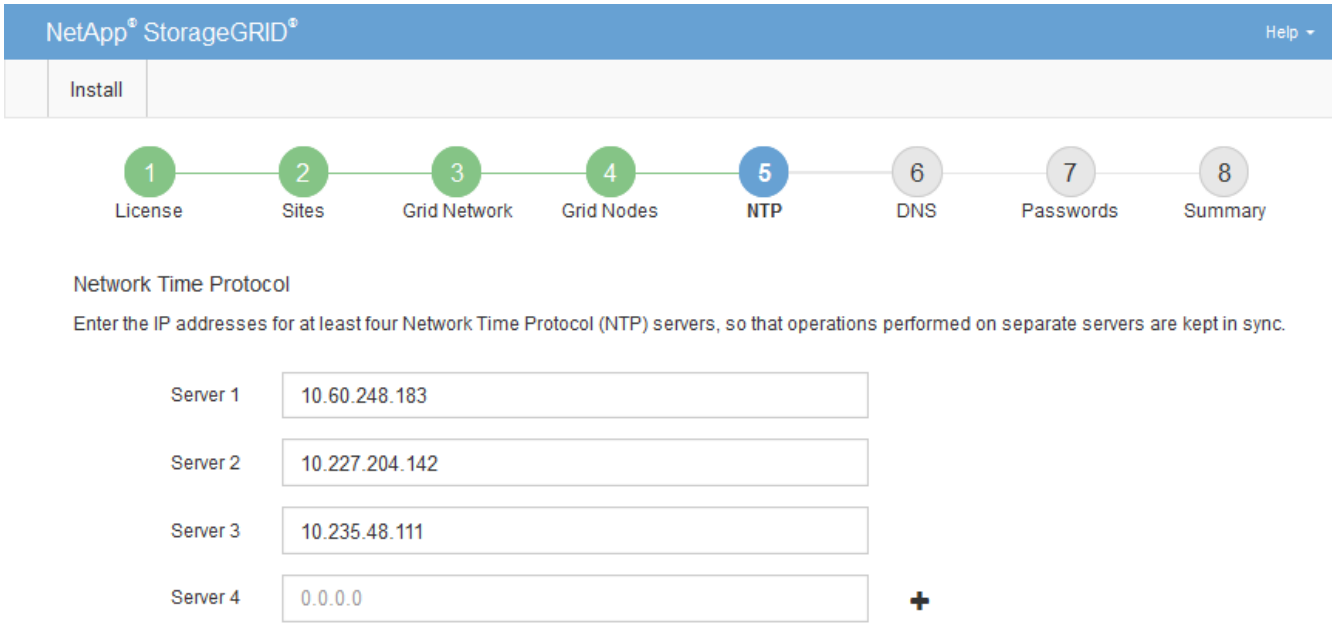
> Ao especificar a fonte NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft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

Especificando informações do servidor do sistema de nomes de domínio

Você deve especificar informações do sistema de nomes de domínio (DNS) para o seu sistema StorageGRID, para que você possa acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

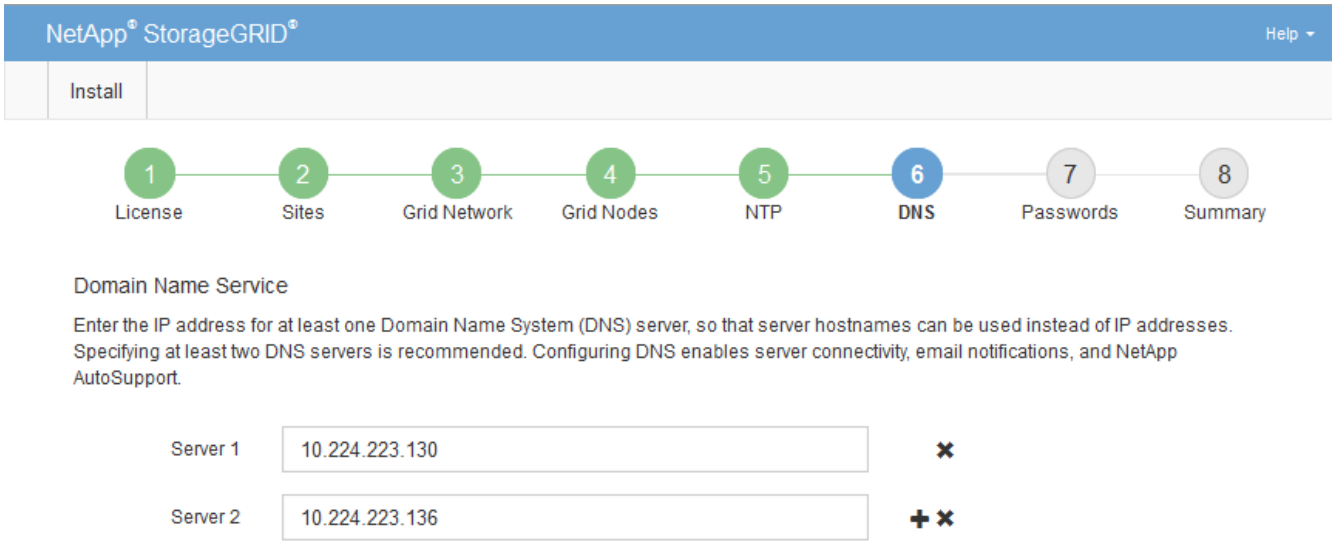
Especificar informações do servidor DNS permite que você use nomes de host de nome de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações de e-mail e AutoSupport. É recomendável especificar pelo menos dois servidores DNS.

> Forneça dois a seis endereços IPv4 para servidores DNS. Você deve selecionar servidores DNS que cada site pode acessar localmente no caso de rede ser aterrissada. Isso é para garantir que um site islanded continua a ter acesso ao serviço DNS. Depois de configurar a lista de servidores DNS em toda a grade, você pode personalizar ainda mais a lista de servidores DNS para cada nó. Para obter detalhes, consulte as informações sobre como modificar a configuração DNS nas instruções de recuperação e manutenção.

Se as informações do servidor DNS forem omitidas ou configuradas incorretamente, um alarme DNST será acionado no serviço SSM de cada nó da grade. O alarme é apagado quando o DNS está configurado corretamente e as novas informações do servidor atingiram todos os nós da grade.

Passos

1. 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**.

Especificando 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 arquivo Passwords.txt 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.

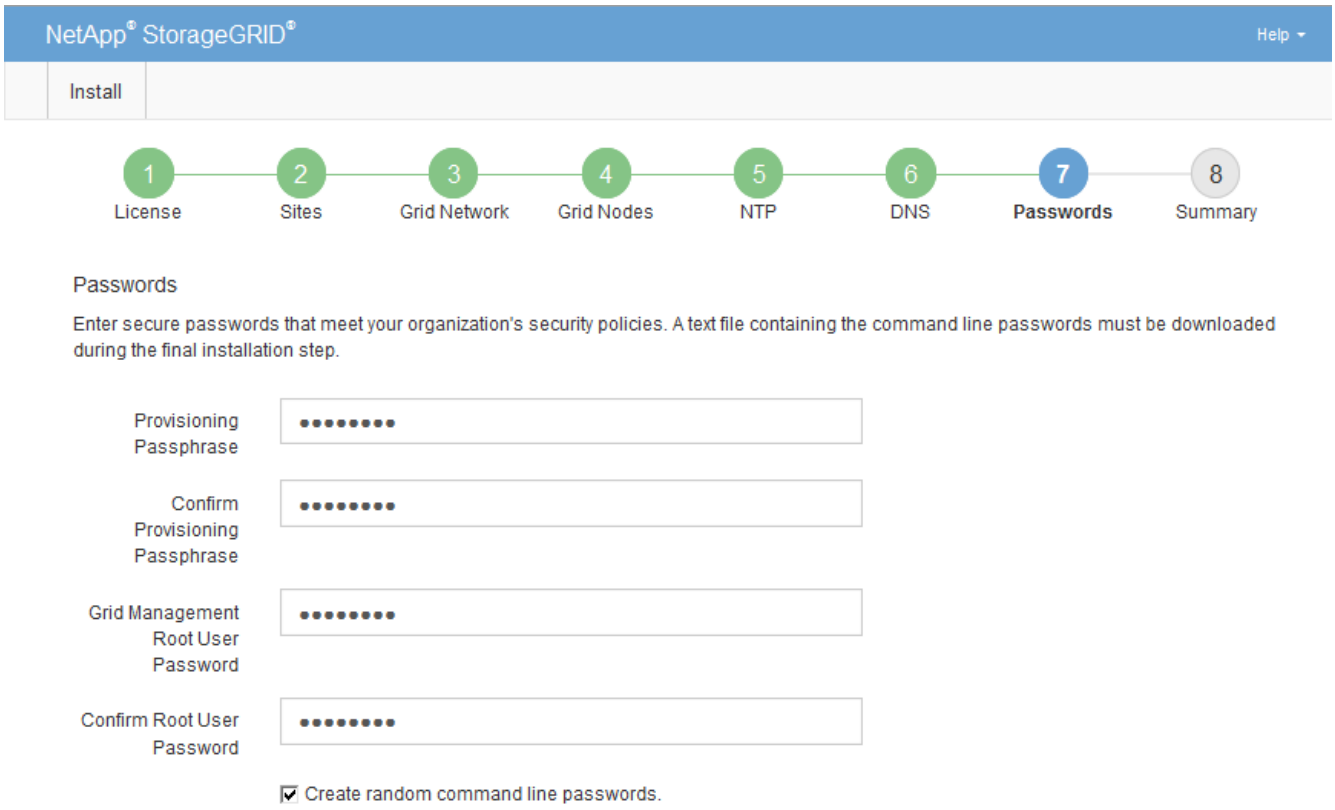
   Armazene a senha de provisionamento em um local seguro.

   > Se após a conclusão da instalação e você quiser alterar a senha de provisionamento mais tarde, você pode usar o Gerenciador de Grade. Selecione **Configuração Controle de Acesso senhas de Grade**.

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 opcionalmente 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. Desmarque **criar senhas de linha de comando aleatórias** apenas para grades de demonstração se você quiser usar senhas padrão para acessar os 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. Tem de transferir este ficheiro para concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas no arquivo Passwords.txt, contido no arquivo Pacote de recuperação.

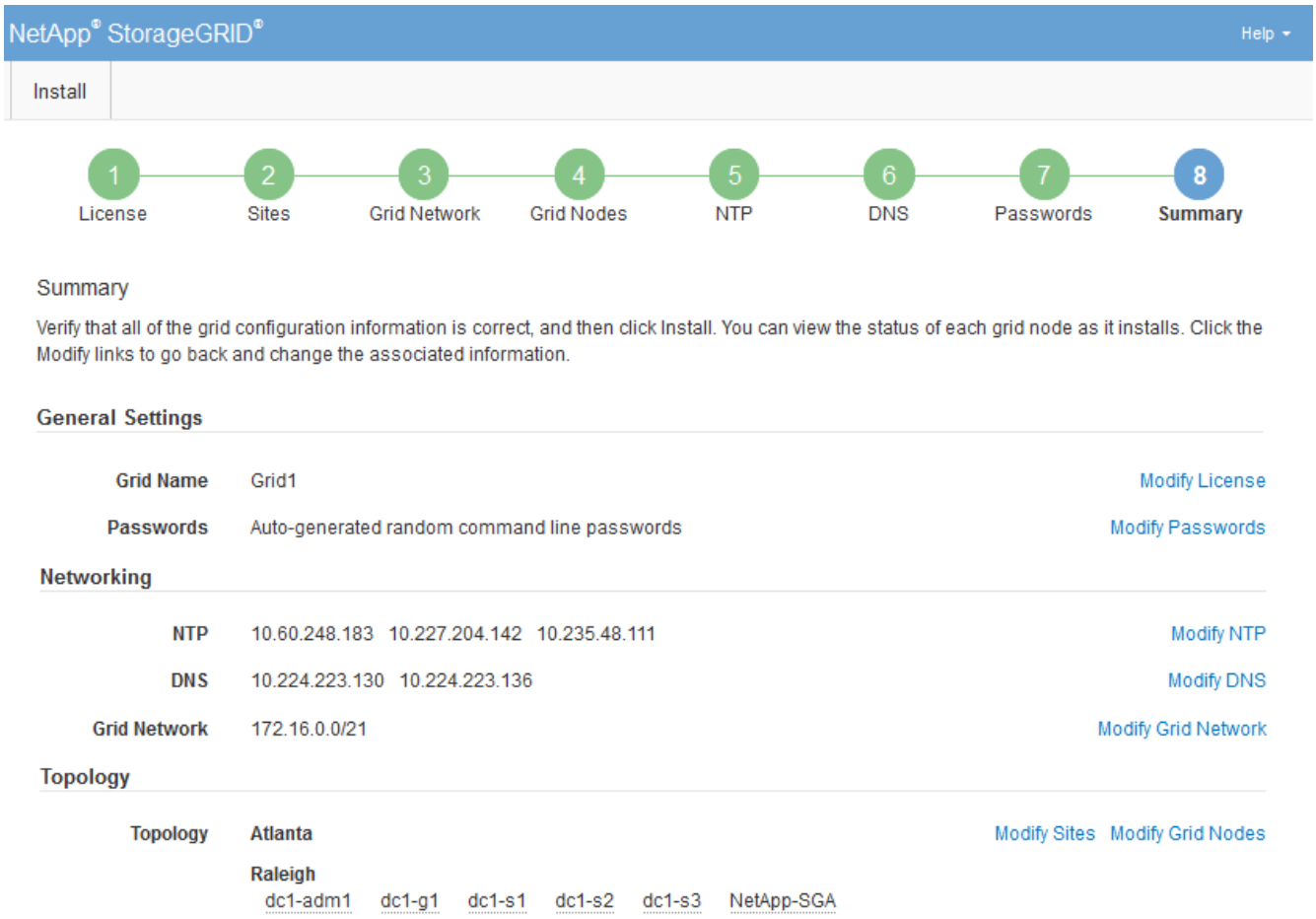
6. Clique em **seguinte**.

Rever a sua configuração e concluir 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.

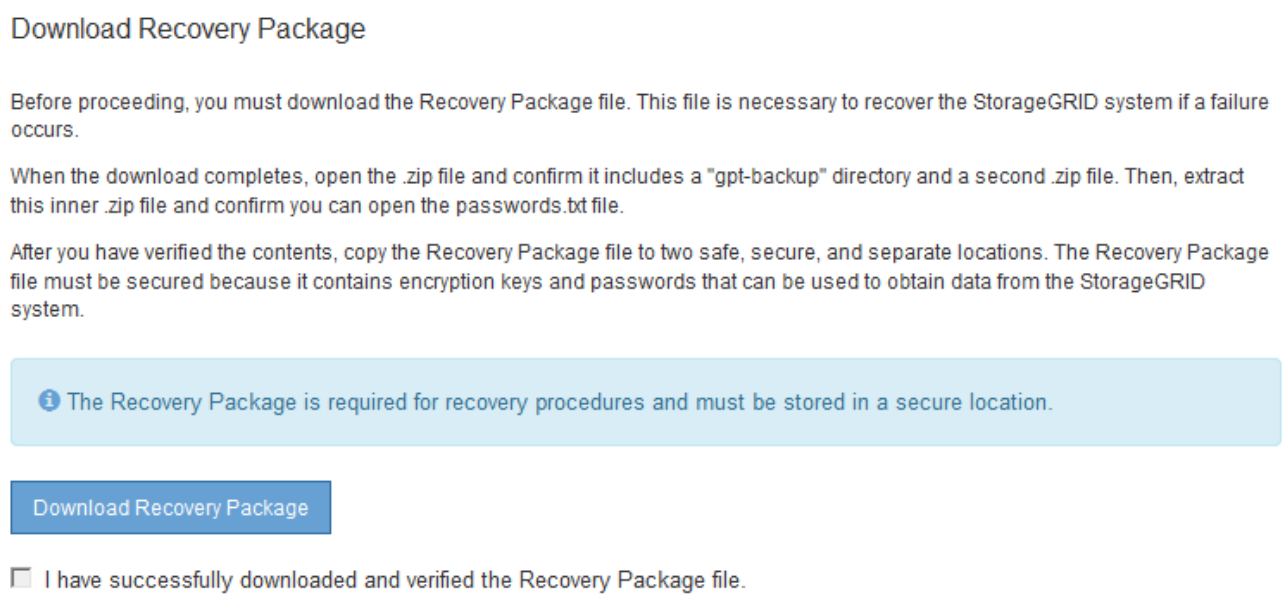
4. Clique em **Download Recovery Package**.

   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 não é possível concluir a instalação e aceder ao sistema StorageGRID até transferir e verificar este ficheiro.

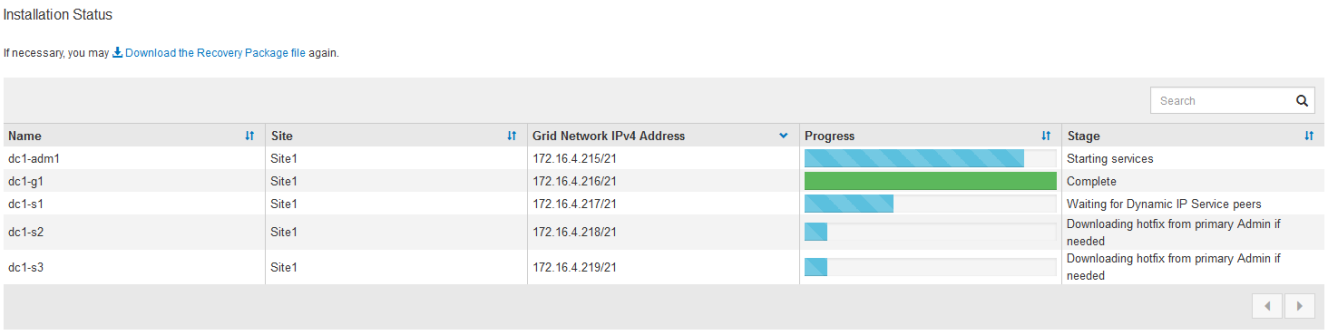
5. Verifique se você pode extrair o conteúdo do `.zip` arquivo e salvá-lo em dois locais seguros, seguros e separados.

> 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 seus endereços IP são alterados, o que pode causar interrupções se uma alteração de endereço 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. Consulte as informações sobre como configurar endereços IP nas instruções de recuperação e manutenção.
- 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.

Automatizando a instalação

É possível 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.

Automatizando 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 e manual do Ansible são fornecidos com o arquivo de instalação na pasta /extras. 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.

Automatizando a configuração do StorageGRID

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

O que você vai precisar

- 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 amostra (`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, você precisa extrair o `Passwords.txt` arquivo e procurar 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

"Configurar a grelha e concluir a instalação"

"Visão geral da API REST de instalação"

Visão geral da 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 (JavaScript Object Notation).

> Todas as operações de API que você executa usando a página da Web do API Docs 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 seu sistema StorageGRID e, caso precise 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.

Informações relacionadas

"Automatizando a instalação"

Onde ir a seguir

Depois de concluir uma instalação, você deve executar uma série de etapas de integração e configuração. Alguns passos são necessários; outros são opcionais.

Tarefas necessárias

- Crie uma conta de locatário para cada protocolo de cliente (Swift ou S3) que será usado para armazenar objetos em seu sistema StorageGRID.
- Controle o acesso ao sistema configurando grupos e contas de usuário. Opcionalmente, você pode

configurar uma fonte de identidade federada (como ative Directory ou OpenLDAP), para que você possa importar grupos de administração e usuários. Ou, você pode criar grupos e usuários locais.

- Integre e teste os aplicativos cliente API S3 ou Swift que você usará para fazer upload de objetos para seu sistema StorageGRID.
- Quando estiver pronto, configure as regras de gerenciamento do ciclo de vida das informações (ILM) e a política de ILM que você deseja usar para proteger os dados do objeto.

> Quando você instala o StorageGRID, a política ILM padrão, Diretiva de cópias de linha de base 2, está ativa. Esta política inclui a regra ILM (fazer 2 cópias) e aplica-se se nenhuma outra política tiver sido ativada.

- Se a instalação incluir nós de storage do dispositivo, use o software SANtricity para concluir as seguintes tarefas:
  - Ligue a cada dispositivo StorageGRID.
  - Verifique a receção dos dados do AutoSupport.
- Se o seu sistema StorageGRID incluir quaisquer nós de arquivamento, configure a conexão do nó de arquivamento ao sistema de storage de arquivamento externo de destino.

> Se algum nó de arquivamento usar o Tivoli Storage Manager como o sistema de armazenamento de arquivamento externo, você também deve configurar o Tivoli Storage Manager.

- Revise e siga as diretrizes de fortalecimento do sistema StorageGRID para eliminar os riscos de segurança.
- Configurar notificações por e-mail para alertas do sistema.

Tarefas opcionais

- Se você quiser receber notificações do sistema de alarme (legado), configure listas de e-mail e notificações por e-mail para alarmes.
- Atualize os endereços IP do nó da grade se eles tiverem sido alterados desde que você planejou sua implantação e gerou o Pacote de recuperação. Consulte as informações sobre como alterar endereços IP nas instruções de recuperação e manutenção.
- Configure a criptografia de armazenamento, se necessário.
- Configure a compactação de armazenamento para reduzir o tamanho dos objetos armazenados, se necessário.
- Configurar acesso de cliente de auditoria. Você pode configurar o acesso ao sistema para fins de auditoria por meio de um compartilhamento de arquivos NFS ou CIFS. Consulte as instruções para administrar o StorageGRID.

> A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

Solução de 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, consulte as instruções para monitoramento e solução de problemas do StorageGRID. Para obter ajuda para solucionar problemas de instalação do aparelho, consulte as instruções de instalação e manutenção dos seus aparelhos. Se precisar de ajuda adicional, entre em Contato com o suporte técnico.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Suporte à NetApp"

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 VMware

Saiba como instalar o StorageGRID em implantações VMware.

- "Visão geral da instalação"
- "Planejamento e preparação"
- "Implantação de nós de grade de máquina virtual no VMware vSphere Web Client"
- "Configurar a grelha e concluir a instalação"
- "Automatizando a instalação"
- "Visão geral da API REST de instalação"
- "Onde ir a seguir"
- "Solução de problemas de instalação"

Visão geral da instalação

A instalação de um sistema StorageGRID em um ambiente VMware inclui três etapas principais.

1. **Preparação**: Durante o Planejamento e a preparação, você executa as seguintes tarefas:
   - Saiba mais sobre os requisitos de hardware, software, máquina virtual, armazenamento e desempenho do StorageGRID.
   - Saiba mais sobre os detalhes da rede StorageGRID para que você possa configurar sua rede adequadamente. Para obter mais informações, consulte as diretrizes de rede do StorageGRID.
   - Identifique e prepare os servidores físicos que você planeja usar para hospedar seus nós de grade do StorageGRID.
   - Nos servidores que você preparou:
     - Instale o VMware vSphere Hypervisor

    - Configure os hosts ESX
    - Instalar e configurar o VMware vSphere e o vCenter
2. **Implantação**: Implante nós de grade usando o VMware vSphere Web Client. Quando você implementa nós de grade, eles são criados como parte do sistema StorageGRID e conetados a uma ou mais redes.
    a. Use o VMware vSphere Web Client, um arquivo .vmdk e um conjunto de modelos de arquivo .ovf para implantar os nós baseados em software como máquinas virtuais (VMs) nos servidores preparados na etapa 1.
    b. Use o Instalador de dispositivos StorageGRID para implantar nós de dispositivos StorageGRID.

    > As instruções de instalação e integração específicas de hardware não estão incluídas no procedimento de instalação do StorageGRID. Para saber como instalar dispositivos StorageGRID, consulte as instruções de instalação e manutenção do seu aparelho.

3. **Configuração**: Quando todos os nós tiverem sido implantados, use o StorageGRIDGrid Manager para configurar a grade e concluir a instalação.

Essas instruções recomendam uma abordagem padrão para implantar e configurar um sistema StorageGRID em um ambiente VMware. Consulte também as informações sobre as seguintes abordagens alternativas:

- Use o script deploy-vsphere-ovftool.sh Bash (disponível no arquivo de instalação) para implantar nós de grade no VMware vSphere.
- Automatize a implantação e configuração do sistema StorageGRID usando um script de configuração Python (fornecido no arquivo de instalação).
- Automatize a implantação e a configuração dos nós de grade do dispositivo com um script de configuração Python (disponível no arquivo de instalação ou no instalador do dispositivo StorageGRID).
- Se você é um desenvolvedor avançado de implantações do StorageGRID, use as APIS REST de instalação para automatizar a instalação de nós de grade do StorageGRID.

Informações relacionadas

"Planejamento e preparação"

"Implantação de nós de grade de máquina virtual no VMware vSphere Web Client"

"Configurar a grelha e concluir a instalação"

"Automatizando a instalação"

"Visão geral da API REST de instalação"

"Diretrizes de rede"

Planejamento e preparação

Antes de implantar nós de grade e configurar a grade StorageGRID, você deve estar familiarizado com as etapas e requisitos para concluir o procedimento.

Os procedimentos de implantação e configuração do StorageGRID presumem que você está familiarizado com a arquitetura e a funcionalidade operacional do sistema StorageGRID.

Você pode implantar um único local ou vários locais de uma só vez. No entanto, todos os locais precisam

atender ao requisito mínimo de ter pelo menos três nós de storage.

Antes de iniciar o procedimento de implantação do nó e configuração da grade, você deve:

- Planeje a implantação do StorageGRID.
- Instale, conete e configure todo o hardware necessário, incluindo quaisquer dispositivos StorageGRID, de acordo com as especificações.

> As instruções de instalação e integração específicas de hardware não estão incluídas no procedimento de instalação do StorageGRID. Para saber como instalar dispositivos StorageGRID, consulte as instruções de instalação e manutenção do seu aparelho.

- Entenda as opções de rede disponíveis e como cada opção de rede deve ser implementada em nós de grade. Consulte as diretrizes de rede do StorageGRID.
- Reúna todas as informações de rede com antecedência. A menos que você esteja usando DHCP, reúna os endereços IP para atribuir a cada nó de grade e os endereços IP dos servidores DNS (Domain Name System) e NTP (Network Time Protocol) que serão usados.
- Decida qual das ferramentas de implantação e configuração disponíveis você deseja usar.

Informações relacionadas

"Diretrizes de rede"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

Materiais necessários

Antes de instalar o StorageGRID, você deve reunir e preparar os materiais necessários.

Item	Notas
Licença NetApp StorageGRID	Você deve ter uma licença NetApp válida e assinada digitalmente. **Nota**: O arquivo de instalação do StorageGRID inclui uma licença gratuita que não fornece qualquer direito de suporte para o produto.
Arquivo de instalação do StorageGRID para VMware	Você deve baixar o arquivo de instalação do StorageGRID e extrair os arquivos.
Software e documentação da VMware	Durante a instalação, você implanta nós de grade virtual em máquinas virtuais no VMware vSphere Web Client.para versões com suporte, consulte a Matriz de interoperabilidade.

Item	Notas
Serviço de laptop	O sistema StorageGRID é instalado através de um laptoO portátil de serviço tem de ter: • Porta de rede • Cliente SSH (por exemplo, PuTTY) • Navegador da Web suportado
Documentação do StorageGRID	• Notas de versão • Instruções para administrar o StorageGRID

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Transferir e extrair os ficheiros de instalação do StorageGRID"

"Requisitos do navegador da Web"

"Administrar o StorageGRID"

"Notas de lançamento"

Transferir e extrair os ficheiros de instalação do StorageGRID

Você deve baixar os arquivos de instalação do StorageGRID e extrair os arquivos.

Passos

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

   "NetApp Downloads: 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 aparecer uma instrução Caution/MustRead, leia-a e marque a caixa de seleção.

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

5. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.
6. Na coluna **Instalar StorageGRID**, selecione o software apropriado.

   Transfira o `.tgz` ficheiro de arquivo ou `.zip` para a sua plataforma.

   ◦ `StorageGRID-Webscale-version-VMware-uniqueID.zip`

   ◦ `StorageGRID-Webscale-version-VMware-uniqueID.tgz`

   Use o `.zip` arquivo se você estiver executando o Windows no laptop de serviço.

1. Salve e extraia o arquivo de arquivo.
2. Escolha os arquivos que você precisa na lista a seguir.

   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 de arquivamento.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós do Gateway.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de storage baseados em máquina virtual.
Ferramenta de script de implantação	Descrição
	Um script de shell Bash usado para automatizar a implantação de nós de grade virtual.
	Um arquivo de configuração de exemplo para uso com o `deploy-vsphere-ovftool.sh` script.

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 script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.
	Um arquivo de configuração de exemplo para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.

Informações relacionadas

"Manter recuperar"

Requisitos de software

Você pode usar uma máquina virtual para hospedar qualquer tipo de nó de grade do StorageGRID. Uma máquina virtual é necessária para cada nó de grade instalado no servidor VMware.

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 de grade do StorageGRID.

Para versões com suporte do software VMware vSphere Hypervisor e VMware vCenter Server, consulte a Matriz de interoperabilidade.

Para obter as etapas necessárias para instalar esses produtos VMware, consulte a documentação da VMware.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

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.

Para obter informações sobre servidores suportados, consulte a Matriz de interoperabilidade.

Cada nó do StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Pelo menos 24 GB por nó e 2 a 16 GB menos do que a RAM total do sistema, dependendo do total de RAM disponível e da quantidade de software que não seja StorageGRID executado no sistema

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), considere 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 de administração, monitoramento e atualização do 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 as informações sobre os requisitos de armazenamento.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Requisitos de storage e desempenho"

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

"Atualizar o software"

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 AFF

Se você estiver implantando um nó StorageGRID como uma máquina virtual com armazenamento atribuído a partir de um sistema NetApp AFF, 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.

> Em uma implantação de produção, não execute mais de um nó de armazenamento em um único servidor de máquina virtual. O uso de um host de máquina virtual dedicado para cada nó de armazenamento fornece um domínio de falha isolado.

Outros tipos de nós, como nós de administração ou nós de gateway, podem ser implantados no mesmo host de máquina virtual ou podem ser implantados em seus próprios hosts de máquina virtual dedicados, conforme necessário. No entanto, se você tiver vários nós do mesmo tipo (dois nós de Gateway, por exemplo), não instale todas as instâncias no mesmo host de máquina virtual.

Requisitos de storage por tipo de nó

Em um ambiente de produção, as máquinas virtuais para nós de grade do StorageGRID devem atender a requisitos diferentes, dependendo dos tipos de nós.

> Os snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte os procedimentos de recuperação e manutenção 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.
Nó de gateway	LUN DE 100 GB PARA OS
Nó de arquivo	LUN DE 100 GB PARA OS

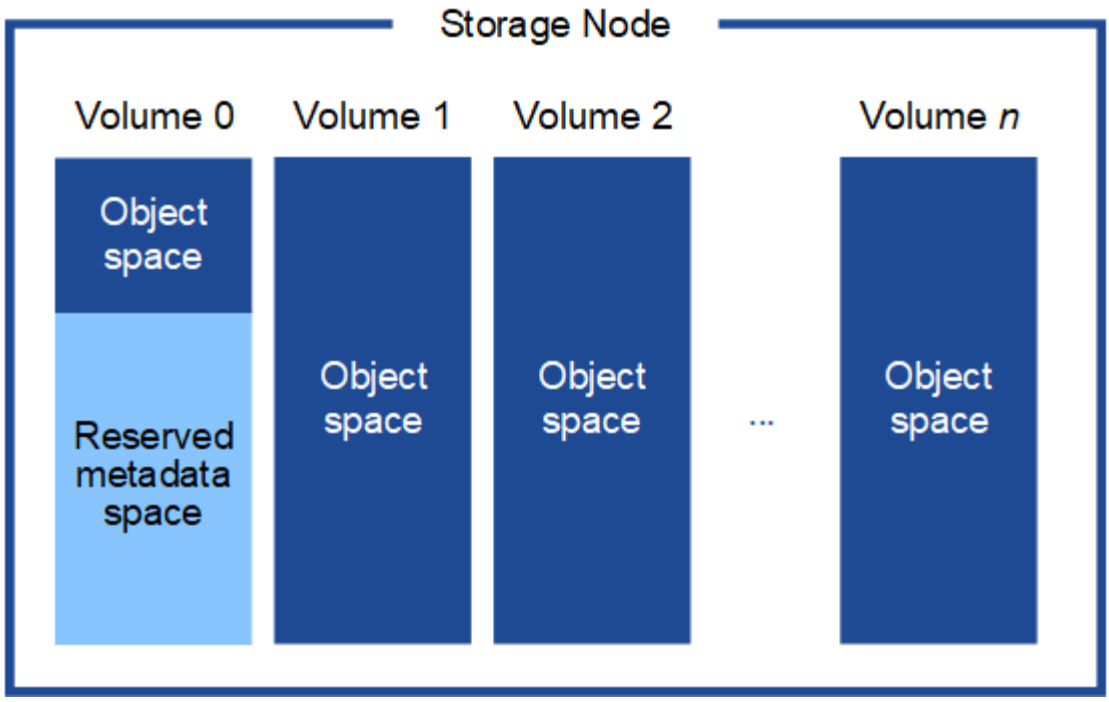
> Dependendo do nível de auditoria configurado, do tamanho das entradas do usuário, como o nome da chave do objeto S3 e a quantidade de dados de log de auditoria que você precisa preservar, talvez seja necessário aumentar o tamanho do LUN de log de auditoria em cada nó de administração. Como regra geral, 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 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 Storage Read-Only (somente leitura de armazenamento) na inicialização e armazenar somente metadados de objetos.

- Se você estiver instalando um novo sistema StorageGRID 11,5 e cada nó de armazenamento tiver 128 GB ou mais de RAM, deverá atribuir 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 detalhes, vá para as instruções de administração do StorageGRID e procure "armazenamento de metadados de objetos".

"Administrar o StorageGRID"

Informações relacionadas

"Manter recuperar"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Implantação de nós de grade de máquina virtual no VMware vSphere Web Client

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. Se você precisar implantar qualquer nó de storage do dispositivo StorageGRID, consulte as instruções de instalação e manutenção do dispositivo depois de implantar todos os nós de grade da máquina virtual.

- "Coletando informações sobre seu ambiente de implantação"
- "Como os nós de grade descobrem o nó de administração principal"
- "Implantando um nó StorageGRID como uma máquina virtual"

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

"SG5600 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG6000 dispositivos de armazenamento"

Coletando 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.

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 de grade 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.
- Se você não estiver usando DHCP, os detalhes de rede necessários para cada nó de grade (endereço IP, gateway e máscara de rede).
- Se você não estiver usando DHCP, o endereço IP do nó de administração principal na rede de grade. Consulte "como os nós de grade descobrem o nó de administrador 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).
- 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).

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 você pretende adicionar. Consulte ""requisitos de armazenamento e desempenho".

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 (Domain Name System)

Informações relacionadas

"Como os nós de grade descobrem o nó de administração principal"

"Requisitos de storage e desempenho"

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 de 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.

Implantando 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. Opcionalmente, você pode remapear portas de nós ou aumentar as configurações de CPU ou memória para o nó antes de ligá-lo.

O que você vai precisar

- Você revisou os tópicos de Planejamento e preparação e entende os requisitos de software, CPU e RAM, armazenamento e desempenho.

  "Planejamento e preparação"

- 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-<em>SG-version</em>-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-archive.ovf vsphere-archive.mf	O arquivo de modelo e o arquivo de manifesto para um nó de arquivo.
vsphere-gateway.ovf vsphere-gateway.mf	O arquivo de modelo e o arquivo de manifesto para um Gateway Node.
vsphere-storage.ovf vsphere-storage.mf	O arquivo de modelo e o arquivo de manifesto para um nó de armazenamento.

- 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 servidor de máquina virtual.

> Em uma implantação de produção, não execute mais de um nó de armazenamento em um único servidor de máquina virtual. O uso de um host de máquina virtual dedicado para cada nó de armazenamento fornece um domínio de falha isolado.

- Se você estiver implantando um nó como parte de uma operação de expansão ou recuperação, terá as instruções para expandir um sistema StorageGRID ou as instruções de recuperação e manutenção.
  - "Expanda sua grade"
  - "Manter recuperar"
- Se você estiver implantando um nó StorageGRID como uma máquina virtual com armazenamento atribuído a partir de um sistema NetApp AFF, 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, nós de gateway e nós de arquivamento.

Se estiver a instalar um novo sistema StorageGRID:

- Você deve implantar o nó de administração principal antes de implantar qualquer outro nó de grade.
- 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 ao nó de administração principal pela rede de grade.

Se você precisar remapear qualquer uma das portas do nó, não ligue o novo nó até que a configuração do remapeamento da 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-<em>SG-version</em>-SHA.vmdk
   vsphere-<em>node</em>.ovf
   vsphere-<em>node</em>.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-<em>SG-version</em>-SHA.vmdk
sphere-primary-admin.ovf
sphere-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).

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.
   - 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 não utilizar a rede de cliente, selecione o mesmo destino que selecionou para a rede de grelha.

7. Em **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. 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.

c. 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 as diretrizes de rede para as portas usadas pelo StorageGRID.

    "Diretrizes de rede"

    > ⓘ 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. Role para trás até o topo da tabela e selecione **Editar**.
        ii. Na guia tipo, selecione **User Configurable** e **Save**.
        iii. Selecione **Definir valor**.
        iv. 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
        ```

        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. Role para trás até o topo da tabela e selecione **Editar**.

ii. Na guia tipo, selecione **User Configurable** e **Save**.

iii. Selecione **Definir valor**.

iv. 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
```

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 grelha e concluir a instalação

Você conclui a instalação configurando o sistema StorageGRID a partir do Gerenciador de Grade no nó Admin principal.

- "Navegando para o Gerenciador de Grade"
- "Especificando as informações da licença do StorageGRID"
- "Adicionar sites"
- "Especificando sub-redes de rede de Grade"

- "Aprovando nós de grade pendentes"
- "Especificando informações do servidor Network Time Protocol"
- "Especificando informações do servidor do sistema de nomes de domínio"
- "Especificando as senhas do sistema StorageGRID"
- "Rever a sua configuração e concluir a instalação"
- "Diretrizes de pós-instalação"

Navegando para o Gerenciador de Grade

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

O que você vai precisar

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 um dos seguintes endereços:

   `https://primary_admin_node_ip`

   `client_network_ip`

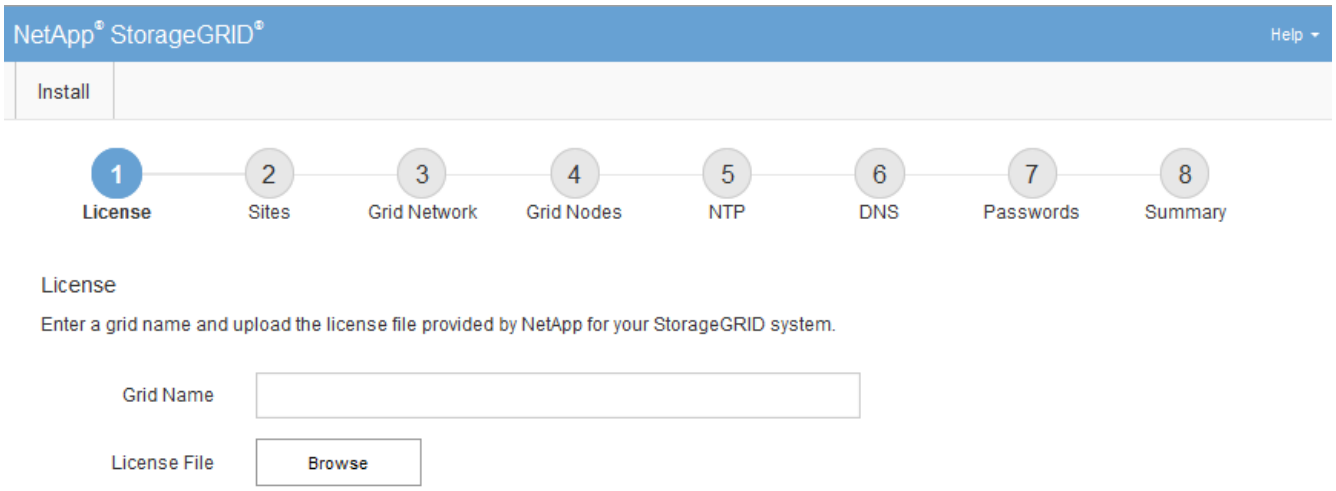
   Como alternativa, você pode acessar o Gerenciador de Grade na porta 8443:

   `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. Clique em **Instalar um sistema StorageGRID**.

   A página usada para configurar uma grade StorageGRID é exibida.



Especificando 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

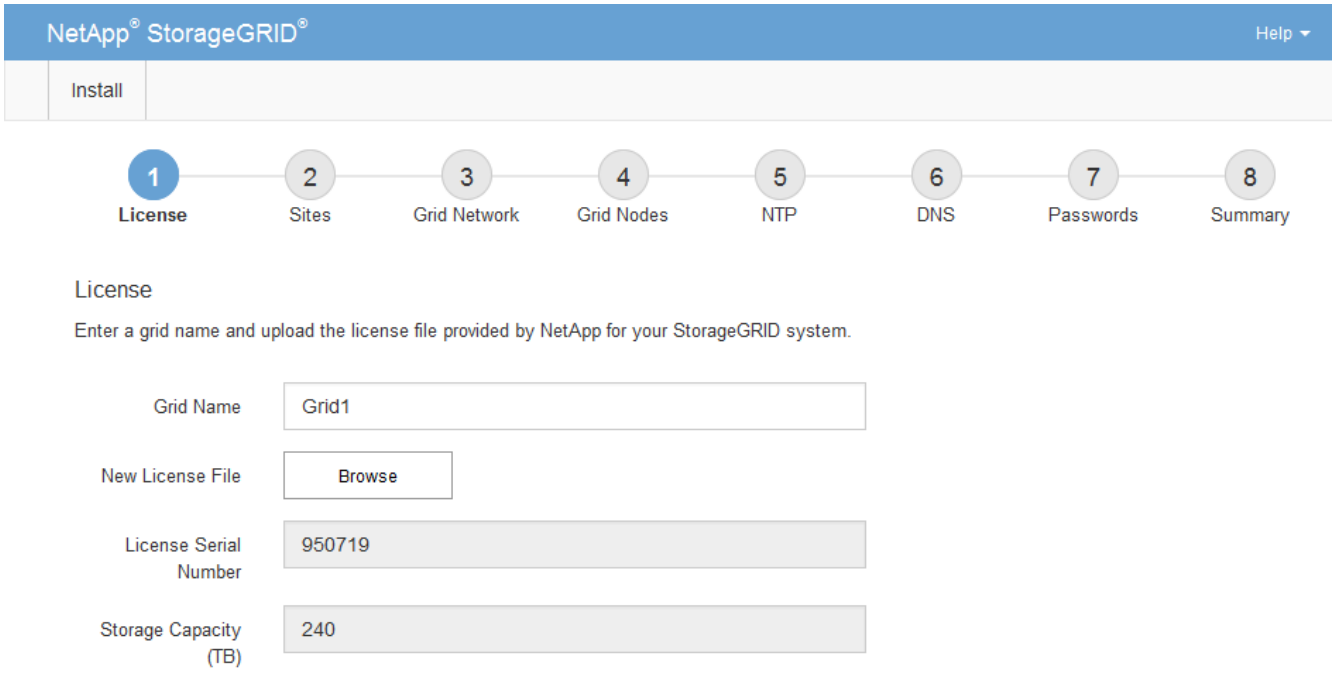
1. Na página Licença, insira um nome significativo para o seu sistema StorageGRID em **Nome da Grade**.

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

2. Clique em **Procurar**, localize o ficheiro de licença do NetApp (`NLFunique_id.txt`) e clique em **abrir**.

   O arquivo de licença é validado e o número de série e a capacidade de armazenamento licenciada são exibidos.

   > 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. Clique em **seguinte**.

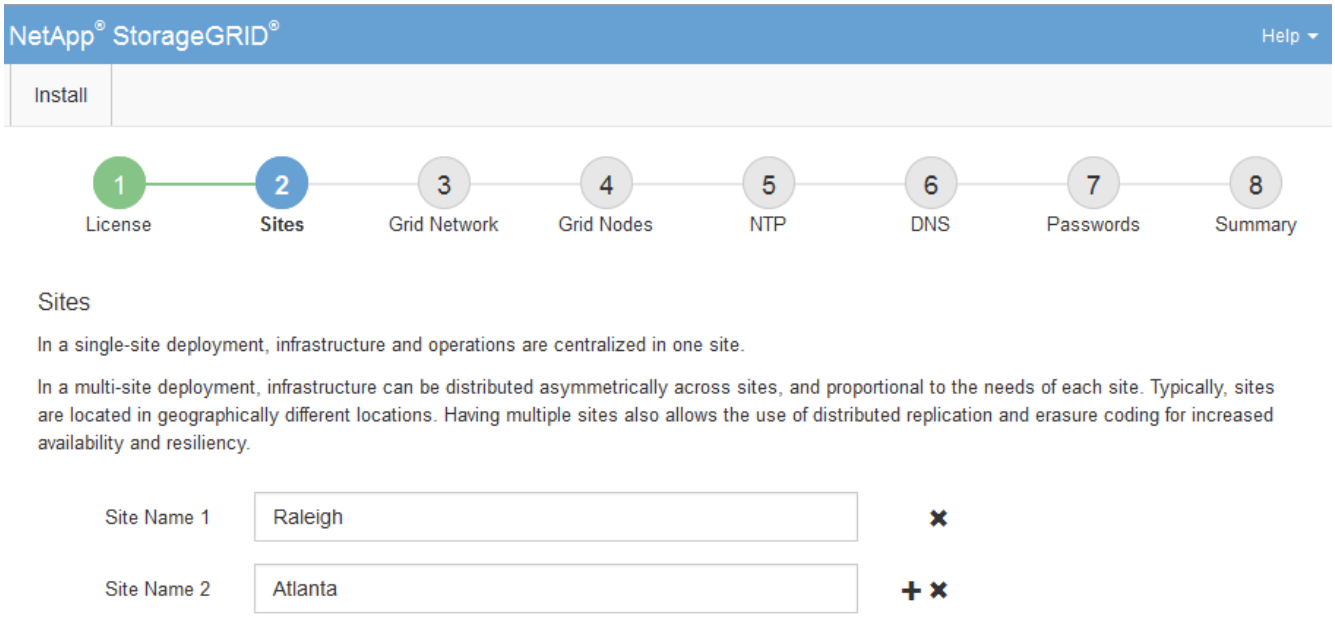
Adicionar sites

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**.

Especificando sub-redes de rede de Grade

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

Sobre esta tarefa

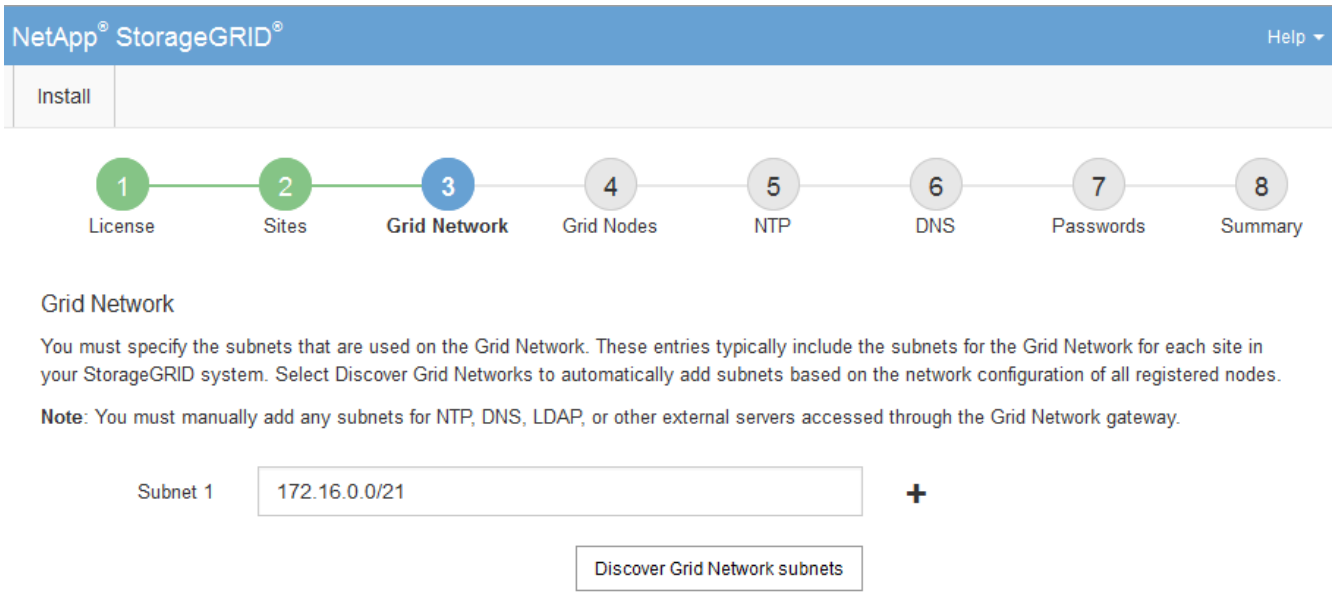
As entradas de sub-rede incluem as sub-redes para a rede de Grade para cada site no seu sistema StorageGRID, juntamente com quaisquer sub-redes que precisam ser acessíveis através da rede de Grade.

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.

   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.



3. Clique em **seguinte**.

Aprovando nós de grade pendentes

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

O que você vai precisar

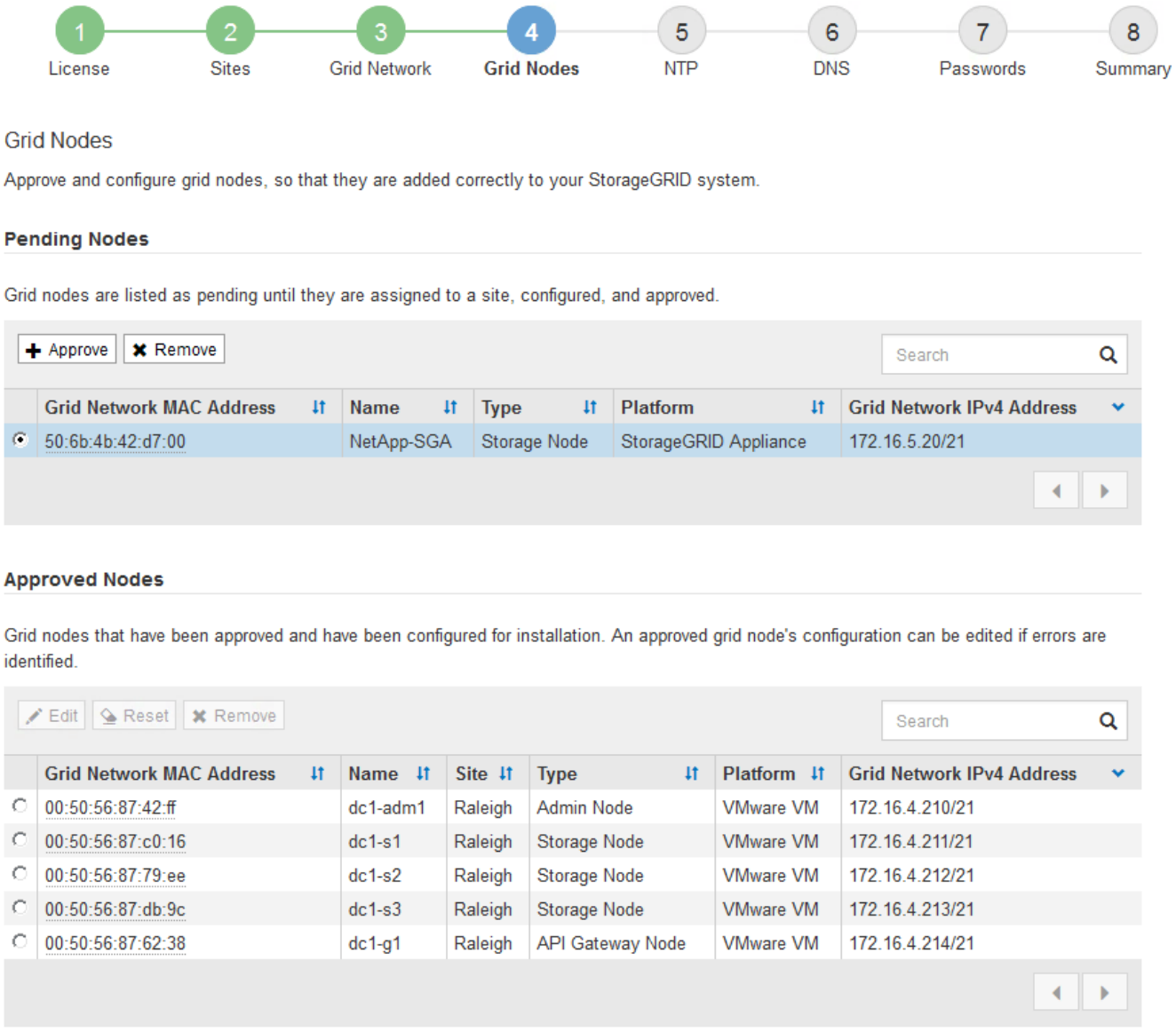
Todos os nós de grade de dispositivos virtuais e StorageGRID devem ter sido implantados.

Passos

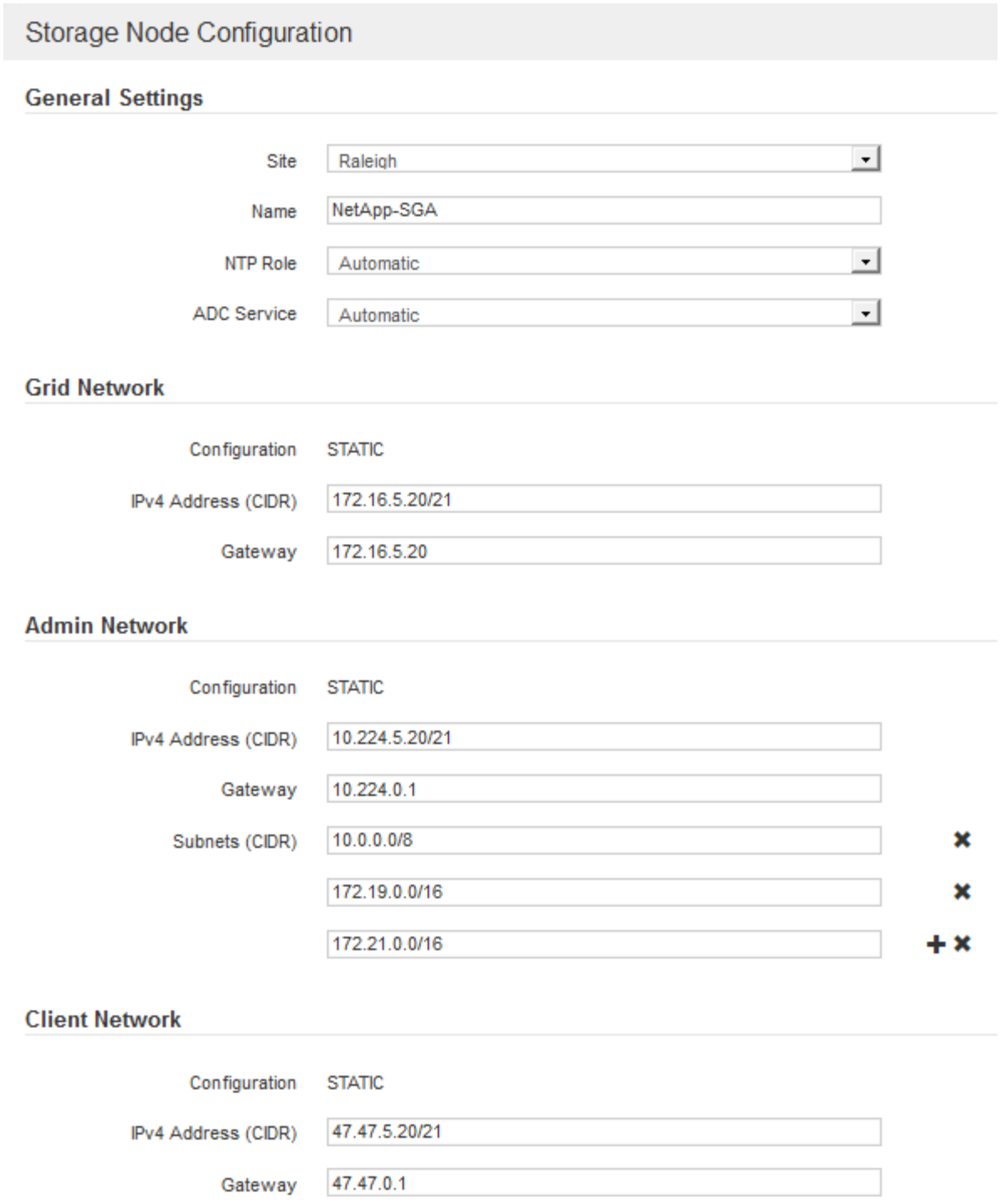
1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade implantados.

   Se um nó de grade estiver ausente, confirme que ele foi implantado com sucesso.

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 site com o qual este nó de grade será associado.
- **Nome**: O nome que será atribuído ao nó e o nome que será exibido no Gerenciador de Grade. O nome padrão é o nome que você especificou quando configurou o nó. Durante esta etapa do processo de instalação, você pode alterar o nome conforme necessário.

> Depois de concluir a instalação, não é possível alterar o nome do nó.

> 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.

- **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. Você não pode 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 garantir que o endereço IP resultante não esteja 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 garantir que o endereço IP resultante não esteja 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 **Configurar rede Configuração de ligação** 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, redefina 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.

   Para obter informações adicionais, consulte as instruções de instalação e manutenção 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 garantir que o endereço IP resultante não esteja 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 **Configurar rede Configuração de ligação** 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, redefina o nó.

   f. Remova o nó da tabela nós pendentes.

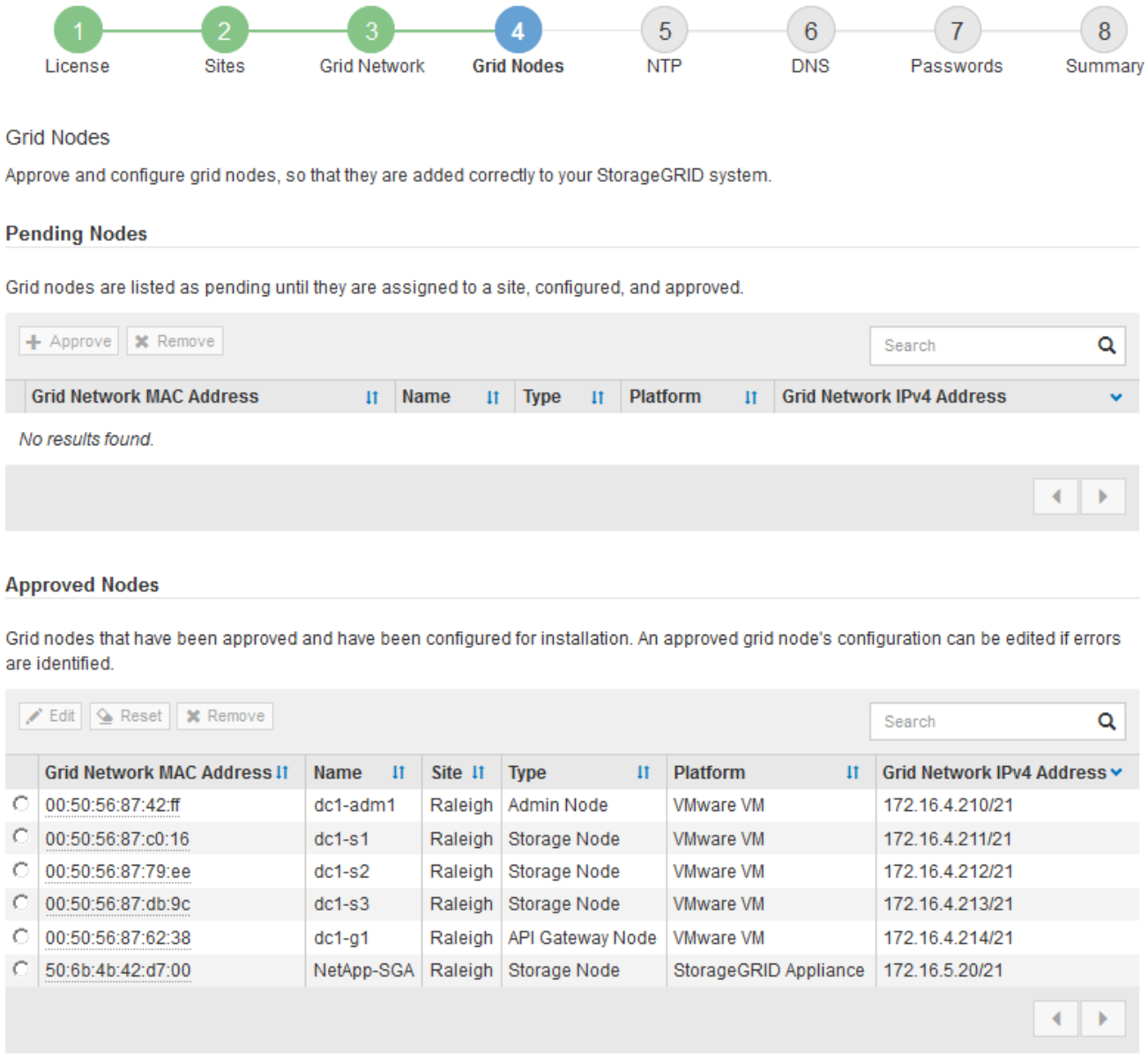
   g. Aguarde que o nó reapareça na lista de nós pendentes.

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

      Para obter informações adicionais, consulte as instruções de instalação e manutenção 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**.

Especificando 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"

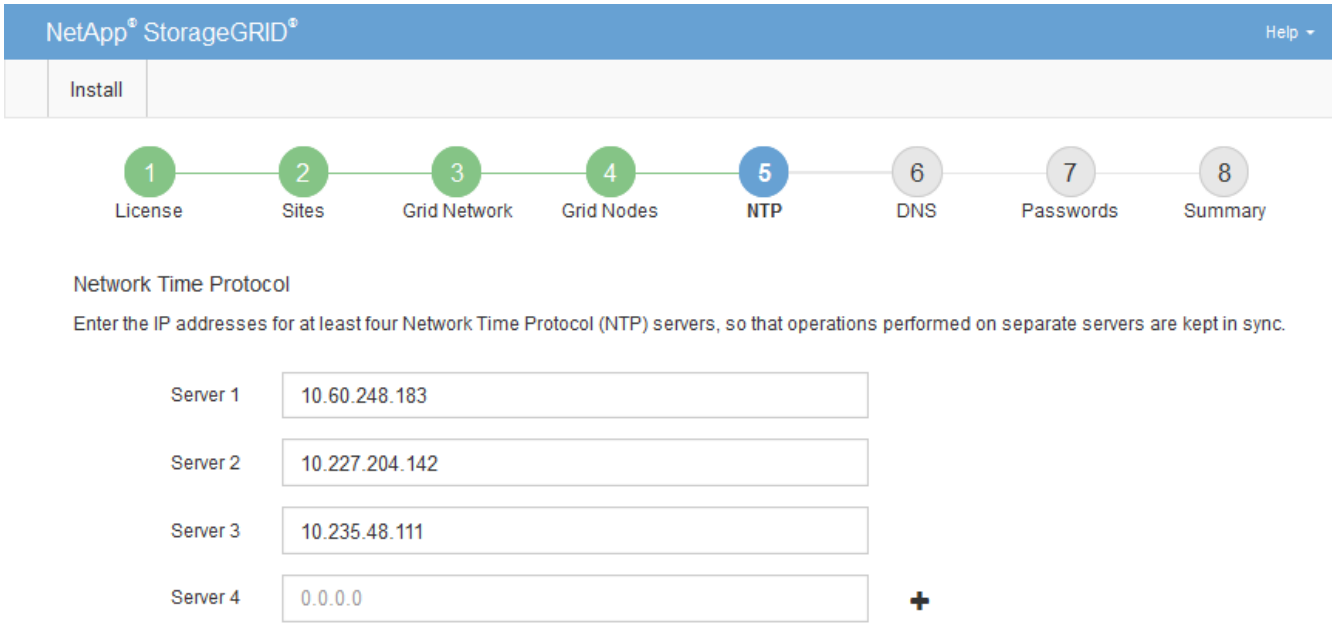
Os servidores NTP externos são usados pelos nós aos quais você atribuiu funções primárias NTP anteriormente.

> 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**.

Especificando informações do servidor do sistema de nomes de domínio

Você deve especificar informações do sistema de nomes de domínio (DNS) para o seu sistema StorageGRID, para que você possa acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

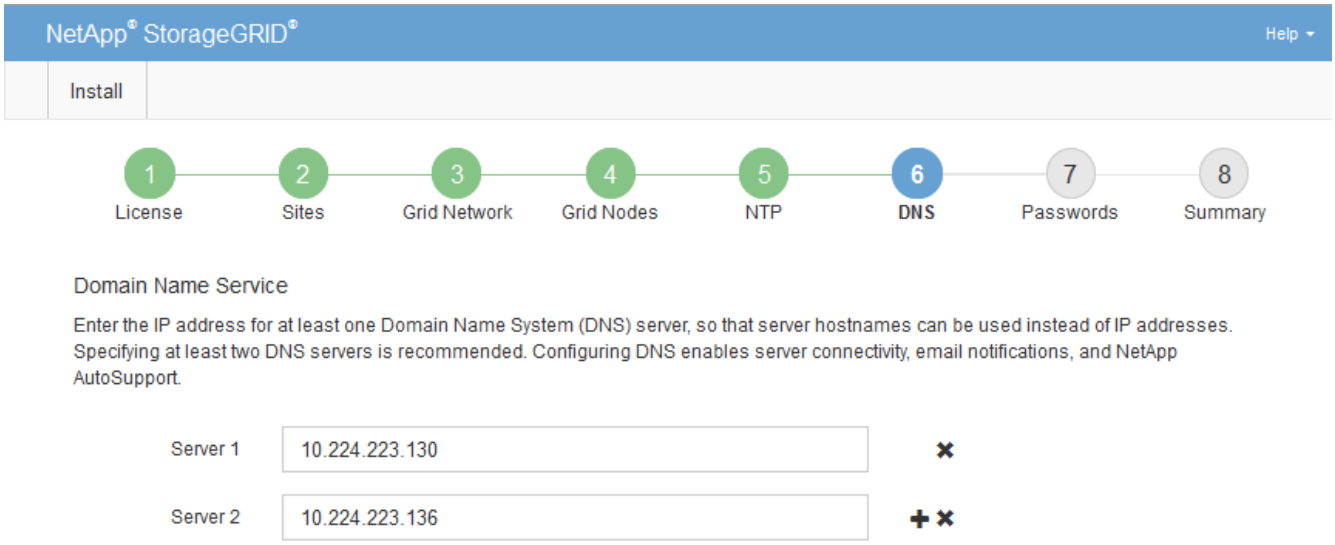
Especificar informações do servidor DNS permite que você use nomes de host de nome de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações de e-mail e AutoSupport. É recomendável especificar pelo menos dois servidores DNS.

> Forneça dois a seis endereços IPv4 para servidores DNS. Você deve selecionar servidores DNS que cada site pode acessar localmente no caso de rede ser aterrissada. Isso é para garantir que um site islanded continua a ter acesso ao serviço DNS. Depois de configurar a lista de servidores DNS em toda a grade, você pode personalizar ainda mais a lista de servidores DNS para cada nó. Para obter detalhes, consulte as informações sobre como modificar a configuração DNS nas instruções de recuperação e manutenção.

Se as informações do servidor DNS forem omitidas ou configuradas incorretamente, um alarme DNST será acionado no serviço SSM de cada nó da grade. O alarme é apagado quando o DNS está configurado corretamente e as novas informações do servidor atingiram todos os nós da grade.

Passos

1. 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**.

Informações relacionadas

"Manter recuperar"

Especificando 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.

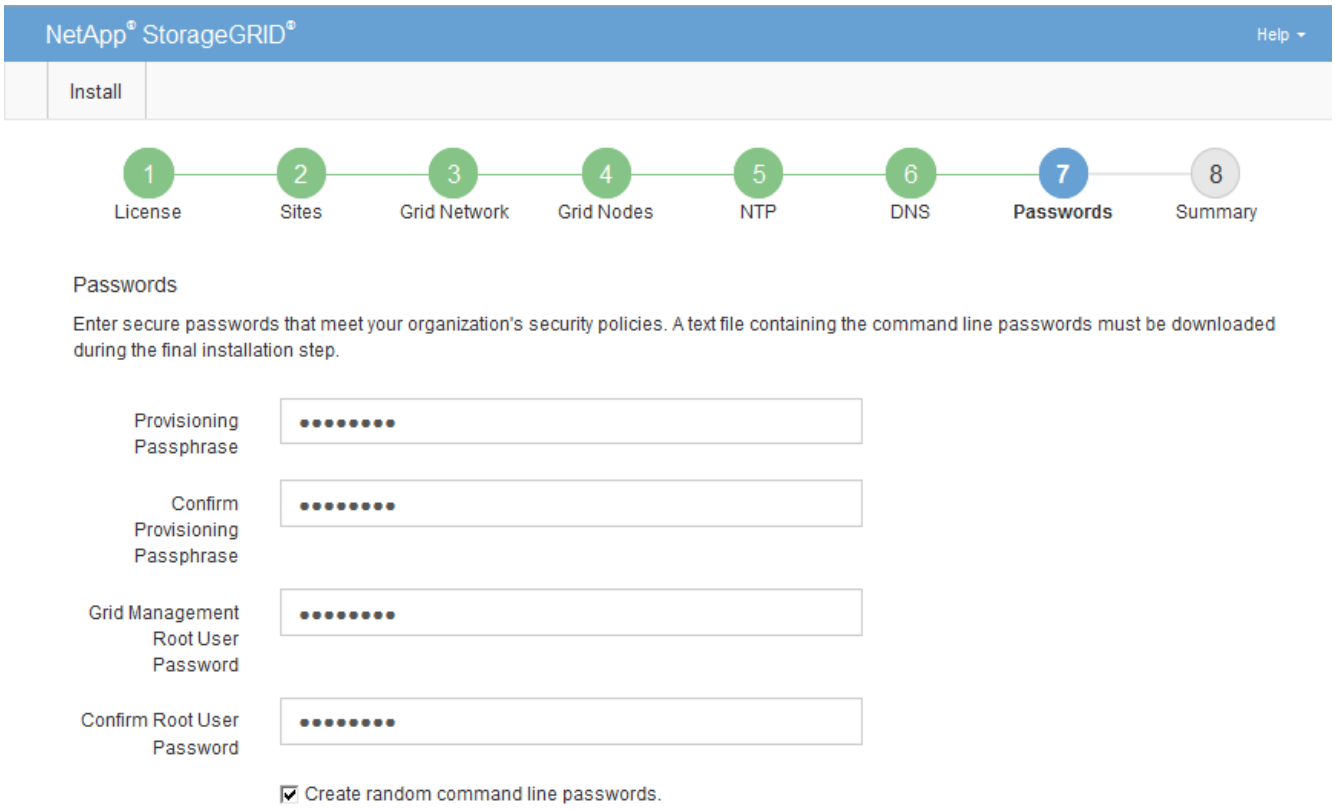
   Armazene a senha de provisionamento em um local seguro.

   > ⓘ Se após a conclusão da instalação e você quiser alterar a senha de provisionamento mais tarde, você pode usar o Gerenciador de Grade. Selecione **Configuração Controle de Acesso senhas de Grade**.

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 opcionalmente 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. Desmarque **criar senhas de linha de comando aleatórias** apenas para grades de demonstração se você quiser usar senhas padrão para acessar os 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. Tem de transferir este ficheiro para concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas `Passwords.txt` no arquivo, contido no arquivo Pacote de recuperação.

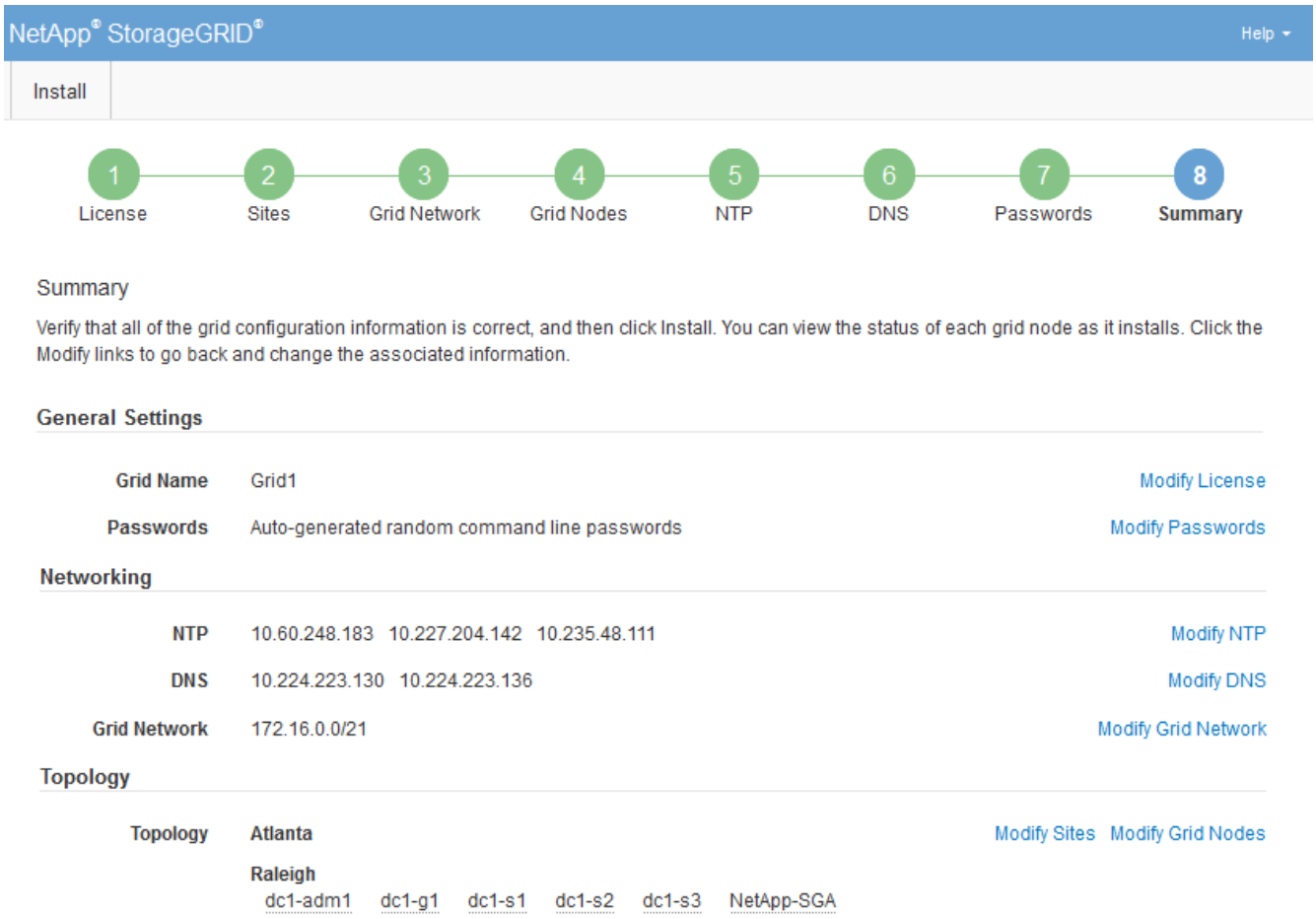
6. Clique em **seguinte**.

Rever a sua configuração e concluir 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.

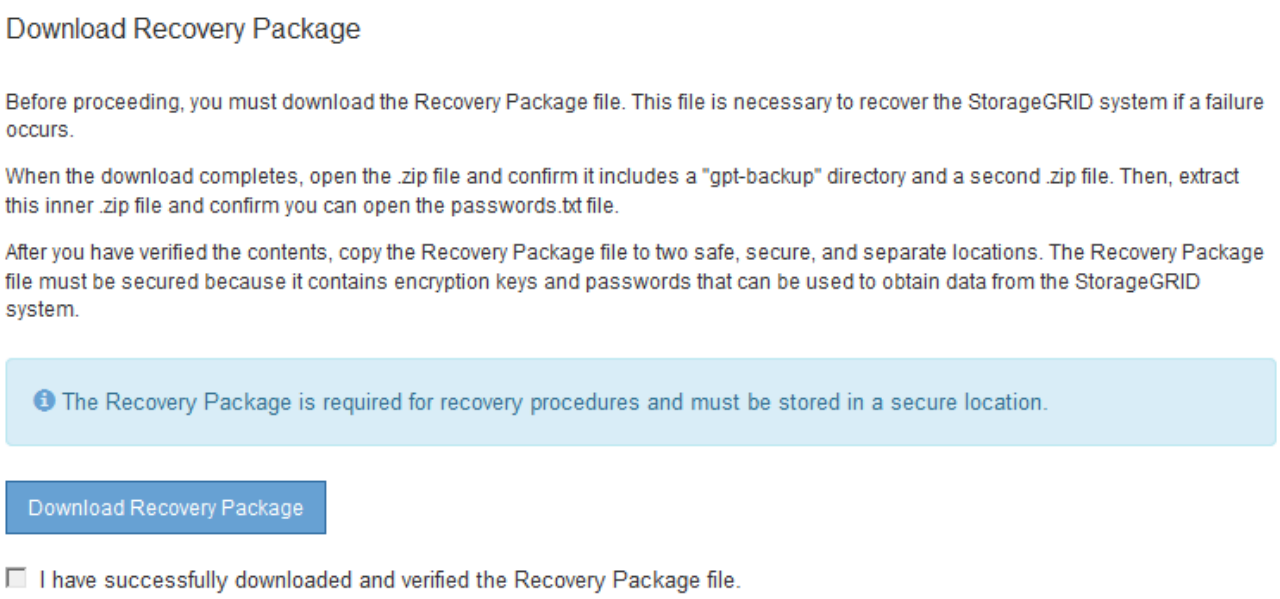
4. Clique em **Download Recovery Package**.

   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 não é possível concluir a instalação e aceder ao sistema StorageGRID até transferir e verificar este ficheiro.

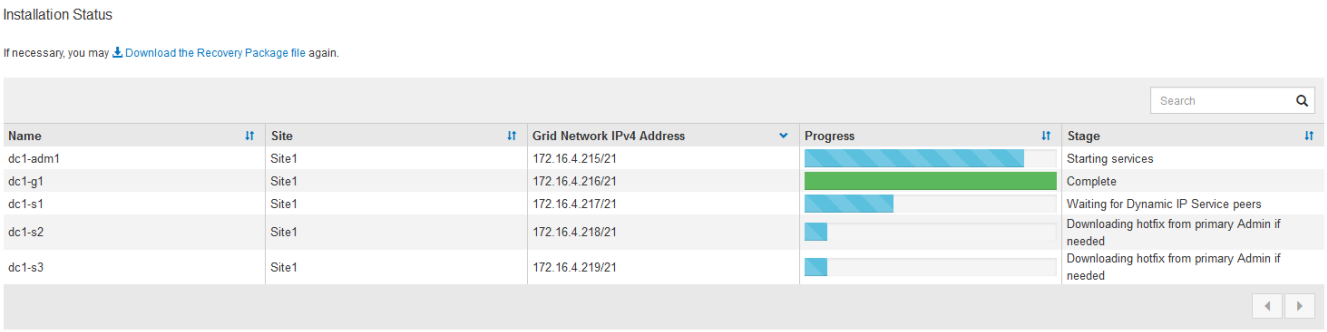
5. Verifique se você pode extrair o conteúdo do `.zip` arquivo e salvá-lo em dois locais seguros, seguros e separados.

> 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. Faça login no Gerenciador de Grade usando o usuário "root" e a senha que você especificou 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 seus endereços IP são alterados, o que pode causar interrupções se uma alteração de endereço 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. Consulte as informações sobre como configurar endereços IP nas instruções de recuperação e manutenção.
- 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.

Automatizando a instalação

Você pode automatizar a implantação de nós de grade virtual VMware, a configuração de nós de grade e a configuração de dispositivos StorageGRID.

- "Automatizando a implantação de nó de grade no VMware vSphere"
- "Automatizando a configuração do StorageGRID"

Automatizando a implantação de nó de grade no VMware vSphere

Você pode automatizar a implantação de nós de grade do StorageGRID no VMware vSphere.

O que você vai precisar

- Você tem acesso a um sistema Linux/Unix com o Bash 3,2 ou posterior.
- Você tem o VMware OVF Tool 4,1 instalado e configurado corretamente.
- Você sabe o nome de usuário e a senha necessários para acessar o VMware vSphere usando a ferramenta OVF.
- 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.

- Recolheu todas as informações necessárias para o ficheiro de configuração. Consulte "Coletando 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.
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-archive.ovf vsphere-archive.mf	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de arquivamento.
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 arquivo de configuração de exemplo para uso com o `deploy-vsphere-ovftool.sh` script.

Definindo 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 arquivo de configuração de exemplo, para que você não precise criar o arquivo do zero.

Passos

1. Faça uma cópia do arquivo de configuração de amostra (`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=thin
--datastore='<em>datastore_name</em>'
```

  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-<em>version</em>/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 = DHCP
```

- **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 = 8192
```

  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 à 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. 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. 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.

- **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.

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, VM_Archive_Node ou VM_API_Gateway_Node
- **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

  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
```

A configuração adicional a seguir é opcional 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
```

Nó de arquivo

A seguinte configuração adicional é necessária para nós de arquivo:

- **NODE_TYPE**: VM_Archive_Node

Esta entrada de exemplo é para um nó de arquivo que está nas redes de Grade e Admin, mas não na rede de cliente.

```
[DC1-ARC1]
  NODE_TYPE = VM_Archive_Node

  GRID_NETWORK_IP = 10.1.0.4
  ADMIN_NETWORK_IP = 10.3.0.4

  ADMIN_IP = 10.1.0.2
```

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.

Informações relacionadas

"Como os nós de grade descobrem o nó de administração principal"

"Diretrizes de rede"

Executando 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 de grade do StorageGRID no VMware vSphere.

O que você vai precisar

- 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               |
+------------------------------+----------+----------------------+
```

Automatizando a configuração do StorageGRID

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

O que você vai precisar

- 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 amostra (`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 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 .zip do pacote de recuperação 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, você precisa extrair o arquivo Passwords.txt e procurar 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

"Navegando para o Gerenciador de Grade"

"Visão geral da API REST de instalação"

Visão geral da 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 (JavaScript Object Notation).

> Todas as operações de API que você executa usando a página da Web do API Docs 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 seu sistema StorageGRID e, caso precise 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.

Onde ir a seguir

Depois de concluir uma instalação, você deve executar uma série de etapas de integração e configuração. Alguns passos são necessários; outros são opcionais.

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 cada protocolo de cliente (Swift ou S3) que será usado para armazenar objetos em seu sistema StorageGRID.
- Controle o acesso ao sistema configurando grupos e contas de usuário. Opcionalmente, você pode configurar uma fonte de identidade federada (como ative Directory ou OpenLDAP), para que você possa importar grupos de administração e usuários. Ou, você pode criar grupos e usuários locais.
- Integre e teste os aplicativos cliente API S3 ou Swift que você usará para fazer upload de objetos para seu sistema StorageGRID.
- Quando estiver pronto, configure as regras de gerenciamento do ciclo de vida das informações (ILM) e a política de ILM que você deseja usar para proteger os dados do objeto.

  > Quando você instala o StorageGRID, a política ILM padrão, Diretiva de cópias de linha de base 2, está ativa. Esta política inclui a regra ILM (fazer 2 cópias) e aplica-se se nenhuma outra política tiver sido ativada.

- Se a instalação incluir nós de storage do dispositivo, use o software SANtricity para concluir as seguintes tarefas:
  - Ligue a cada dispositivo StorageGRID.
  - Verifique a receção dos dados do AutoSupport.
- Se o seu sistema StorageGRID incluir quaisquer nós de arquivamento, configure a conexão do nó de arquivamento ao sistema de storage de arquivamento externo de destino.

Se algum nó de arquivamento usar o Tivoli Storage Manager como o sistema de armazenamento de arquivamento externo, você também deve configurar o Tivoli Storage Manager.

- Revise e siga as diretrizes de fortalecimento do sistema StorageGRID para eliminar os riscos de segurança.
- Configurar notificações por e-mail para alertas do sistema.

Tarefas opcionais

- Se você quiser receber notificações do sistema de alarme (legado), configure listas de e-mail e notificações por e-mail para alarmes.
- Atualize os endereços IP do nó da grade se eles tiverem sido alterados desde que você planejou sua implantação e gerou o Pacote de recuperação. Consulte as informações sobre como alterar endereços IP nas instruções de recuperação e manutenção.
- Configure a criptografia de armazenamento, se necessário.
- Configure a compactação de armazenamento para reduzir o tamanho dos objetos armazenados, se necessário.
- Configurar acesso de cliente de auditoria. Você pode configurar o acesso ao sistema para fins de auditoria por meio de um compartilhamento de arquivos NFS ou CIFS. Consulte as instruções para administrar o StorageGRID.

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

Solução de 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)

Para saber como acessar os arquivos de log, consulte as instruções para monitoramento e solução de problemas do StorageGRID. Para obter ajuda para solucionar problemas de instalação do aparelho, consulte as instruções de instalação e manutenção dos seus aparelhos. Se precisar de ajuda adicional, entre em Contato com o suporte técnico.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Suporte à NetApp"

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.

Atualizar o software

Saiba como atualizar um sistema StorageGRID para uma nova versão.

- "Sobre o StorageGRID 11,5"
- "Planejamento e preparação de atualização"
- "Realizar a atualização"
- "Solução de problemas de atualização"

Sobre o StorageGRID 11,5

Antes de iniciar uma atualização, revise esta seção para saber mais sobre os novos recursos e aprimoramentos no StorageGRID 11,5, determinar se algum recurso foi obsoleto ou removido e saber mais sobre alterações nas APIs do StorageGRID.

- "Novidades do StorageGRID 11,5"
- "Recursos removidos ou obsoletos"
- "Alterações na API Grid Management"

- "Alterações na API de gerenciamento do locatário"

Novidades do StorageGRID 11,5

O StorageGRID 11,5 apresenta o bloqueio de objeto S3, suporte para criptografia KMIP de dados, melhorias de usabilidade para o ILM, uma interface de usuário do Gerenciador de locatário reprojetada, suporte para desativação de um site StorageGRID e um procedimento de clone de nó de dispositivo.

S3 bloqueio de objetos para dados compatíveis

O recurso bloqueio de objetos S3 no StorageGRID 11,5 é uma solução de proteção de objetos equivalente ao bloqueio de objetos S3 no Amazon Simple Storage Service (Amazon S3). Você pode habilitar a configuração global de bloqueio de objeto S3 para um sistema StorageGRID para permitir que as contas de locatário S3 criem buckets com o bloqueio de objeto S3 ativado. O locatário pode então usar um aplicativo cliente S3 para especificar opcionalmente as configurações de retenção e retenção legal para os objetos nesses buckets.

O bloqueio de objetos S3 permite que os usuários do locatário cumpram os regulamentos que exigem que determinados objetos sejam mantidos por um período de tempo fixo ou indefinidamente.

Saiba mais

- "Gerenciar objetos com ILM"
- "Use S3"
- "Use uma conta de locatário"

Gerenciamento de chaves de criptografia KMS

Agora você pode configurar um ou mais servidores de gerenciamento de chaves externas (KMS) no Gerenciador de Grade para fornecer chaves de criptografia para serviços e dispositivos de armazenamento do StorageGRID. Cada cluster de KMS ou KMS usa o Key Management Interoperability Protocol (KMIP) para fornecer uma chave de criptografia aos nós do dispositivo no site associado do StorageGRID. 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.

> Se você quiser usar o gerenciamento de chaves de criptografia, use o Instalador de dispositivos StorageGRID para ativar a configuração **criptografia de nó** para o dispositivo antes de adicionar o dispositivo à grade.

Saiba mais

- "Administrar o StorageGRID"

Melhorias de usabilidade para o gerenciamento do ciclo de vida das informações (ILM)

- Agora você pode ver a capacidade total de um pool de armazenamento, incluindo a quantidade de espaço usado e livre. Você também pode ver quais nós estão incluídos em um pool de storage e quais regras de ILM e perfis de codificação de apagamento usam o pool de storage.
- Agora você pode criar regras de ILM que se aplicam a mais de uma conta de locatário.
- Quando você cria uma regra ILM para codificação de apagamento, agora você é lembrado de definir o filtro avançado tamanho do objeto (MB) para maior que 0,2 para garantir que objetos muito pequenos não sejam codificados para apagamento.

- A interface de política ILM agora garante que a regra ILM padrão será sempre usada para quaisquer objetos não correspondidos por outra regra. A partir do StorageGRID 11,5, a regra padrão não pode usar nenhum filtro básico ou avançado e é automaticamente colocada como a última regra na política.

  > Se a sua política ILM atual não estiver em conformidade com os novos requisitos, você poderá continuar a usá-la depois de atualizar para o StorageGRID 11,5. No entanto, se você tentar clonar uma política não conforme após a atualização, será solicitado que você selecione uma regra padrão que não inclua filtros e você deverá colocar a regra padrão no final da política.

- O pool de storage de todos os nós de storage de estoque não é mais selecionado por padrão quando você cria uma nova regra de ILM ou um novo perfil de codificação de apagamento. Além disso, agora você pode remover o pool de storage de todos os nós de storage, contanto que não seja usado em nenhuma regra.

  > O uso do pool de storage de todos os nós de storage não é recomendado porque esse pool de storage contém todos os locais. Várias cópias de um objeto podem ser colocadas no mesmo local se você usar esse pool de storage com um sistema StorageGRID que inclui mais de um local.

- Agora você pode remover a 2 regra fazer cópias de estoque (que usa o pool de storage de todos os nós de storage), contanto que ela não seja usada em uma política ativa ou proposta.
- Os objetos armazenados em um Cloud Storage Pool agora podem ser excluídos imediatamente (exclusão síncrona).

Saiba mais

- "Gerenciar objetos com ILM"

Melhorias no Gerenciador de Grade

- A página de contas do locatário redesenhada facilita a visualização do uso da conta do locatário. A tabela de resumo do locatário agora inclui colunas para espaço usado, utilização de cota, cota e contagem de objetos. Um novo botão **View Details** acessa uma visão geral de cada locatário, bem como detalhes sobre os buckets do S3 ou os contentores Swift da conta. Além disso, agora você pode exportar dois `.csv` arquivos para uso do locatário: Um contendo valores de uso para todos os locatários e outro contendo detalhes sobre os buckets ou contentores de um locatário.

  Relacionadas a essa alteração, três novas métricas do Prometheus foram adicionadas para rastrear o uso da conta de locatário:

  - `storagegrid_tenant_usage_data_bytes`
  - `storagegrid_tenant_usage_object_count`
  - `storagegrid_tenant_usage_quota_bytes`

- O novo campo **modo de acesso** na página grupos de administração (**Configuração Controle de acesso**) permite especificar se as permissões de gerenciamento para o grupo são leitura-gravação (padrão) ou somente leitura. Os usuários que pertencem a um grupo com modo de acesso de leitura e gravação podem alterar as configurações e executar operações no Gerenciador de Grade e na API de Gerenciamento de Grade. Os usuários que pertencem a um grupo com modo de acesso somente leitura só podem exibir as configurações e recursos selecionados para o grupo.

Ao atualizar para o StorageGRID 11,5, a opção de modo de acesso de leitura e gravação é selecionada para todos os grupos de administração existentes.

- A interface de usuário do AutoSupport foi redesenhada. Agora você pode configurar mensagens AutoSupport acionadas por eventos, acionadas pelo usuário e semanais a partir de uma única página no Gerenciador de Grade. Você também pode configurar um destino adicional para mensagens AutoSupport.

Se o AutoSupport não tiver sido ativado, uma mensagem de lembrete será exibida no Painel de Gerenciamento de Grade.

- Ao visualizar o gráfico **Storage Used - Object Data** na página nodos, agora você pode ver estimativas da quantidade de dados de objeto replicados e da quantidade de dados codificados de apagamento na grade, site ou nó de armazenamento (**nós *grid/site/nó de armazenamento* Storage**).
- As opções de menu do Gerenciador de Grade foram reorganizadas para facilitar a localização das opções. Por exemplo, um novo submenu **Configurações de rede** foi adicionado ao menu **Configuração** e as opções nos menus **Manutenção** e **suporte** agora estão listadas em ordem alfabética.

Saiba mais

- "Administrar o StorageGRID"

Melhorias para o Gerenciador do Locatário

- A aparência e a organização da interface de usuário do Tenant Manager foram completamente redesenhadas para melhorar a experiência do usuário.
- O novo painel do Tenant Manager fornece um resumo de alto nível de cada conta: Ele fornece detalhes do bucket e mostra o número de buckets ou contentores, grupos, usuários e endpoints de serviços de plataforma (se configurado).

Saiba mais

- "Use uma conta de locatário"

Certificados de cliente para exportação de métricas Prometheus

Agora você pode fazer upload ou gerar certificados de cliente (**Configuração Controle de Acesso certificados de Cliente**), que podem ser usados para fornecer acesso seguro e autenticado ao banco de dados do StorageGRID Prometheus. Por exemplo, você pode usar certificados de cliente se precisar monitorar o StorageGRID externamente usando o Grafana.

Saiba mais

- "Administrar o StorageGRID"

Melhorias no balanceador de carga

- Ao lidar com solicitações de roteamento em um local, o serviço Load Balancer agora executa roteamento com reconhecimento de carga: Considera a disponibilidade da CPU dos nós de storage no mesmo local. Em alguns casos, as informações sobre a disponibilidade da CPU estão limitadas ao local onde o serviço Load Balancer está localizado.

O reconhecimento da CPU não será ativado até que pelo menos dois terços dos nós de storage em um local tenham sido atualizados para o StorageGRID 11,5 e estejam relatando estatísticas da CPU.

- Para maior segurança, agora você pode especificar um modo de encadernação para cada ponto de extremidade do balanceador de carga. A fixação de endpoint permite restringir a acessibilidade de cada endpoint a grupos específicos de alta disponibilidade ou interfaces de nó.

Saiba mais

- "Administrar o StorageGRID"

Alterações de metadados de objetos

- **Nova métrica de espaço reservado real**: Para ajudá-lo a entender e monitorar o uso do espaço de metadados de objetos em cada nó de armazenamento, uma nova métrica Prometheus é mostrada no gráfico Storage Used - Object Metadata para um nó de armazenamento (**nós *Storage Node* Storage** * Storage * Storage * Storage * Storage *).

  ```
  storagegrid_storage_utilization_metadata_reserved
  ```

  A métrica **espaço reservado real** indica quanto espaço o StorageGRID reservou para metadados de objetos em um nó de armazenamento específico.

- **Espaço de metadados aumentado para instalações com nós de armazenamento maiores**: A configuração espaço reservado de metadados em todo o sistema foi aumentada para sistemas StorageGRID que contêm nós de armazenamento com 128 GB ou mais de RAM, como segue:

  - **8 TB para novas instalações**: Se você estiver instalando um novo sistema StorageGRID 11,5 e cada nó de armazenamento na grade tiver 128 GB ou mais de RAM, a configuração de espaço reservado de metadados em todo o sistema agora será definida como 8 TB em vez de 3 TB.
  - **4 TB para atualizações**: Se você estiver atualizando para o StorageGRID 11,5 e cada nó de armazenamento em qualquer site tiver 128 GB ou mais de RAM, a configuração espaço reservado de metadados em todo o sistema agora será definida como 4 TB em vez de 3 TB.

    Os novos valores para a configuração espaço reservado de metadados aumentam o espaço permitido de metadados para esses nós de armazenamento maiores, até 2,64 TB, e garantem que o espaço adequado de metadados seja reservado para futuras versões de hardware e software.

    > Se os seus nós de armazenamento tiverem RAM suficiente e espaço suficiente no volume 0, você poderá aumentar manualmente a configuração espaço reservado de metadados até 8 TB após a atualização. A reserva de espaço adicional de metadados após a atualização do StorageGRID 11,5 simplificará futuras atualizações de hardware e software.
    >
    > "Aumentando a configuração espaço reservado metadados"

  +

    > Se o seu sistema StorageGRID armazenar (ou é esperado que armazene) mais de 2,64 TB de metadados em qualquer nó de armazenamento, o espaço permitido de metadados pode ser aumentado em alguns casos. Se cada um dos seus nós de storage tiver espaço livre disponível no volume de storage 0 e mais de 128 GB de RAM, entre em Contato com o representante da conta do NetApp. O NetApp analisará seus requisitos e aumentará o espaço de metadados permitido para cada nó de storage, se possível.

- **Limpeza automática de metadados excluídos**: Quando 20% ou mais dos metadados armazenados em

um nó de storage estiverem prontos para serem removidos (porque os objetos correspondentes foram excluídos), o StorageGRID agora pode executar uma compactação automática nesse nó de storage. Esse processo de segundo plano só é executado se a carga no sistema for baixa, ou seja, quando houver CPU, espaço em disco e memória disponíveis. O novo processo de compactação remove os metadados de objetos excluídos antes das versões anteriores e ajuda a liberar espaço para que novos objetos sejam armazenados.

Saiba mais

- "Administrar o StorageGRID"

Alterações ao suporte à API REST do S3

- Agora você pode usar a API REST do S3 para especificar S3 bloqueio de objetos configurações:
  - Para criar um bucket com o bloqueio de objetos S3 ativado, use uma solicitação DE armazenamento COLOCAR com o `x-amz-bucket-object-lock-enabled` cabeçalho.
  - Para determinar se o bloqueio de objeto S3 está ativado para um bucket, use uma solicitação DE configuração OBTER bloqueio de objeto.
  - Ao adicionar uma versão de objeto a um bucket com o bloqueio de objeto S3 ativado, use os seguintes cabeçalhos de solicitação para especificar as configurações de retenção legal e retenção: `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date` E `x-amz-object-lock-legal-hold`.
- Agora você pode USAR EXCLUIR vários objetos em um bucket versionado.
- Agora você pode usar as solicitações de criptografia PUT, GET E DELETE Bucket para gerenciar a criptografia de um bucket existente do S3.
- Uma pequena alteração foi feita para um nome de campo para o `Expiration` parâmetro. Esse parâmetro é incluído na resposta a uma solicitação PUT Object, HEAD Object ou GET Object se uma regra de expiração na configuração do ciclo de vida se aplicar a um objeto específico. O campo que indica qual regra de expiração foi correspondida foi nomeado anteriormente `rule_id` . Este campo foi renomeado para para `rule-id` corresponder à implementação da AWS.
- Por padrão, a solicitação de uso do armazenamento S3 GET agora tenta recuperar o armazenamento usado por uma conta de locatário e seus buckets usando consistência global forte. Se a consistência global forte não puder ser alcançada, o StorageGRID tentará recuperar as informações de uso usando consistência de site forte.
- O `Content-MD5` cabeçalho de solicitação agora é suportado corretamente.

Saiba mais

- "Use S3"

O tamanho máximo para objetos CloudMirror aumentou para 5 TB

O tamanho máximo para objetos que podem ser replicados para um bucket de destino pelo serviço de replicação do CloudMirror foi aumentado para 5 TB, que é o tamanho máximo de objeto suportado pelo StorageGRID.

Saiba mais

- "Use S3"
- "Use Swift"

Novos alertas adicionados

Os seguintes novos alertas foram adicionados para o StorageGRID 11,5:

- Erro de comunicação do Appliance BMC
- Detectada avaria no canal de fibra do dispositivo
- Falha na porta HBA Fibre Channel do dispositivo
- Porta LACP do aparelho em falta
- Erro de auto-compactador Cassandra
- Métricas do compactador automático Cassandra desatualizadas
- Cassandra compactions sobrecarregado
- A e/S do disco é muito lenta
- Expiração do certificado CA de KMS
- Expiração do certificado do cliente KMS
- 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
- KMS não está configurado
- A chave KMS falhou ao desencriptar um volume de aparelho
- Expiração do certificado do servidor DE KMS
- Baixo espaço livre para piscina de armazenamento
- Erro de quadro de receção de rede do nó
- Conectividade de storage do dispositivo de serviços degradada
- Degradação da conectividade de storage do dispositivo (conectividade de storage do dispositivo anteriormente denominada degradada)
- Uso de cota de locatário alto
- Reinicialização inesperada do nó

Saiba mais

- "Monitorizar Resolução de problemas"

Suporte TCP para traps SNMP

Agora você pode selecionar TCP (Transmission Control Protocol) como o protocolo para destinos de intercetação SNMP. Anteriormente, apenas o protocolo UDP (User Datagram Protocol) era suportado.

Saiba mais

- "Monitorizar Resolução de problemas"

Melhorias de instalação e rede

- **Clonagem de endereços MAC**: Agora é possível usar a clonagem de endereços MAC para melhorar a segurança de determinados ambientes. A clonagem de endereços MAC permite que você use uma NIC

virtual dedicada para rede de Grade, rede de administração e rede de cliente. Fazer com que o contentor Docker use o endereço MAC da NIC dedicada no host permite evitar o uso de configurações de rede de modo promíscuo. Três novas chaves de clonagem de endereço MAC foram adicionadas ao arquivo de configuração de nó para nós baseados em Linux (bare metal).

- * Descoberta automática de rotas de host DNS e NTP*: Anteriormente, havia restrições em qual rede seus servidores NTP e DNS tinham que se conetar, como o requisito de que você não poderia ter todos os seus servidores NTP e DNS na rede de clientes. Agora, essas restrições são removidas.

Saiba mais

- "Instale o Red Hat Enterprise Linux ou CentOS"
- "Instale Ubuntu ou Debian"

Suporte para rebalanceamento de dados codificados por apagamento (EC) após a expansão do nó de storage

O procedimento EC Rebalanceance é um novo script de linha de comando que pode ser necessário depois de adicionar novos nós de storage. Ao executar o procedimento, o StorageGRID redistribui fragmentos codificados de apagamento entre os nós de storage existentes e recém-expandidos em um local.

> Só deve efetuar o procedimento de reequilíbrio CE em casos limitados. Por exemplo, se você não puder adicionar o número recomendado de nós de storage em uma expansão, use o procedimento EC Rebalancement para permitir que objetos codificados de apagamento adicionais sejam armazenados.

Saiba mais

- "Expanda sua grade"

Procedimentos de manutenção novos e revistos

- **Desativação do site**: Agora você pode remover um site operacional do seu sistema StorageGRID. O procedimento de desativação do local conetado remove um local operacional e preserva os dados. O novo assistente do Decommission Site orienta-o através do processo (**Manutenção Decommission Decommission Site**).
- * Clonagem de nó do dispositivo*: Agora você pode clonar um nó de dispositivo existente para atualizar o nó para um novo modelo de dispositivo. Por exemplo, você pode clonar um nó de dispositivo de capacidade menor para um dispositivo de capacidade maior. Você também pode clonar um nó de dispositivo para implementar novas funcionalidades, como a nova configuração **Node Encryption** necessária para a criptografia KMS.
- * Capacidade de alterar a senha de provisionamento*: Agora você pode alterar a senha de provisionamento (**Configuração Controle de Acesso senhas de Grade**). A frase-passe é necessária para procedimentos de recuperação, expansão e manutenção.
- * Comportamento aprimorado da senha SSH*: Para melhorar a segurança dos dispositivos StorageGRID, a senha SSH não é mais alterada quando você coloca um dispositivo no modo de manutenção. Além disso, novos certificados de host SSH e chaves de host são gerados quando você atualiza um nó para o StorageGRID 11,5.

> Se você usar SSH para fazer login em um nó após a atualização para o StorageGRID 11,5, receberá um aviso de que a chave do host foi alterada. Esse comportamento é esperado e você pode aprovar a nova chave com segurança.

Saiba mais

- "Manter recuperar"

Alterações nos dispositivos StorageGRID

- **Acesso direto ao Gerenciador de sistemas SANtricity para dispositivos de armazenamento**: Agora você pode acessar a interface de usuário do Gerenciador de sistemas SANtricity do e-Series a partir do Instalador de dispositivos StorageGRID e do Gerenciador de Grade. O uso desses novos métodos permite o acesso ao Gerenciador de sistema do SANtricity sem usar a porta de gerenciamento no dispositivo. Os usuários que precisam acessar o Gerenciador de sistema do SANtricity a partir do Gerenciador de Grade devem ter a nova permissão de Administrador do dispositivo de armazenamento.
- **Criptografia de nó**: Como parte do novo recurso de criptografia KMS, uma nova configuração **criptografia de nó** foi adicionada ao Instalador de dispositivos StorageGRID. Se você quiser usar o gerenciamento de chaves de criptografia para proteger os dados do dispositivo, ative essa configuração durante o estágio de configuração de hardware da instalação do dispositivo.
- **Conetividade de porta UDP**: Agora você pode testar a conetividade de rede de um dispositivo StorageGRID para portas UDP, como as usadas para um servidor NFS ou DNS externo. No Instalador de dispositivos StorageGRID, selecione **Configurar rede Teste de conetividade de porta (nmap)**.
- **Automatizar instalação e configuração**: Uma nova página de upload de configuração JSON foi adicionada ao Instalador de dispositivos StorageGRID (**Avançado Atualização de Configuração de dispositivos**). Esta página permite que você use um arquivo para configurar vários dispositivos em grandes grades. Além disso, o `configure-sga.py` script Python foi atualizado para corresponder aos recursos do Instalador de appliance StorageGRID.

Saiba mais

- "Aparelhos de serviços SG100 SG1000"
- "SG6000 dispositivos de armazenamento"
- "SG5700 dispositivos de armazenamento"
- "SG5600 dispositivos de armazenamento"

Alterações nas mensagens de auditoria

- * Limpeza automática de objetos sobrescritos*: Anteriormente, os objetos que foram sobrescritos não foram removidos do disco em casos específicos, o que resultou em consumo adicional de espaço. Esses objetos sobrescritos, que são inacessíveis aos usuários, agora são removidos automaticamente para economizar espaço de armazenamento. Consulte a mensagem de auditoria da LKCU para obter mais informações.
- **Novos códigos de auditoria para bloqueio de objetos S3**: Quatro novos códigos de auditoria foram adicionados à mensagem de auditoria SPUT para incluir S3 bloqueio de objetoscabeçalhos de solicitação:
  - LKEN: Bloqueio de objetos ativado
  - LKLH: Bloqueio de objetos retenção legal
  - LKMD: Modo de retenção de bloqueio de objetos
  - LKRU: Data limite de retenção do bloqueio de objetos
- **Novos campos para o tempo da última modificação e tamanho do objeto anterior**: Agora você pode rastrear quando um objeto foi substituído, bem como o tamanho do objeto original.
  - O campo MTME (Last Modified Time) foi adicionado às seguintes mensagens de auditoria:
    - SDEL (S3 DELETE)
    - SPUT (S3 POSTOS)

        - WDEL (SWIFT DELETE)
        - WPUT (Swift PUT)
    - O campo CSIZ (tamanho do objeto anterior) foi adicionado à mensagem de auditoria OVWR (Object Overwrite).

Saiba mais

- "Rever registos de auditoria"

Novo arquivo nms.requestlog

Um novo arquivo de log, `/var/local/log/nms.requestlog`, é mantido em todos os nós de administração. Este arquivo contém informações sobre conexões de saída da API de gerenciamento para serviços internos do StorageGRID.

Saiba mais

- "Monitorizar Resolução de problemas"

Alterações na documentação do StorageGRID

- Para facilitar a localização das informações e requisitos de rede e esclarecer que as informações também se aplicam aos nós de dispositivos StorageGRID, a documentação de rede foi movida dos guias de instalação baseados em software (Ubuntu/Debian e VMware) para um novo guia de rede.

  "Diretrizes de rede"

- Para facilitar a localização de instruções e exemplos relacionados ao ILM, a documentação para gerenciar objetos com gerenciamento do ciclo de vida das informações foi movida do *Guia do Administrador* para um novo guia ILM.

  "Gerenciar objetos com ILM"

- Um novo guia do FabricPool fornece uma visão geral da configuração do StorageGRID como uma camada de nuvem do NetApp FabricPool e descreve as práticas recomendadas para configurar o ILM e outras opções do StorageGRID para um workload do FabricPool.

  "Configurar o StorageGRID para FabricPool"

- Agora você pode acessar vários vídeos instrucionais do Gerenciador de Grade. Os vídeos atuais fornecem instruções para gerenciar alertas, alertas personalizados, regras ILM e políticas ILM.

Recursos removidos ou obsoletos

Alguns recursos foram removidos ou obsoletos no StorageGRID 11,5. Você deve revisar esses itens para entender se você precisa atualizar aplicativos de cliente ou modificar sua configuração antes de atualizar.

Comando de consistência fraca removido

O controle de consistência fraca foi removido para o StorageGRID 11,5. Depois de atualizar, serão aplicados os seguintes comportamentos:

- As solicitações para definir consistência fraca para um bucket S3 ou Swift serão bem-sucedidas, mas o nível de consistência será definido como disponível.

- Os buckets e os contentores existentes que usam consistência fraca serão silenciosamente atualizados para usar a consistência disponível.
- As solicitações que têm um cabeçalho de controle de consistência fraco realmente usarão a consistência disponível, se aplicável.

O controle de consistência disponível comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações HEAD. O controle de consistência disponível oferece maior disponibilidade para OPERAÇÕES PRINCIPAIS do que "read-after-novo-write" se os nós de storage não estiverem disponíveis.

Alarme para integridade da grade obsoleta

A `/grid/health/topology` API, que verifica a existência de *alarmes* ativos em nós, está obsoleta. Em seu lugar, um novo `/grid/node-health` endpoint foi adicionado. Essa API retorna o status atual de cada nó verificando se há *alertas* ativos em nós.

Funcionalidade de conformidade obsoleta

O recurso bloqueio de objetos S3 no StorageGRID 11,5 substitui o recurso de conformidade que estava disponível nas versões anteriores do StorageGRID. Como o novo recurso de bloqueio de objetos do S3 está em conformidade com os requisitos do Amazon S3, ele deprecia o recurso proprietário de conformidade do StorageGRID, que agora é conhecido como ""conformidade legada"".

Se você ativou anteriormente a configuração de conformidade global, a nova configuração global de bloqueio de objetos S3 será ativada automaticamente quando você atualizar para o StorageGRID 11,5. Os usuários do locatário não poderão mais criar novos buckets com a conformidade habilitada no StorageGRID. No entanto, conforme necessário, os usuários do locatário podem continuar a usar e gerenciar quaisquer buckets em conformidade legados existentes.

No Gerenciador do Tenant, um ícone de escudo indica um bucket em conformidade com o legado. Buckets em conformidade com legado também podem ter um crachá de retenção HOLD para indicar que o bucket está sob um guarda legal.

"KB: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

"Gerenciar objetos com ILM"

Alerta "'S3 multipart too small" removido

O alerta **S3 multipart too small** foi removido. Anterior, esse alerta foi acionado se um cliente S3 tentou concluir um upload de várias partes com peças que não atenderam aos limites de tamanho do Amazon S3. Após a atualização para o StorageGRID 11,5, quaisquer solicitações de upload de várias partes que não atendam aos seguintes limites de tamanho falharão:

- 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 de peças grandes reduz a sobrecarga de metadados do StorageGRID.
- Para objetos menores que 5 GiB, considere usar upload não multipart.

Alertas de "ligação do dispositivo para baixo na rede de grelha" removidos

Os alertas a seguir foram removidos. Se a rede de Grade estiver inativa, as métricas que acionariam esses alertas não estarão acessíveis:

- Link do utilitário de serviços para baixo na rede de Grade
- Ligação do dispositivo de armazenamento na rede de grelha

Suporte para nome de domínio totalmente qualificado removido da configuração SNMP

Ao configurar um servidor SNMP no controlador de gerenciamento de placa base (BMC) para o SG6000, SG100 ou SG1000, agora você deve especificar um endereço IP em vez de um nome de domínio totalmente qualificado. Se um nome de domínio totalmente qualificado tiver sido configurado anteriormente, altere-o para um endereço IP antes de atualizar para o StorageGRID 11,5.

Atributos legados removidos

Os seguintes atributos legados foram removidos. Conforme aplicável, informações equivalentes são fornecidas pelas métricas Prometheus:

Atributo legado	Métrica equivalente Prometheus
BREC	StorageGRID_service_network_received_bytes
BTRA	StorageGRID_service_network_transmitted_bytes
CQST	StorageGRID_metadata_queries_average_latency_milésimos de segundo
HAIS	StorageGRID_http_sessions_incoming_tented
HCCS	StorageGRID_http_sessions_incoming_currently_established
IES	StorageGRID_http_sessions_incoming_failed
HISC	StorageGRID_http_sessions_incoming_successful
LHAC	*none*
NREC	*none*
NTSO (desvio da fonte de tempo escolhido)	StorageGRID_ntp_chosen_time_source_offset_milissegundos
NTRA	*none*
SLOD	StorageGRID_service_load
SMM	StorageGRID_service_memory_usage_bytes

Atributo legado	Métrica equivalente Prometheus
SUTM	StorageGRID_service_cpu_seconds
SVUT	StorageGRID_service_uptime_seconds
TRBS (total de bits por segundo recebidos)	*none*
TRXB	StorageGRID_network_received_bytes
TTBS (total de bits por segundo transmitidos)	*none*
TTXB	StorageGRID_network_transmitted_bytes

As seguintes alterações relacionadas também foram feitas:

- As `network_received_bytes` métricas e `network_transmitted_bytes` Prometheus foram alteradas de medidores para contadores porque os valores dessas métricas só aumentam. Se você estiver usando essas métricas atualmente em consultas Prometheus, você deve começar a usar a `increase()` função na consulta.
- A tabela recursos de rede foi removida da guia recursos para serviços do StorageGRID. (Selecione **Support Tools Grid Topology**.then, selecione ***node Service* Resources**.)
- A página sessões HTTP foi removida para nós de storage. Anteriormente, você poderia acessar esta página selecionando **Support Tools Grid Topology** e, em seguida, selecionando ***Storage Node* LDR HTTP**.
- O alarme DE HCCS (sessões de entrada atualmente estabelecidas) foi removido.
- O alarme NTSO (desvio da fonte de tempo escolhido) foi removido.

Alterações na API Grid Management

O StorageGRID 11,5 usa a versão 3 da API de gerenciamento de grade. A versão 3 desconsidera a versão 2; no entanto, a versão 1 e a versão 2 ainda são suportadas.

> Você pode continuar usando a versão 1 e a versão 2 da API de gerenciamento com o StorageGRID 11,5; no entanto, o suporte para essas versões da API será removido em uma versão futura do StorageGRID. Depois de atualizar para o StorageGRID 11,5, as APIs v1 e v2 obsoletas podem ser desativadas usando a `PUT /grid/config/management` API.

Nova seção de certificados de cliente

A nova seção `/grid/client-certificates` , permite configurar certificados de cliente para fornecer acesso seguro e autenticado ao banco de dados do StorageGRID Prometheus. Por exemplo, você pode monitorar o StorageGRID externamente usando o Grafana.

Endpoints de conformidade legados movidos para a nova seção S3-object-lock

Com a introdução do bloqueio de objetos do StorageGRID S3, as APIs usadas para gerenciar as configurações de conformidade legadas para a grade foram movidas para uma nova seção da interface de usuário do Swagger. A seção **S3-object-lock** inclui os dois `/grid/compliance-global` endpoints de API, que agora controlam a configuração global de bloqueio de objetos S3D. Os URIs de endpoint permanecem inalterados para compatibilidade com aplicativos existentes.

Terminal de contas Swift-admin-password removido

O seguinte endpoint de API de contas, que foi obsoleto no StorageGRID 10,4, agora foi removido:

```
https://<IP-Address>/api/v1/grid/accounts/<AccountID>/swift-admin-password
```

Nova seção de senhas de grade

A seção **Grid-passwords** permite operações para gerenciamento de senhas de grade. A seção inclui dois `/grid/change-provisioning-passphrase` endpoints de API. Os endpoints permitem que os usuários alterem a senha de provisionamento do StorageGRID e recuperem o status da alteração da senha.

Permissão de StorageAdmin adicionada à API Groups

A `/grid/groups` API agora inclui a permissão storageAdmin.

Novo parâmetro para a API de uso de armazenamento

A `GET /grid/accounts/{id}/usage` API agora tem um `strictConsistency` parâmetro. Para impor uma consistência global forte ao recuperar informações de uso de storage entre nós de storage, defina este parâmetro como `true`. Quando esse parâmetro é definido como `false` (padrão), o StorageGRID tenta recuperar informações de uso usando consistência global forte, mas volta para consistência de site forte se a consistência global forte não puder ser atendida.

Nova API de integridade do nó

Um novo `/grid/node-health` endpoint foi adicionado. Essa API retorna o status atual de cada nó verificando se há *alertas* ativos nos nós. A `/grid/health/topology` API, que verifica a existência de *alarmes* ativos em nós, está obsoleta.

Altere para ID da regra de alerta "ApplianceStorageShelvesPowerSupplyDegraded"

O ID da regra de alerta "ApplianceStorageShelvesPowerSupplyDegraded" foi renomeado para "ApplianceStorageShelvesDegraded" para refletir melhor o comportamento real do alerta.

Informações relacionadas

"Administrar o StorageGRID"

Alterações na API de gerenciamento do locatário

O StorageGRID 11,5 usa a versão 3 da API de gerenciamento do locatário. A versão 3 desconsidera a versão 2; no entanto, a versão 1 e a versão 2 ainda são suportadas.

Você pode continuar usando a versão 1 e a versão 2 da API de gerenciamento com o StorageGRID 11,5; no entanto, o suporte para essas versões da API será removido em uma versão futura do StorageGRID. Depois de atualizar para o StorageGRID 11,5, as APIs v1 e v2 obsoletas podem ser desativadas usando a `PUT /grid/config/management` API.

Novo parâmetro para API de uso de armazenamento de locatário

A `GET /org/usage` API agora tem um `strictConsistency` parâmetro. Para impor uma consistência global forte ao recuperar informações de uso de storage entre nós de storage, defina este parâmetro como `true`. Quando esse parâmetro é definido como `false` (padrão), o StorageGRID tenta recuperar informações de uso usando consistência global forte, mas volta para consistência de site forte se a consistência global forte não puder ser atendida.

Informações relacionadas

"Use S3"

"Use uma conta de locatário"

Planejamento e preparação de atualização

Você deve Planejar a atualização do seu sistema StorageGRID para garantir que o sistema esteja pronto para a atualização e que a atualização possa ser concluída com interrupção mínima.

Passos

1. "Estimando o tempo para concluir uma atualização"
2. "Como seu sistema é afetado durante a atualização"
3. "Impacto de uma atualização em grupos e contas de usuários"
4. "Verificando a versão instalada do StorageGRID"
5. "Obtenção dos materiais necessários para uma atualização de software"
6. "Transferir os ficheiros de atualização do StorageGRID"
7. "Transferir o pacote de recuperação"
8. "Verificar o estado do sistema antes de atualizar o software"

Estimando o tempo para concluir uma atualização

Ao Planejar uma atualização para o StorageGRID 11,5, você deve considerar quando atualizar, com base em quanto tempo a atualização pode demorar. Você também deve estar 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.

Durante a atualização do StorageGRID 11,4 para o 11,5, as tabelas do banco de dados Cassandra nos nós de armazenamento serão atualizadas. A tarefa **Atualizar banco de dados** ocorre em segundo plano, mas pode exigir uma grande quantidade de tempo para ser concluída. Enquanto o banco de dados está sendo atualizado, você pode usar com segurança novos recursos, aplicar hotfixes e executar operações de recuperação de nó. No entanto, poderá ser impedido de executar outros procedimentos de manutenção.

Se uma expansão for urgentemente necessária, execute a expansão antes de atualizar para 11,5.

Tarefa de atualização	Descrição	Tempo aproximado necessário	Durante esta tarefa
Inicie o serviço de atualização	As pré-verificações de atualização são executadas, o arquivo de software é distribuído e o serviço de atualização é iniciado.	3 minutos por nó de grade, a menos que erros de validação sejam relatados	Conforme necessário, você pode executar as pré-verificações de atualização manualmente antes da janela de manutenção de atualização agendada.
Atualizar nós de grade (nó de administração principal)	O nó Admin principal é interrompido, atualizado e reiniciado.	Até 30 minutos	Não é possível acessar o nó de administração principal. Os erros de conexão são relatados, o que você pode ignorar.
Atualizar nós de grade (todos os outros nós)	O software em todos os outros nós de grade é atualizado, na ordem em que você aprova os nós. Cada nó no seu sistema será reduzido um de cada vez por vários minutos cada.	De 15 a 45 minutos por nó, com os nós de storage 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. • Não execute outro procedimento de manutenção, como hotfix, desativação ou expansão. **Observação:** se você precisar executar um procedimento de recuperação, entre em Contato com o suporte técnico.

Tarefa de atualização	Descrição	Tempo aproximado necessário	Durante esta tarefa
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 execute outro procedimento de manutenção.
Atualizar base de dados	As tabelas de banco de dados Cassandra, que existem em todos os nós de storage, são atualizadas.	Horas ou dias, com base na quantidade de metadados em seu sistema	Durante a tarefa **Upgrade Database**, a grade atualizada funcionará normalmente; no entanto, a atualização ainda estará em andamento. Durante esta tarefa, você pode: • Use os novos recursos na nova versão do StorageGRID. • Alterar a configuração do nível de auditoria. • Atualize a configuração do ILM. • Aplique um hotfix. • Recuperar um nó. **Observação:** você não pode executar um procedimento de desativação ou expansão até que as **etapas de atualização final** sejam concluídas.
Etapas finais da atualização	Os arquivos temporários são removidos e a atualização para a nova versão é concluída.	5 minutos	Quando a tarefa **etapas de atualização final** for concluída, você poderá executar todos os procedimentos de manutenção.

Passos

1. Estime o tempo necessário para atualizar todos os nós de grade (considere todas as tarefas de atualização, exceto **Upgrade Database**).
   a. Multiplique o número de nós em seu sistema StorageGRID por 30 minutos/nó (média).
   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. Estime o tempo necessário para atualizar o banco de dados.
   a. No Gerenciador de Grade, selecione **nós**.
   b. Selecione a primeira entrada na árvore (grade inteira) e selecione a guia **armazenamento**.
   c. Passe o cursor sobre o gráfico **armazenamento usado - metadados de objetos** e localize o valor **usado**, que indica quantos bytes de metadados de objetos estão em sua grade.
   d. Divida o valor **usado** por 1,5 TB/dia para determinar quantos dias serão necessários para atualizar o banco de dados.
4. Calcule o tempo total estimado para a atualização adicionando os resultados das etapas 1, 2 e 3.

Exemplo: Estimando o tempo de atualização do StorageGRID 11,4 para o 11,5

Suponha que seu sistema tenha 14 nós de grade, dos quais 8 são nós de Linux. Além disso, suponha que o valor **usado** para metadados de objetos é de 6 TB.

1. Multiplique 14 por 30 minutos/nó e adicione 1 hora. O tempo estimado para atualizar todos os nós é de 8 horas.
2. Vários 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.
3. Divida 6 por 1,5 TB/dia. O número estimado de dias para a tarefa **Upgrade Database** é de 4 dias.

> Enquanto a tarefa **Upgrade Database** está em execução, você pode usar com segurança novos recursos, aplicar hotfixes e executar operações de recuperação de nó.

4. Adicione os valores juntos. Você deve permitir 5 dias para concluir a atualização do seu sistema para o StorageGRID 11,5.0.

Como seu sistema é afetado durante a atualização

Você deve entender 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. Os nós de grade são derrubados um de cada vez durante a atualização, portanto, não há um momento em que todos os nós de grade estão indisponíveis.

Para permitir disponibilidade contínua, você deve garantir que os objetos sejam armazenados de forma redundante usando as políticas de ILM apropriadas. Você também deve garantir que todos os clientes externos S3 ou Swift estejam configurados para enviar solicitações para um dos seguintes:

- Um endpoint StorageGRID configurado como um 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

O firmware do dispositivo foi atualizado

Durante a atualização do StorageGRID 11,5:

- Todos os nós do dispositivo StorageGRID são atualizados automaticamente para a versão 3,5 do firmware do instalador do StorageGRID Appliance.
- Os dispositivos SG6060 e SGF6024 são atualizados automaticamente para a versão 3B03.EX do firmware do BIOS e para a versão do firmware do BMC BMC 3.90.07.
- Os dispositivos SG100 e SG1000 são atualizados automaticamente para a versão 3B08.EC do firmware do BIOS e para a versão 4.64.07 do firmware do BMC.

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). 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 11,5, mas outros nós ainda estão executando o StorageGRID 11,4.

Em geral, esses alertas serão apagados quando a atualização for concluída.

Após a conclusão da atualização, você pode revisar qualquer alerta relacionado a atualização selecionando **alertas resolvidos recentemente** no Painel do Gerenciador de Grade.

> Durante a atualização para o StorageGRID 11,5, o alerta **posicionamento ILM inalcançável** pode ser acionado quando os nós de storage são interrompidos. Este alerta pode persistir por 1 dia após a atualização ser concluída com sucesso.

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

Até que a tarefa **Ativar novo recurso** seja concluída:

- Não faça alterações na configuração da grade.
- Não altere a configuração do nível de auditoria.
- 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.

Até que a tarefa **etapas de atualização final** seja concluída:

- Não execute um procedimento de expansão.
- Não efetue um procedimento de desativação.

Impacto de uma atualização em grupos e contas de usuários

Você deve entender o impactos da atualização do StorageGRID para que possa atualizar grupos e contas de usuário adequadamente após a conclusão da atualização.

Alterações nas permissões e opções de grupo

Depois de atualizar para o StorageGRID 11,5, opcionalmente selecione as novas permissões e opções a seguir (**Configuração Controle de Acesso grupos de administradores**).

Permissão ou opção	Descrição
Administrador do dispositivo de armazenamento	Necessário para acessar a interface de usuário do Gerenciador de sistema do SANtricity a partir do Gerenciador de Grade.
Modo de acesso	Ao gerenciar grupos, você pode selecionar **somente leitura** para esta nova opção para impedir que os usuários alterem as configurações e os recursos selecionados para o grupo. Os usuários em grupos com modo de acesso somente leitura podem exibir as configurações, mas não podem alterá-las.

Informações relacionadas

"Administrar o StorageGRID"

Verificando a versão instalada do StorageGRID

Antes de iniciar a atualização, tem de verificar se a versão anterior do StorageGRID está atualmente instalada com a correção disponível mais recente aplicada.

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. Selecione **Ajuda sobre**.
3. Verifique se a **versão** é 11,4.*x*.*y*.

   No número da versão do StorageGRID 11,4.*x*.*y*:

   - A versão principal tem um valor *x* de 0 (11,4.0).
   - Uma versão menor, se disponível, tem um valor *x* diferente de 0 (por exemplo, 11,4.1).
   - Um hotfix, se disponível, tem um valor *y* (por exemplo, 11,4.0,1).

   > Se você tiver uma versão anterior do StorageGRID, você deve atualizar para qualquer versão 11,4 antes de atualizar para o StorageGRID 11,5. Você não precisa estar na versão menor mais alta 11,4 para atualizar para o StorageGRID 11,5.

4. Se você não estiver em uma versão do StorageGRID 11,4, você deve atualizar para a versão 11,4, uma versão de cada vez, usando as instruções para cada versão.

   Você também deve aplicar o hotfix mais recente para cada versão do StorageGRID antes de atualizar para o próximo nível.

   Um possível caminho de atualização é mostrado no exemplo.

5. Quando estiver no StorageGRID 11,4, vá para a página de downloads do NetApp para StorageGRID e veja se há hotfixes disponíveis para a versão do StorageGRID 11,4.*x*.

   "NetApp Downloads: StorageGRID"

6. Verifique se a versão do StorageGRID 11,4.*x* tem a correção mais recente aplicada.
7. Se necessário, baixe e aplique o hotfix StorageGRID 11,4.*x.y* mais recente para sua versão do StorageGRID 11,4.*x*.

   Consulte as instruções de recuperação e manutenção para obter informações sobre a aplicação de hotfixes.

Exemplo: Preparando a atualização para o StorageGRID 11,5 a partir da versão 11.3.0.8

O exemplo a seguir mostra as etapas de atualização para se preparar para uma atualização do StorageGRID versão 11.3.0.8 para a versão 11,5. Antes de poder atualizar para o StorageGRID 11,5, o sistema tem de ter uma versão do StorageGRID 11,4 instalada com a correção mais recente.

Transfira e instale o software na seguinte sequência para preparar o seu sistema para a atualização:

1. Aplique o hotfix do StorageGRID 11,3.0.*y* mais recente.
2. Atualize para a versão principal do StorageGRID 11.4.0. (Você não precisa instalar nenhuma versão menor do 11,4.*x*.)
3. Aplique o hotfix do StorageGRID 11,4.0.*y* mais recente.

Informações relacionadas

"Administrar o StorageGRID"

"Manter recuperar"

Obtenção dos materiais necessários para uma atualização de software

Antes de iniciar a atualização de software, você deve obter todos os materiais necessários para que você possa concluir a atualização com sucesso.

Item	Notas
Ficheiros de atualização do StorageGRID	Você deve baixar os arquivos necessários para o seu laptop de serviço: • **Todas as plataformas**: `.upgrade` Arquivo • * Qualquer nó no Red Hat Enterprise Linux ou CentOS*: `.upgrade` Arquivo e arquivo RPM (`.zip`ou `.tgz`) • * Qualquer nó no Ubuntu ou Debian*: `.upgrade` Arquivo e arquivo DEB (`.zip`ou `.tgz`)
Serviço de laptop	O computador portátil de serviço deve ter: • Porta de rede • Cliente SSH (por exemplo, PuTTY)
Navegador da Web suportado	Você deve confirmar que o navegador da Web no laptop de serviço é compatível para uso com o StorageGRID 11,5. "Requisitos do navegador da Web" **Observação:** o suporte ao navegador foi alterado para o StorageGRID 11,5. Confirme que está a utilizar uma versão suportada.
Pacote de recuperação (`.zip`) arquivo	Antes de atualizar, você deve baixar o arquivo mais recente do pacote de recuperação, caso ocorram problemas durante a atualização. Depois de atualizar o nó de administração principal, você deve baixar uma nova cópia do arquivo do pacote de recuperação e salvá-lo em um local seguro. O arquivo atualizado do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha. "Transferir o pacote de recuperação"
`Passwords.txt` ficheiro	Este arquivo está incluído no REFERIDO pacote, que faz parte do arquivo do Pacote de recuperação `.zip`. Você deve obter a versão mais recente do 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 listada no `Passwords.txt` arquivo.
Documentação relacionada	• Notas de versão para StorageGRID 11,5. Certifique-se de lê-las cuidadosamente antes de iniciar a atualização. • Instruções para administrar o StorageGRID • Se você estiver atualizando uma implantação Linux, as instruções de instalação do StorageGRID para sua plataforma Linux. • Outra documentação do StorageGRID, conforme necessário.

Informações relacionadas

"Requisitos do navegador da Web"

"Administrar o StorageGRID"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Transferir os ficheiros de atualização do StorageGRID"

"Transferir o pacote de recuperação"

"Notas de lançamento"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Transferir os ficheiros de atualização do StorageGRID

Você deve baixar os arquivos necessários para um laptop de serviço antes de atualizar seu sistema StorageGRID.

O que você vai precisar

Você deve ter instalado todos os hotfixes necessários para a versão do software StorageGRID que você está atualizando. Consulte o procedimento de correção nas instruções de recuperação e manutenção.

Sobre esta tarefa

Você deve baixar o `.upgrade` arquivo para qualquer plataforma. Se algum nó for implantado em hosts Linux, você também deve baixar um arquivo RPM ou DEB, que será instalado antes de iniciar a atualização.

Passos

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

   "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 aparecer uma instrução Caution/MustRead, leia-a e marque a caixa de seleção.

   Esta instrução aparece se houver um hotfix necessário para a versão.

5. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.

   É apresentada a página de transferências para a versão selecionada. A página contém três colunas:

   - Instale o StorageGRID
   - Atualize o StorageGRID
   - Arquivos de suporte para dispositivos StorageGRID

6. Na coluna **Upgrade StorageGRID**, selecione e baixe o `.upgrade` arquivo.

   Cada plataforma requer o `.upgrade` arquivo.

7. Se algum nó for implantado em hosts Linux, baixe também o arquivo RPM ou DEB em qualquer `.tgz` formato ou `.zip`.

   Você deve instalar o arquivo RPM ou DEB em todos os nós do Linux antes de iniciar a atualização.

   > Não são necessários ficheiros adicionais para o SG100 ou SG1000.

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

   - Red Hat Enterprise Linux ou CentOS
     `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`

Informações relacionadas

"Linux: Instalando o pacote RPM ou DEB em todos os hosts"

"Manter recuperar"

Transferir o pacote de recuperação

O arquivo do pacote de recuperação permite restaurar o sistema StorageGRID se ocorrer uma falha.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a senha de provisionamento.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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 **Manutenção** > **sistema** > **Pacote de recuperação**.
2. Digite a senha de provisionamento e selecione **Iniciar download**.

   O download começa imediatamente.

3. Quando o download for concluído:
   a. Abra o `.zip` ficheiro.
   b. Confirme que inclui um `gpt-backup` diretório e um arquivo interno `.zip`.
   c. Extraia o arquivo interno `.zip`.
   d. Confirme que você pode abrir o `Passwords.txt` arquivo.
4. Copie o arquivo do pacote de recuperação baixado (`.zip`) para dois locais seguros, seguros e separados.

> O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Verificar o estado do sistema antes de atualizar o software

Antes de atualizar um sistema StorageGRID, você deve verificar se o sistema está pronto para acomodar a atualização. Você deve garantir que o sistema esteja funcionando normalmente e que todos os nós de grade estejam operacionais.

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. Verifique e resolva quaisquer alertas ativos.

   Para obter informações sobre alertas específicos, consulte as instruções de monitoramento e solução de problemas.

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. Consulte as listas de portas internas e externas na versão 11,5 das diretrizes de rede e certifique-se de que todas as portas necessárias sejam abertas antes de atualizar.

   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.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Administrar o StorageGRID"

"Manter recuperar"

"Diretrizes de rede"

Realizar a atualização

A página Atualização de Software orienta você pelo processo de upload do arquivo necessário e atualização de todos os nós de grade em seu sistema StorageGRID.

O que você vai precisar

Você está ciente do seguinte:

- É necessário atualizar todos os nós de grade para todos os locais de data center a partir do nó Admin principal, usando o Gerenciador de Grade.
- Para detetar e resolver problemas, você pode executar manualmente as pré-verificações de atualização antes de iniciar a atualização real. As mesmas pré-verificações são realizadas quando você inicia a atualização. As falhas de pré-verificação interromperão o processo de atualização e poderão exigir o envolvimento do suporte técnico para serem resolvidas.
- Quando você inicia a atualização, o nó de administração principal é atualizado automaticamente.
- Depois que o nó Admin principal tiver sido atualizado, você pode selecionar quais nós de grade atualizar em seguida.
- É necessário atualizar todos os nós de grade em seu sistema StorageGRID para concluir a atualização, mas você pode atualizar nós de grade individuais em qualquer ordem. Você pode selecionar nós de grade individuais, grupos de nós de grade ou todos os nós de grade. Você pode repetir o processo de seleção de nós de grade quantas vezes for necessário, até que todos os nós de grade em todos os locais sejam

atualizados.

- Quando a atualização começa em um nó de grade, os serviços nesse nó são interrompidos. Mais tarde, o nó de grade é reinicializado. 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.
- Quando todos os nós de grade tiverem sido atualizados, novos recursos serão ativados e você poderá retomar as operações; no entanto, você deve esperar para executar um procedimento de desativação ou expansão até que a tarefa de segundo plano **Atualizar banco de dados** e a tarefa **etapas de atualização final** tenham sido concluídas.
- Você deve concluir a atualização na mesma plataforma de hipervisor com a qual você começou.

Passos

1. "Linux: Instalando o pacote RPM ou DEB em todos os hosts"
2. "Iniciar a atualização"
3. "Atualizando nós de grade e completando a atualização"
4. "Aumentando a configuração espaço reservado metadados"

Informações relacionadas

"Administrar o StorageGRID"

"Estimando o tempo para concluir uma atualização"

Linux: Instalando o pacote RPM ou DEB em todos os hosts

Se algum nó StorageGRID for implantado em hosts Linux, você deverá instalar um pacote RPM ou DEB adicional em cada um desses hosts antes de iniciar a atualização.

O que você vai precisar

Você deve ter baixado um dos arquivos a seguir `.tgz` ou `.zip` da página de downloads do NetApp para o StorageGRID.

Use o `.zip` arquivo se você estiver executando o Windows no laptop de serviço.

Plataforma Linux	Arquivo adicional (escolha um)
Red Hat Enterprise Linux ou CentOS	• `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`

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 da sua plataforma Linux.

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Os novos pacotes são instalados como pacotes adicionais. Não remova os pacotes existentes.

Iniciar a atualização

Quando estiver pronto para executar a atualização, selecione o ficheiro transferido e introduza a frase-passe de aprovisionamento. Como opção, você pode executar as pré-verificações de atualização antes de executar a atualização real.

O que você vai precisar

Você revisou todas as considerações e concluiu todas as etapas em "Planejamento e preparação de atualização".

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. Selecione **Manutenção** > **sistema** > **Atualização de Software**.

   A página Atualização de software é exibida.

3. Selecione **Atualização StorageGRID**.

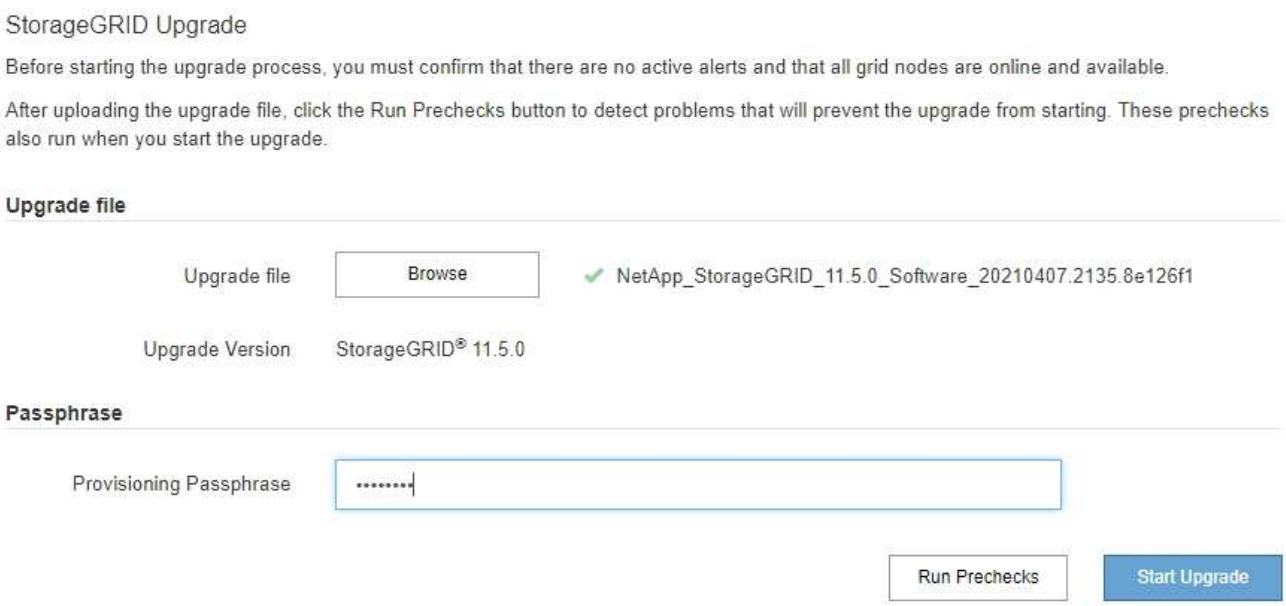
   A página Atualização do StorageGRID é exibida e mostra a data e a hora da atualização mais recente concluída, a menos que o nó de administração principal tenha sido reiniciado ou a API de gerenciamento seja reiniciada desde que a atualização foi realizada.

4. Selecione o `.upgrade` ficheiro que transferiu.
   a. Selecione **Procurar**.
   b. Localize e selecione o arquivo: `NetApp_StorageGRID_version_Software_uniqueID.upgrade`
   c. Selecione **Open**.

      O arquivo é carregado e validado. Quando o processo de validação for concluído, uma marca de seleção verde aparece ao lado do nome do arquivo de atualização.

5. Insira a senha de provisionamento na caixa de texto.

   Os botões **Run Prechecks** e **Start Upgrade** ficam ativados.



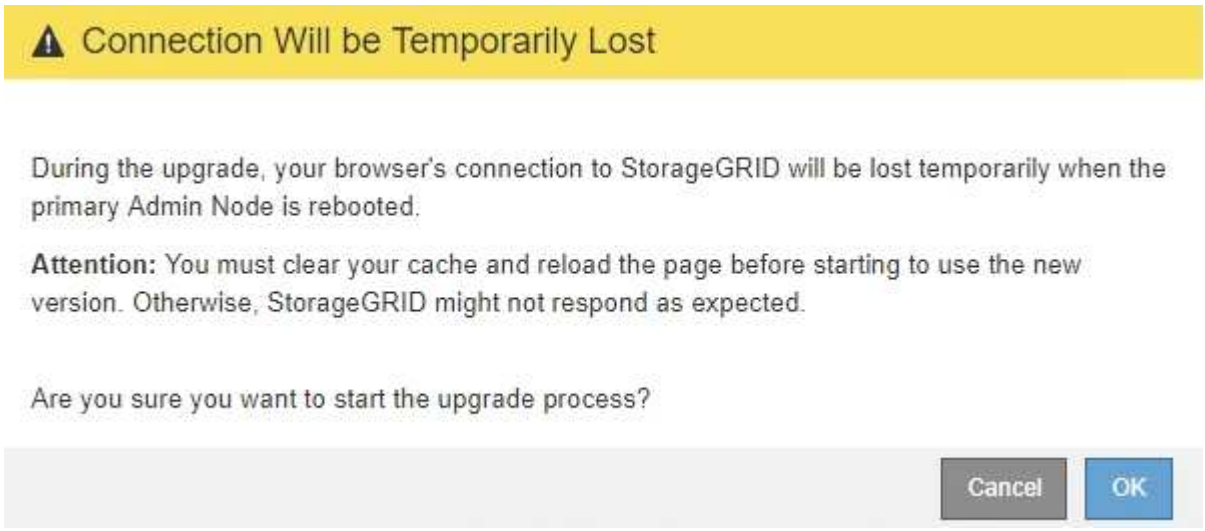
6. Se pretender validar a condição do seu sistema antes de iniciar a atualização real, selecione **Executar pré-verificações**. Em seguida, resolva quaisquer erros de pré-verificação que sejam relatados.

> 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.

> As mesmas pré-verificações são realizadas quando você seleciona **Iniciar atualização**. Selecionar **Executar pré-verificações** permite detetar e resolver problemas antes de iniciar a atualização.

7. Quando estiver pronto para executar a atualização, selecione **Iniciar atualização**.

   Um aviso aparece para lembrá-lo de que a conexão do seu navegador será perdida quando o nó Admin principal for reiniciado. Quando o nó de administração principal estiver disponível novamente, você precisa limpar o cache do navegador da Web e recarregar a página Atualização de software.



8. Selecione **OK** para confirmar o aviso e iniciar o processo de atualização.

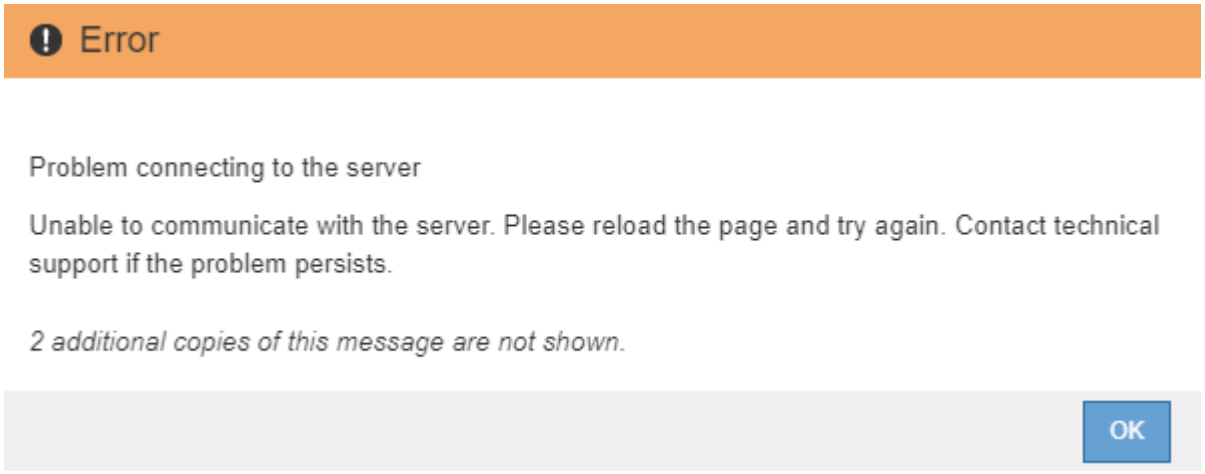
Quando a atualização é iniciada:

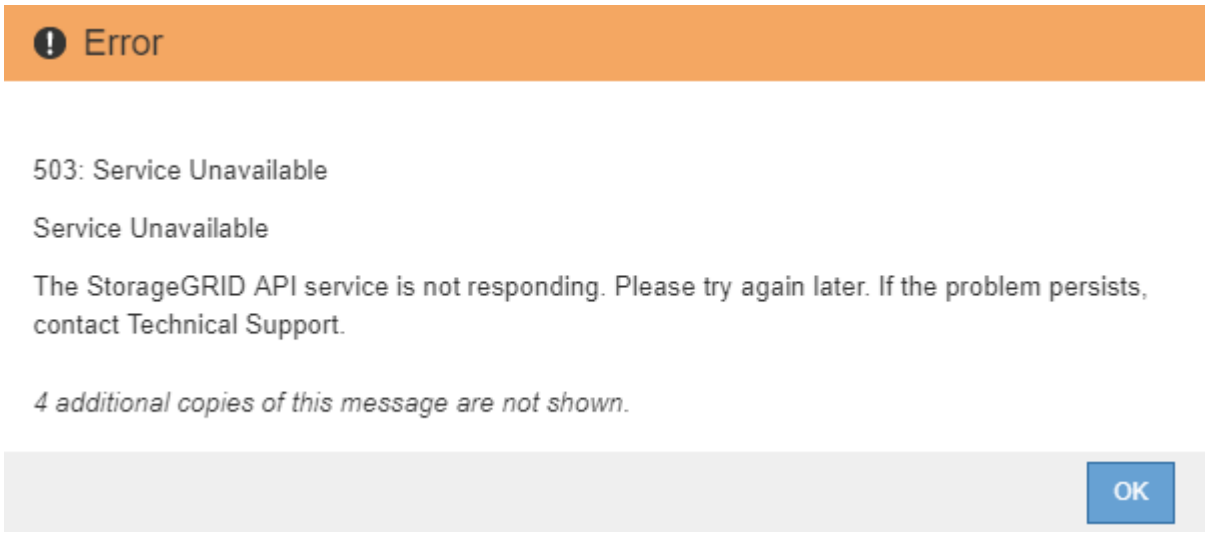
a. As pré-verificações de atualização são executadas.

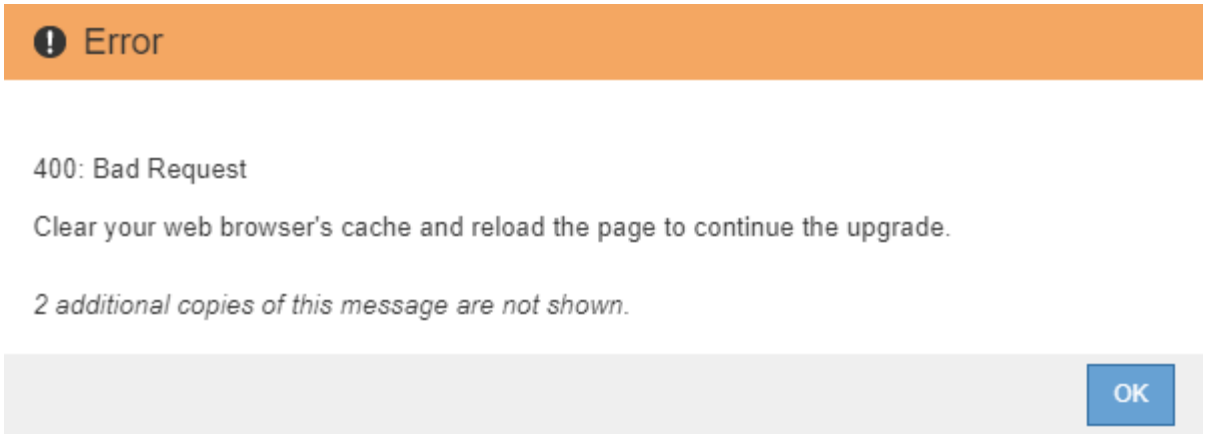
> Se algum erro de pré-verificação for relatado, resolva-os e selecione **Iniciar atualização** novamente.

b. O nó de administração principal é atualizado, o que inclui parar serviços, atualizar o software e reiniciar serviços. Você não poderá 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.

> Enquanto o nó Admin principal está sendo atualizado, várias cópias das seguintes mensagens de erro aparecem, que você pode ignorar.







9. Depois que o nó Admin principal tiver sido atualizado, limpe o cache do navegador da Web, inicie sessão novamente e recarregue a página Atualização de Software.

   Para obter instruções, consulte a documentação do navegador da Web.

   > Você deve limpar o cache do navegador da Web para remover recursos desatualizados usados pela versão anterior do software.

Informações relacionadas

"Planejamento e preparação de atualização"

Atualizando nós de grade e completando a atualização

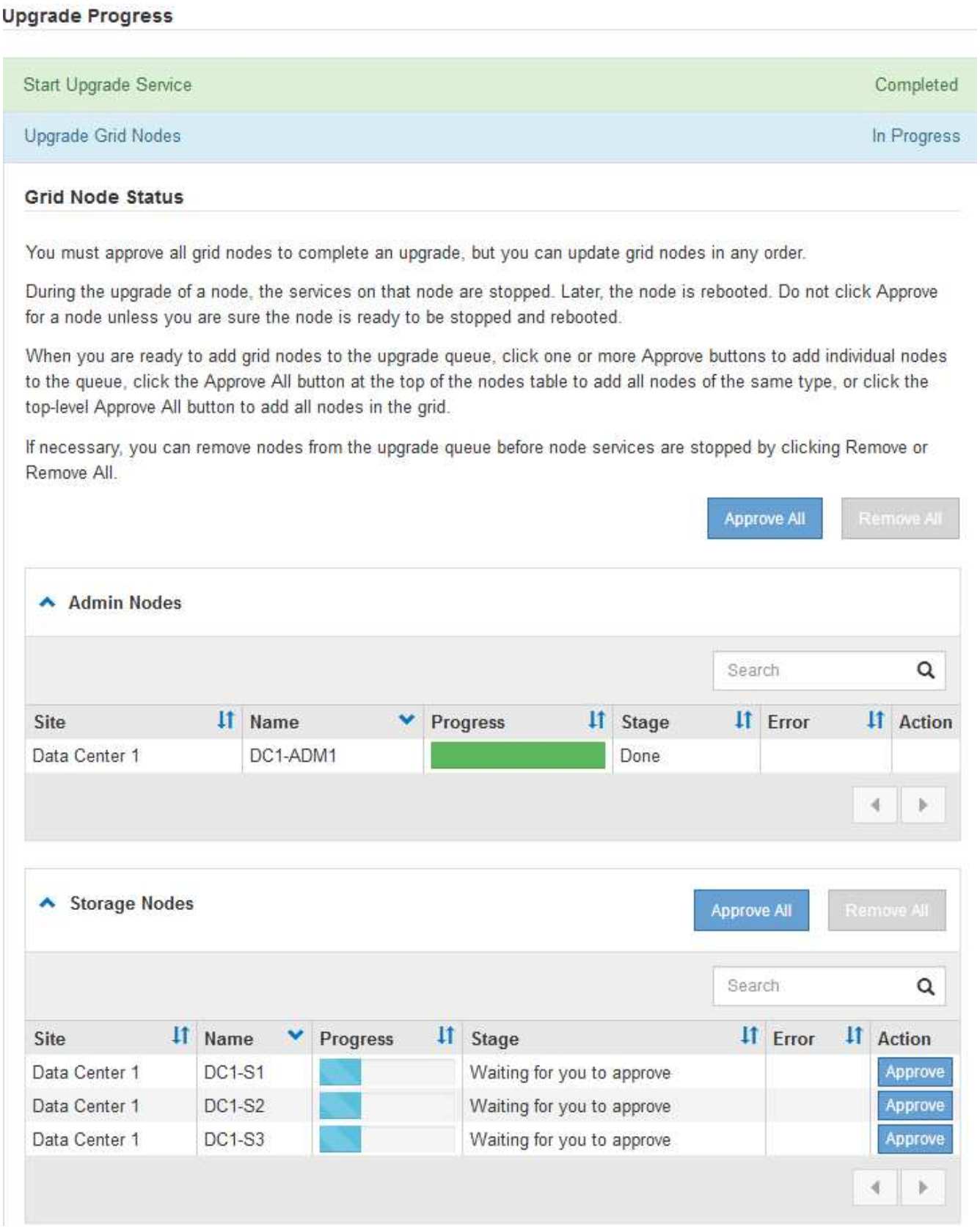
Depois que o nó de administração principal tiver sido atualizado, você deve atualizar todos os outros nós de grade em seu sistema StorageGRID. Você pode personalizar a sequência de atualização selecionando para atualizar nós de grade individuais, grupos de nós de grade ou todos os nós de grade.

Passos

1. Revise a seção progresso da atualização na página Atualização de software, que fornece informações sobre cada tarefa de atualização principal.
   a. **Start Upgrade Service** 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.
   b. Quando a tarefa **Start Upgrade Service** estiver concluída, a tarefa **Upgrade Grid Nodes** será iniciada.
   c. Enquanto a tarefa **Upgrade Grid Nodes** está em andamento, a tabela Grid Node Status (Status do nó de grade) é exibida e mostra a etapa de atualização para cada nó de grade em seu sistema.
2. Depois que os nós de grade aparecerem na tabela Status do nó de grade, mas antes de aprovar qualquer nó de grade, faça o download de uma nova cópia do Pacote de recuperação.

   > Você deve baixar uma nova cópia do arquivo do pacote de recuperação depois de atualizar a versão do software no nó de administração principal. O arquivo do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.

3. Revise as informações na tabela Status do nó de grade. Os nós de grade são organizados em seções por tipo: Nós de administrador, nós de gateway de API, nós de storage e nós de arquivamento.



Um nó de grade pode estar em um desses estágios quando esta página aparecer pela primeira vez:

- Concluído (somente nó de administração principal)
- A preparar a atualização

- Transferência de software na fila
- A transferir
- A aguardar aprovação

4. Aprove os nós de grade que você está pronto para adicionar à fila de atualização. Nós aprovados do mesmo tipo são atualizados um de cada vez.

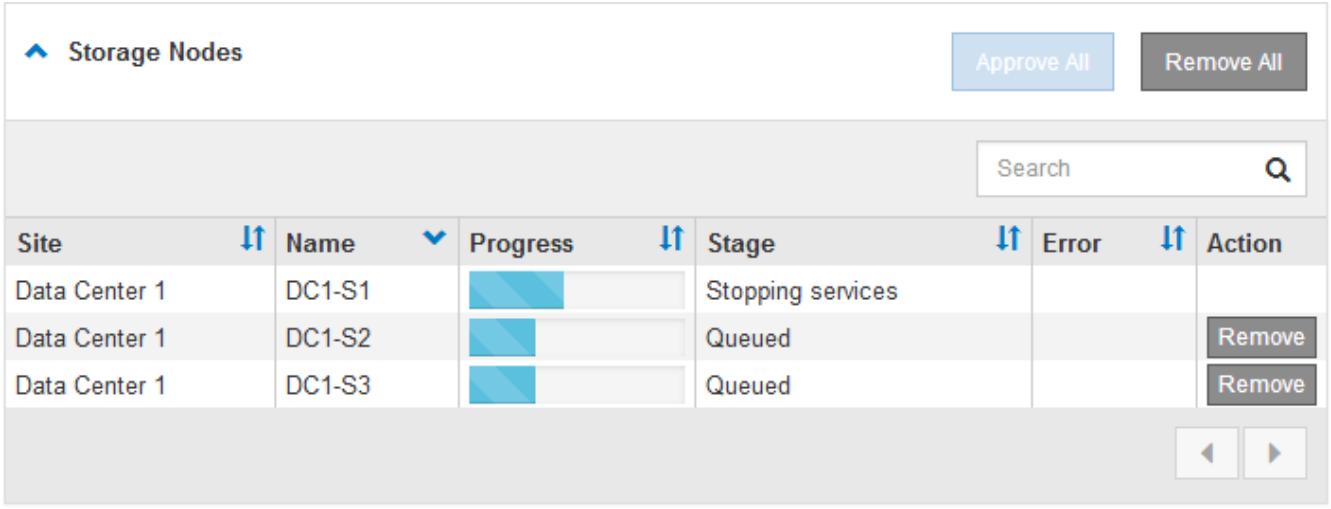
   Se a ordem em que os nós são atualizados for importante, aprove nós ou grupos de nós um de cada vez e aguarde até que a atualização seja concluída em cada nó antes de aprovar o próximo nó ou grupo de nós.

   > Quando a atualização começa em um nó de grade, os serviços nesse nó são interrompidos. Mais tarde, o nó de grade é reinicializado. Essas operações podem causar interrupções de serviço para 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.

   - Selecione um ou mais botões **Approve** para adicionar um ou mais nós individuais à fila de atualização.
   - Selecione o botão **Approve All** em cada seção para adicionar todos os nós do mesmo tipo à fila de atualização.
   - Selecione o botão de nível superior **Approve All** para adicionar todos os nós na grade à fila de atualização.

5. Se precisar remover um nó ou todos os nós da fila de atualização, selecione **Remover** ou **Remover tudo**.

   Como mostrado no exemplo, quando o Stage atinge **parando serviços**, o botão **Remover** fica oculto e você não pode mais remover o nó.



6. Aguarde que cada nó prossiga pelos estágios de atualização, que incluem fila de espera, parada de serviços, parada de contentor, limpeza de imagens do Docker, atualização de pacotes base do SO, reinicialização e inicialização de serviços.

   > Quando um nó de appliance atinge a fase de atualização dos pacotes base do SO, 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.

Quando todos os nós da grade tiverem sido atualizados, a tarefa **Atualizar nós da grade** é mostrada como concluída. As restantes tarefas de atualização são executadas automaticamente e em segundo plano.

7. Assim que a tarefa **Ativar recursos** estiver concluída (o que ocorre rapidamente), você pode começar a usar os novos recursos na versão atualizada do StorageGRID.

   Por exemplo, se você estiver atualizando para o StorageGRID 11,5, agora poderá ativar o bloqueio de objetos S3, configurar um servidor de gerenciamento de chaves ou aumentar a configuração espaço reservado de metadados.

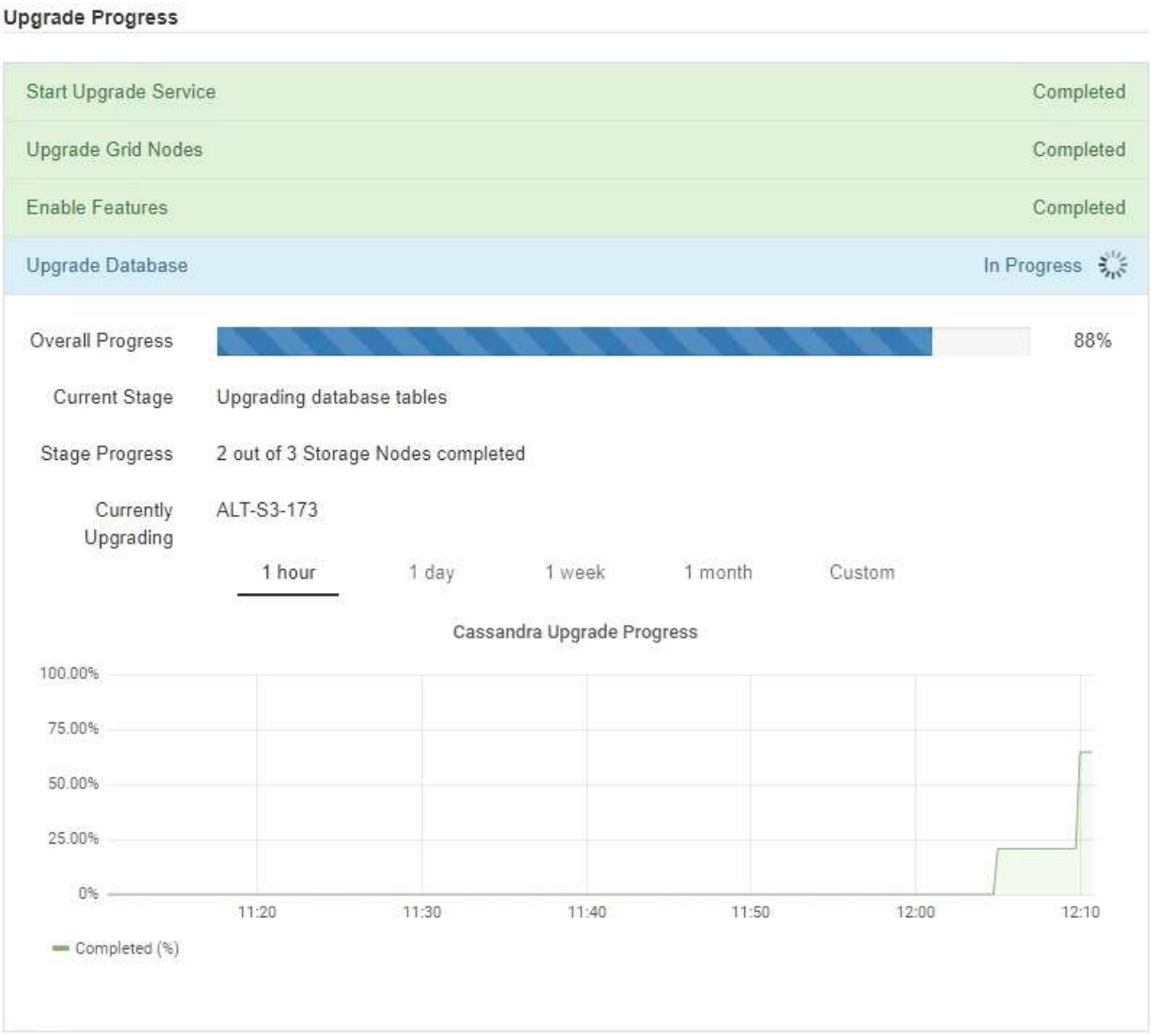
   "Aumentando a configuração espaço reservado metadados"

8. Monitorize periodicamente o progresso da tarefa **Atualizar base de dados**.

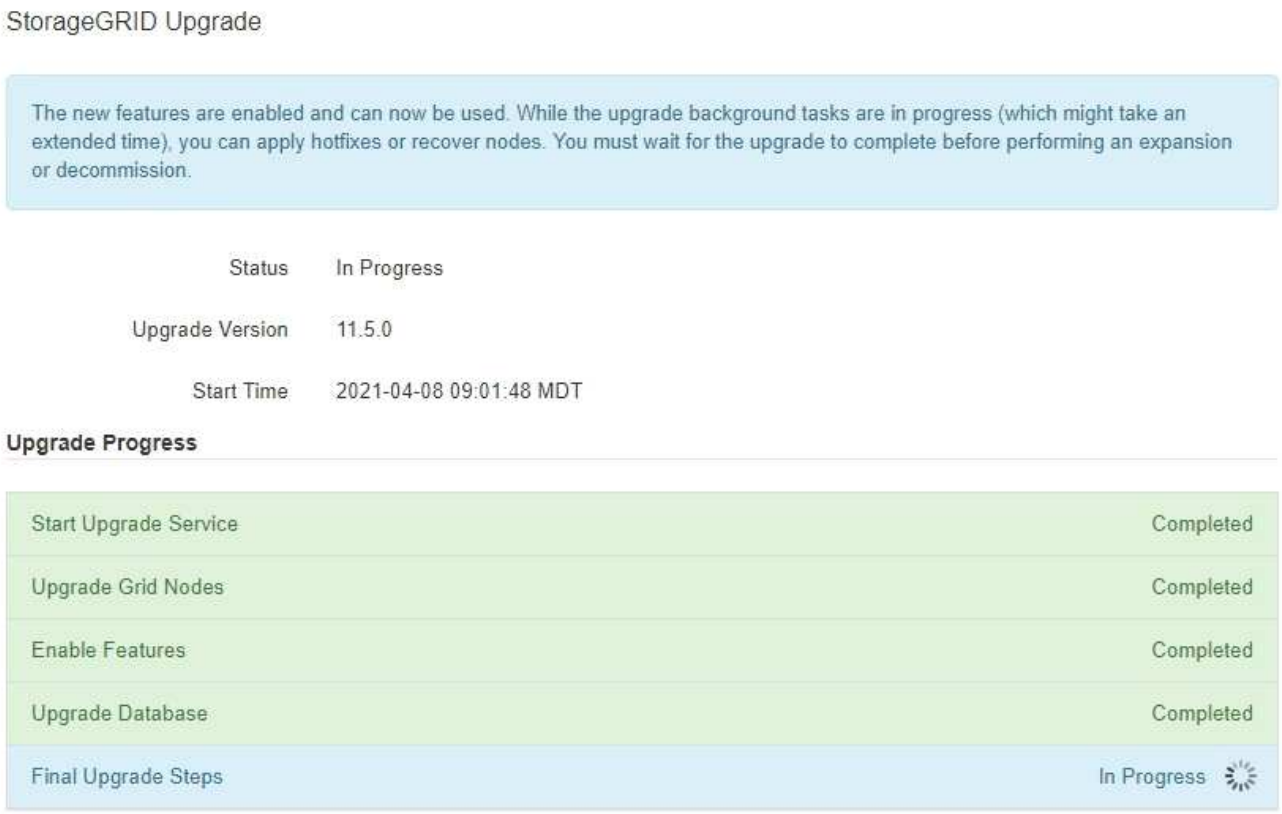
   Durante esta tarefa, o banco de dados Cassandra é atualizado em cada nó de armazenamento.

   > A tarefa **Upgrade Database** pode levar dias para ser concluída. À medida que esta tarefa em segundo plano é executada, você pode aplicar hotfixes ou recuperar nós. No entanto, você deve esperar que a tarefa **etapas de atualização final** seja concluída antes de executar um procedimento de expansão ou desativação.

   Pode rever o gráfico para monitorizar o progresso de cada nó de armazenamento.

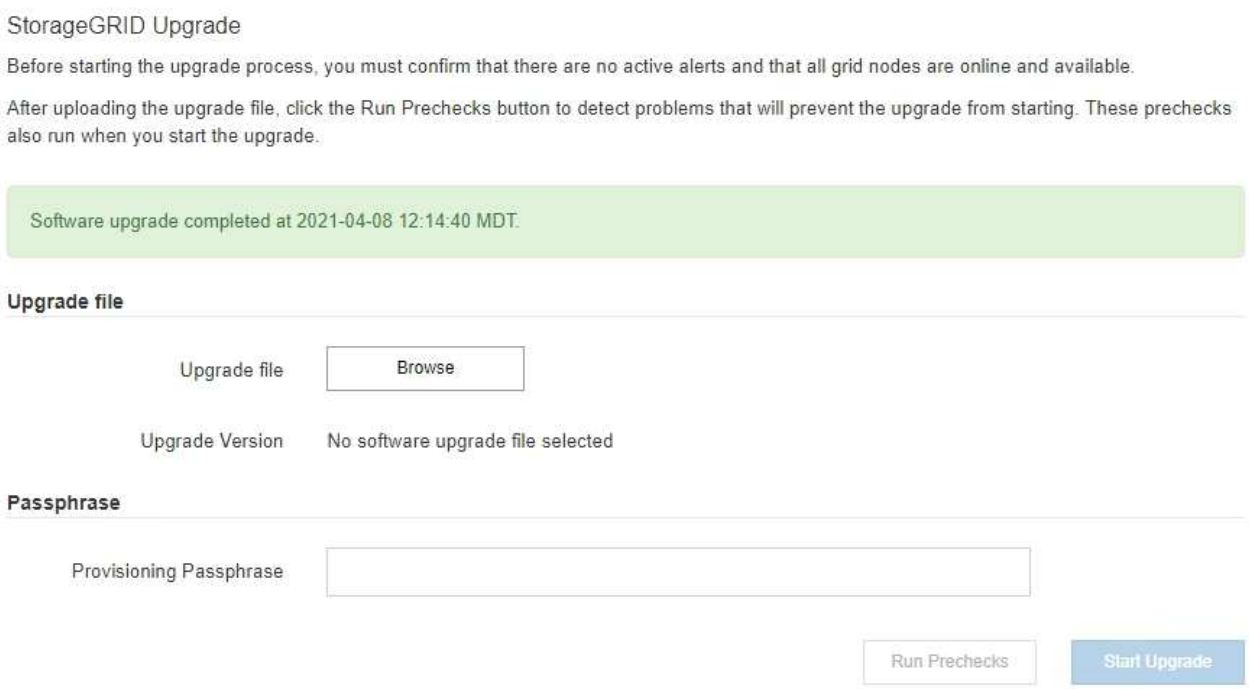


9. Quando a tarefa **Atualizar base de dados** estiver concluída, aguarde alguns minutos para que a tarefa **etapas finais de atualização** seja concluída.



Quando a tarefa etapas de atualização final estiver concluída, a atualização será concluída.

10. Confirme se a atualização foi concluída com êxito.
    a. Faça login no Gerenciador de Grade usando um navegador compatível.
    b. Selecione **Ajuda sobre**.
    c. Confirme se a versão exibida é o que você esperaria.
    d. Selecione **Manutenção sistema Atualização de Software**. Em seguida, selecione **Atualização StorageGRID**.
    e. Confirme se o banner verde mostra que a atualização de software foi concluída na data e hora esperadas.



11. 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.
12. Verifique a página de downloads do NetApp para StorageGRID para ver se há algum hotfixes disponível para a versão do StorageGRID que você acabou de instalar.

    "NetApp Downloads: StorageGRID"

    No número da versão do StorageGRID 11,5.*x.y*:

    - A versão principal tem um valor *x* de 0 (11,5.0).
    - Uma versão menor, se disponível, tem um valor *x* diferente de 0 (por exemplo, 11,5.1).
    - Um hotfix, se disponível, tem um valor *y* (por exemplo, 11,5.0,1).
13. Se disponível, transfira e aplique a correção mais recente para a sua versão do StorageGRID.

    Consulte as instruções de recuperação e manutenção para obter informações sobre a aplicação de hotfixes.

Informações relacionadas

"Transferir o pacote de recuperação"

"Manter recuperar"

Aumentando a configuração espaço reservado metadados

Depois de atualizar para o StorageGRID 11,5, você poderá aumentar a configuração do sistema espaço reservado de metadados se seus nós de armazenamento atenderem a requisitos específicos de RAM e espaço disponível.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root ou a Configuração da Página de topologia de Grade e outras permissões de Configuração de Grade.
- Iniciou a atualização do StorageGRID 11,5 e a tarefa de atualização **Ativar novos recursos** foi concluída.

Sobre esta tarefa

Você pode aumentar manualmente a configuração de espaço reservado de metadados em todo o sistema até 8 TB após a atualização para o StorageGRID 11,5. A reserva de espaço adicional de metadados após a atualização do 11,5 simplificará futuras atualizações de hardware e software.

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 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, vá para as instruções de administração do StorageGRID e procure "armazenamento de metadados de objetos".

"Administrar o StorageGRID"

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. Determine a configuração atual espaço reservado de metadados.
   a. Selecione **Configuração** > **Configurações do sistema** > **Opções de armazenamento**.
   b. Na seção marcas de água de armazenamento, observe o valor de **espaço reservado de metadados**.
3. Certifique-se de que tem espaço disponível suficiente no volume de armazenamento 0 de cada nó de armazenamento para aumentar este valor.
   a. Selecione **nós**.
   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.

4. Certifique-se de que tem pelo menos 128 GB de RAM em cada nó de armazenamento.

a. Selecione **nós**.

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.

5. Atualize a configuração espaço reservado metadados.

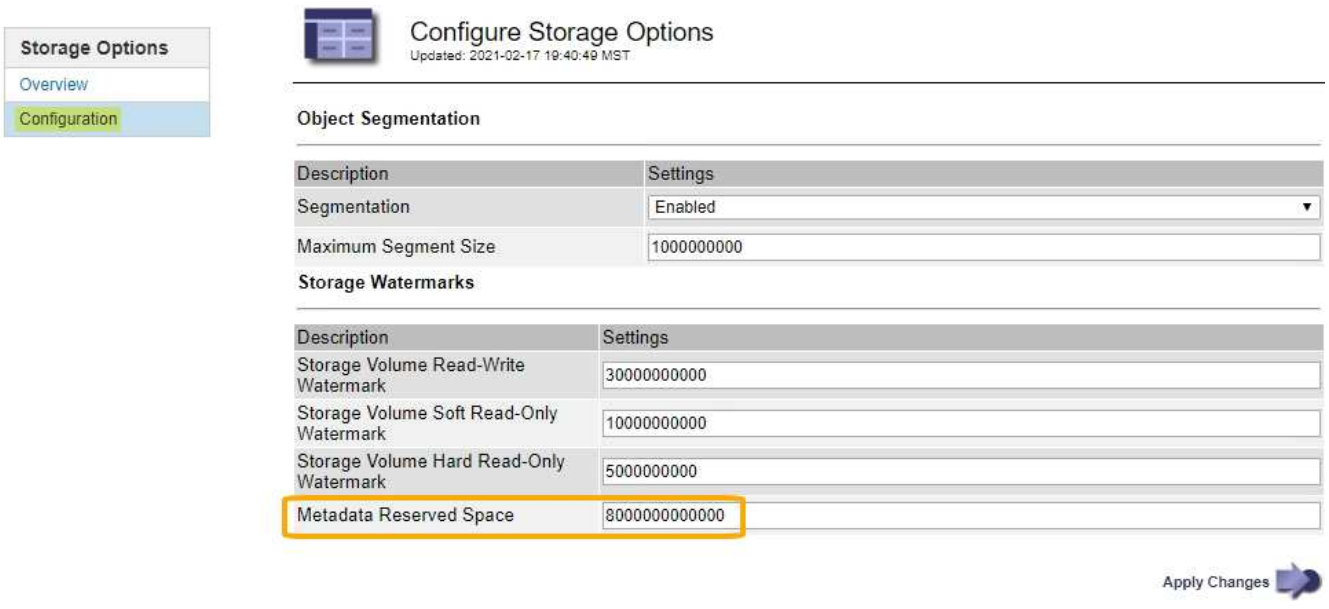
a. Selecione **Configuração** > **Configurações do sistema** > **Opções de armazenamento**.

b. Selecione o separador Configuration (Configuração).

c. Na seção marcas d'água de armazenamento, selecione **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**.

Solução de problemas de atualização

Se a atualização não for concluída com êxito, você poderá resolver o problema sozinho. Se não conseguir resolver um problema, deve recolher as informações necessárias antes de contactar o suporte técnico.

As seções a seguir descrevem como recuperar de situações em que a atualização falhou parcialmente. Contacte o suporte técnico se não conseguir resolver um problema de atualização.

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. Se precisar de ajuda, entre em Contato com o suporte técnico.

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"

Solução de problemas na interface do usuário

Você pode ver problemas com o Gerenciador de Grade ou o Gerenciador do Locatário após atualizar para uma nova versão do software StorageGRID.

A interface Web não responde como esperado

O Gerenciador de Grade ou o Gerente do Locatário podem não responder como esperado depois que o software StorageGRID for atualizado.

Se você tiver problemas com a interface da Web:

- Certifique-se de que está a utilizar um browser suportado.

O suporte do navegador foi alterado para o StorageGRID 11,5. Confirme que está a utilizar uma versão suportada.

- Limpe o cache do navegador da Web.

  Limpar o cache remove recursos desatualizados usados pela versão anterior do software StorageGRID e permite que a interface do usuário funcione corretamente novamente. Para obter instruções, consulte a documentação do navegador da Web.

Informações relacionadas

"Requisitos 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 informando que os seguintes problemas foram identificados pelo pacote de validação de verificação de disponibilidade de imagem do 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.

Mensagem	Causa	Solução
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. Para obter mais informações, consulte as instruções de instalação da sua plataforma Linux.
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.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Instale e mantenha o hardware

SG6000 dispositivos de armazenamento

Saiba como instalar e manter os dispositivos StorageGRID SG6060 e SGF6024.

- "Visão geral dos aparelhos SG6000"
- "Visão geral da instalação e implantação"
- "Preparando-se para a instalação"
- "Instalar o hardware"
- "Configurar o hardware"
- "Implantando um nó de storage de dispositivos"
- "Monitorização da instalação do dispositivo de armazenamento"
- "Automatizando a instalação e a configuração do dispositivo"
- "Visão geral das APIs REST de instalação"
- "Solução de problemas da instalação do hardware"
- "Manutenção do aparelho SG6000"

Visão geral dos aparelhos SG6000

Os dispositivos StorageGRIDSG6000 são plataformas de storage e computação integradas que operam como nós de storage em um sistema StorageGRID. Esses dispositivos podem ser usados em um ambiente de grade híbrida que combina nós de storage do dispositivo e nós de storage virtuais (baseados em software).

Os aparelhos SG6000 oferecem as seguintes caraterísticas:

- Disponível em dois modelos:
  - SG6060, que inclui 60 unidades e é compatível com compartimentos de expansão.
  - SGF6024, que oferece 24 unidades de estado sólido (SSDs).
- Integre os elementos de storage e computação para um nó de storage StorageGRID.
- Inclua o instalador do dispositivo StorageGRID para simplificar a implantação e a configuração do nó de storage.
- Inclua o Gerenciador de sistema do SANtricity para gerenciar e monitorar controladores de storage e unidades.
- Inclua um controlador de gerenciamento de placa base (BMC) para monitorar e diagnosticar o hardware no controlador de computação.
- Suporte até quatro conexões de 10 GbE ou 25 GbE à rede de Grade StorageGRID e à rede de Cliente.
- Dar suporte a unidades FIPS (Federal Information Processing Standard). Quando essas unidades são usadas com o recurso de Segurança da Unidade no Gerenciador de sistema do SANtricity, o acesso não autorizado aos dados é impedido.

Visão geral do SG6060

O dispositivo StorageGRIDSG6060 inclui um controlador de computação e um compartimento de controladora de storage que contém duas controladoras de storage e 60 unidades. Opcionalmente, é possível adicionar gavetas de expansão de 60 unidades ao dispositivo.

SG6060 componentes

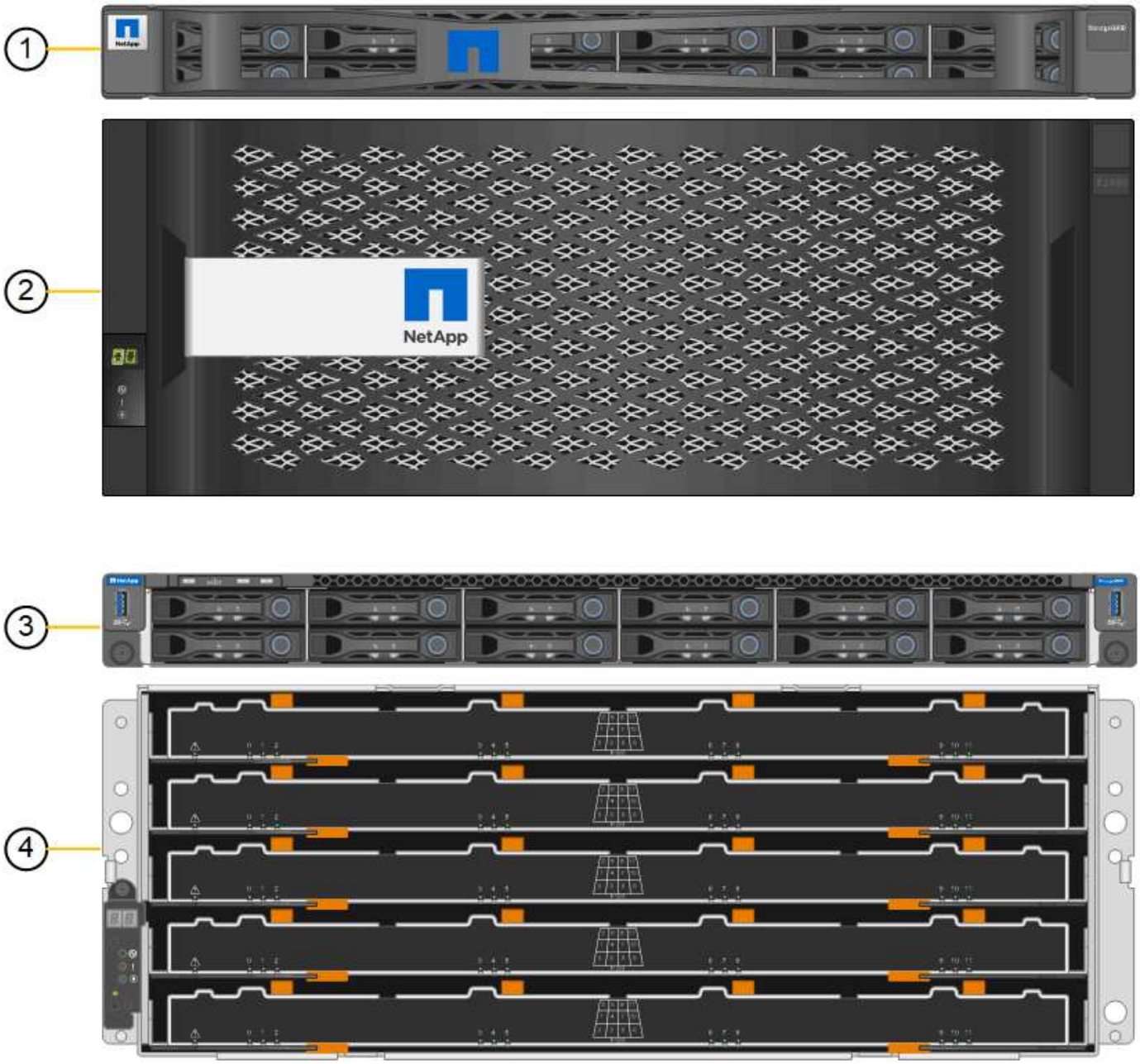
O aparelho SG6060 inclui os seguintes componentes:

Componente	Descrição
Controlador de computação	Controlador SG6000-CN, um servidor de unidade de um rack (1UU) que inclui: • 40 núcleos (80 threads) • 192 GB DE RAM • Até 4 x 25 Gbps de largura de banda agregada Ethernet • Interconexão Fibre Channel (FC) de 4 x 16 Gbps • Controlador de gerenciamento de placa base (BMC) que simplifica o gerenciamento de hardware • Fontes de alimentação redundantes
Compartimento do controlador de storage	Compartimento de controladora e-Series E2860 (storage array), um compartimento de 4U TB que inclui: • Dois controladores e-Series E2800 (configuração duplex) para fornecer suporte a failover de controladora de storage • Compartimento de unidade de cinco gavetas com capacidade para sessenta unidades de 3,5 polegadas (2 unidades de estado sólido, ou SSDs e 58 unidades NL-SAS) • Fontes de alimentação e ventiladores redundantes

Componente	Descrição
Opcional: Prateleiras de expansão de storage **Observação:** as prateleiras de expansão podem ser instaladas durante a implantação inicial ou adicionadas posteriormente.	Compartimento e-Series DE460C, um compartimento de 4U TB que inclui: • Dois módulos de entrada/saída (IOMs) • Cinco gavetas, cada uma com capacidade para 12 unidades NL-SAS, para um total de 60 unidades • Fontes de alimentação e ventiladores redundantes Cada dispositivo SG6060 pode ter uma ou duas gavetas de expansão para um total de 180 unidades.

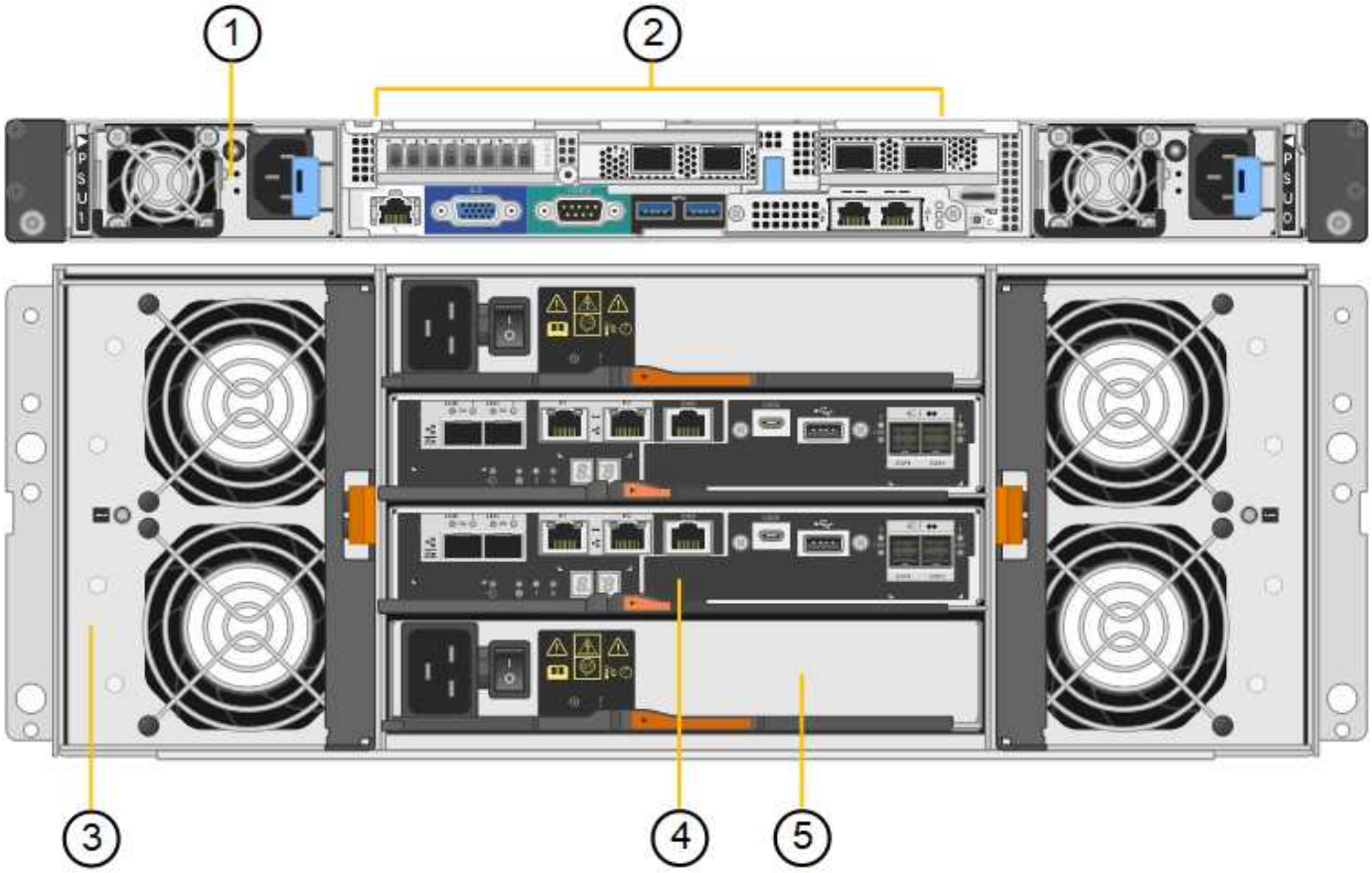
SG6060 diagramas

Esta figura mostra a parte frontal do SG6060, que inclui uma controladora de computação de 1U TB e uma gaveta de 4U TB contendo duas controladoras de storage e 60 unidades em cinco gavetas de unidades.



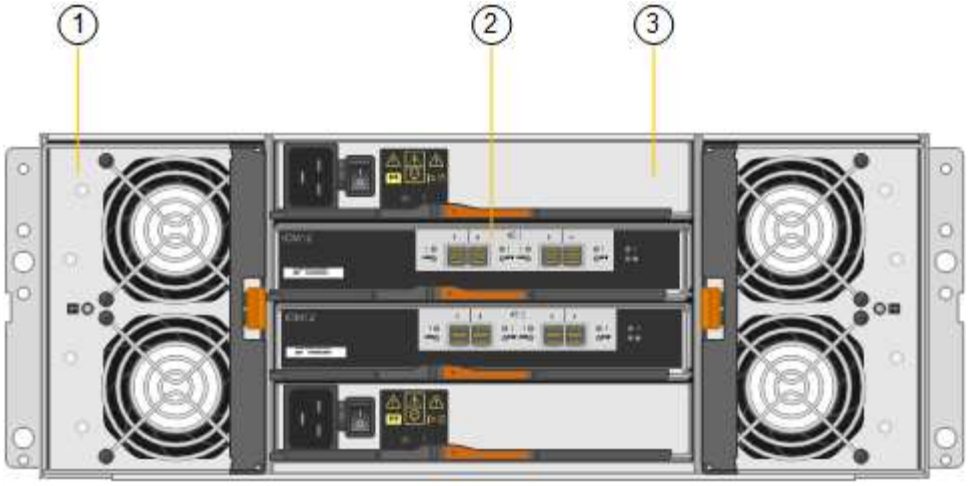
	Descrição
1	Controlador de computação SG6000-CN com moldura frontal
2	Compartimento do controlador E2860 com painel frontal (compartimento de expansão opcional parece idêntico)
3	Controlador de computação SG6000-CN com painel frontal removido
4	Compartimento do controlador E2860 com painel frontal removido (compartimento de expansão opcional parece idêntico)

Essa figura mostra a parte traseira do SG6060, incluindo controladores de computação e storage, ventiladores e fontes de alimentação.



	Descrição
1	Fonte de alimentação (1 de 2) para o controlador de computação SG6000-CN
2	Conetores para controlador de computação SG6000-CN
3	Ventilador (1 de 2) para compartimento do controlador E2860
4	Controlador de armazenamento e-Series E2800 (1 de 2) e conetores
5	Fonte de alimentação (1 de 2) para o compartimento do controlador E2860

Esta figura mostra a parte traseira do compartimento de expansão opcional para o SG6060, incluindo os módulos de entrada/saída (IOMs), ventiladores e fontes de alimentação. Cada SG6060 pode ser instalado com uma ou duas prateleiras de expansão, que podem ser incluídas na instalação inicial ou adicionadas posteriormente.



	Descrição
1	Ventilador (1 de 2) para a prateleira de expansão
2	IOM (1 de 2) para compartimento de expansão
3	Fonte de alimentação (1 de 2) para o compartimento de expansão

Visão geral do SGF6024

O StorageGRIDSGF6024 inclui um controlador de computação e um compartimento de controladora de storage com capacidade para 24 unidades de estado sólido.

SGF6024 componentes

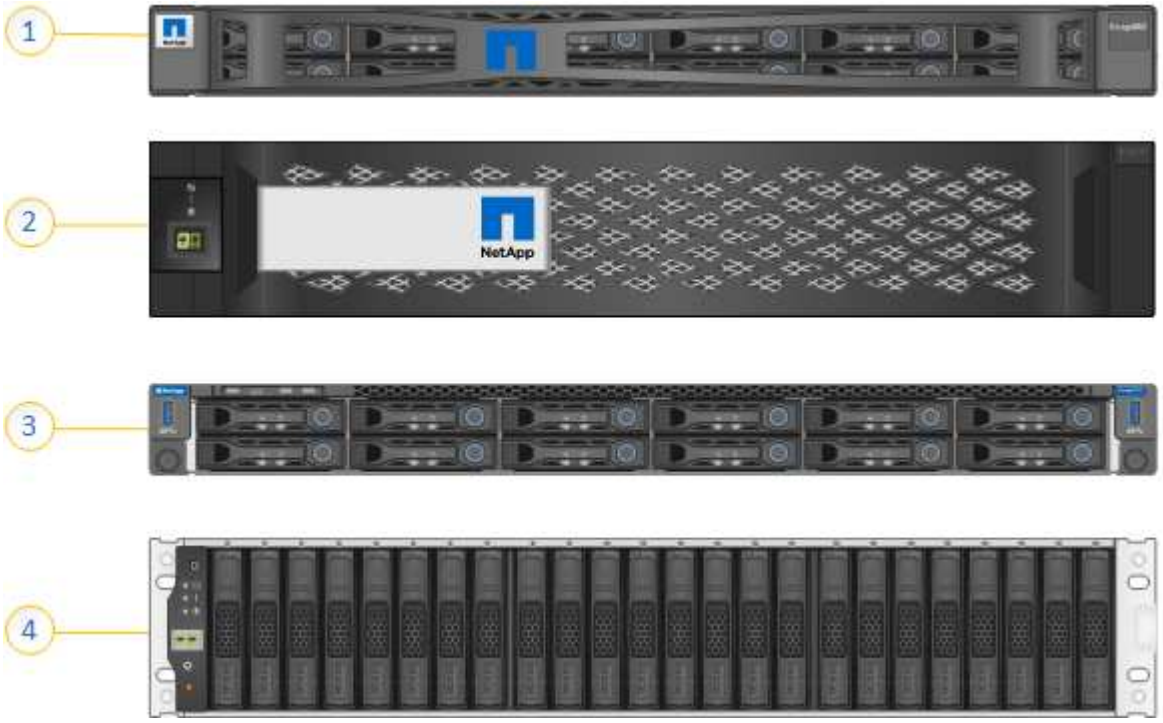
O aparelho SGF6024 inclui os seguintes componentes:

Componente	Descrição
Controlador de computação	Controlador SG6000-CN, um servidor de unidade de um rack (1UU) que inclui: • 40 núcleos (80 threads) • 192 GB DE RAM • Até 4 x 25 Gbps de largura de banda agregada Ethernet • Interconexão Fibre Channel (FC) de 4 x 16 Gbps • Controlador de gerenciamento de placa base (BMC) que simplifica o gerenciamento de hardware • Fontes de alimentação redundantes

Componente	Descrição
Array Flash (compartimento da controladora)	E-Series EF570 flash array (também conhecido como compartimento de controladora), um compartimento de 2U TB que inclui: • Dois controladores e-Series EF570 (configuração duplex) para fornecer suporte a failover de controladora de storage • 24 unidades de estado sólido (também conhecidas como SSDs ou unidades flash) • Fontes de alimentação e ventiladores redundantes

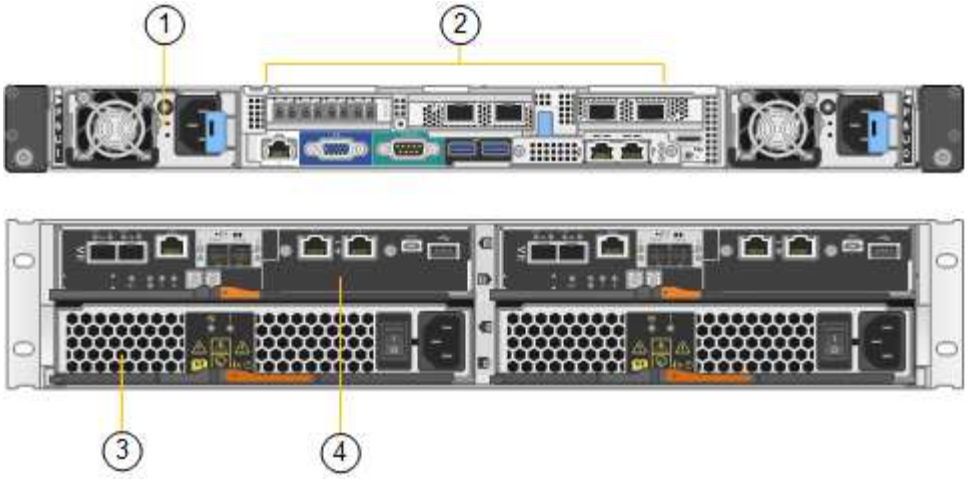
SGF6024 diagramas

Esta figura mostra a parte frontal do SGF6024, que inclui uma controladora de computação 1U e um compartimento 2U contendo duas controladoras de storage e 24 unidades flash.



	Descrição
1	Controlador de computação SG6000-CN com moldura frontal
2	Array Flash EF570 com painel frontal
3	Controlador de computação SG6000-CN com painel frontal removido
4	Array Flash EF570 com painel frontal removido

Essa figura mostra a parte traseira do SGF6024, incluindo controladores de computação e storage, ventiladores e fontes de alimentação.



	Descrição
1	Fonte de alimentação (1 de 2) para o controlador de computação SG6000-CN
2	Conetores para controlador de computação SG6000-CN
3	Fonte de alimentação (1 de 2) para matriz flash EF570
4	Controlador de armazenamento e-Series EF570 (1 de 2) e conetores

Controladores nos dispositivos SG6000

Cada modelo do dispositivo StorageGRIDSG6000 inclui um controlador de computação SG6000-CN em um gabinete 1U e controladores de storage duplex e-Series em um gabinete 2U ou 4U, dependendo do modelo. Reveja os diagramas para saber mais sobre cada tipo de controlador.

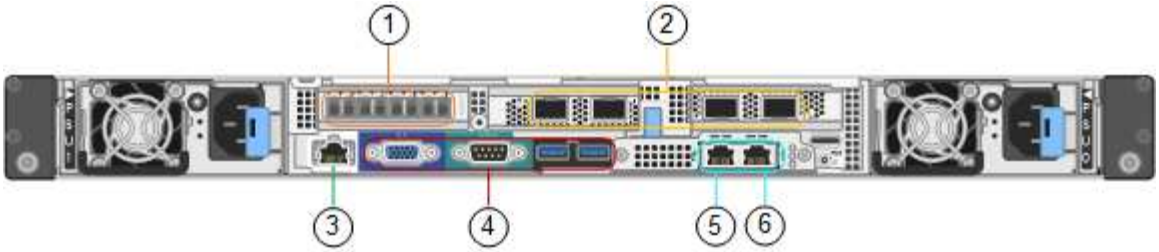
Todos os dispositivos: Controlador de computação SG6000-CN

- Fornece recursos de computação para o dispositivo.
- Inclui o instalador do dispositivo StorageGRID.

> O software StorageGRID não está pré-instalado no dispositivo. Este software é recuperado a partir do Admin Node quando você implementa o dispositivo.

- Pode se conetar a todas as três redes StorageGRID, incluindo a rede de Grade, a rede Admin e a rede cliente.
- Conecta-se aos controladores de storage e-Series e opera como iniciador.

Esta figura mostra os conetores na parte de trás do SG6000-CN.



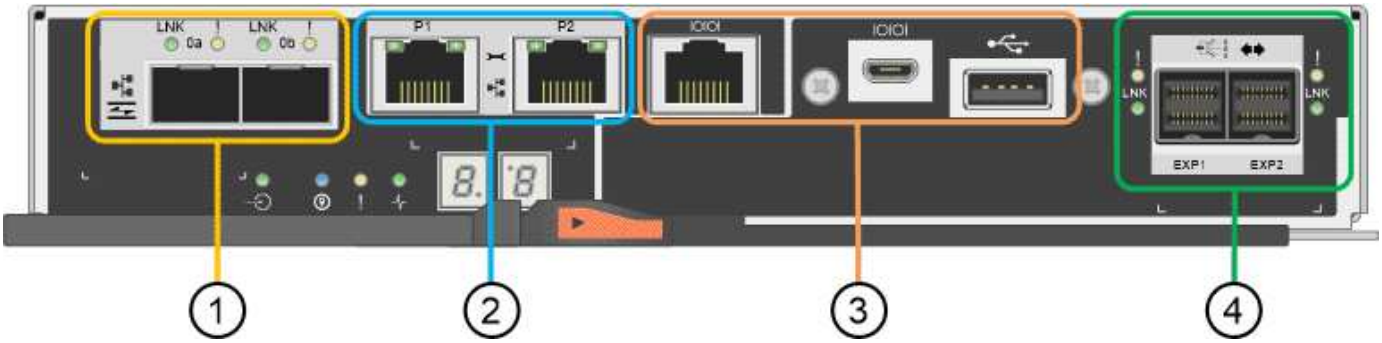
	Porta	Tipo	Utilização
1	Portas de interconexão 1-4	Fibre Channel (FC) de 16 GB/s, com ótica integrada	Ligue o controlador SG6000-CN aos controladores E2800 (duas ligações a cada E2800).
2	Portas de rede 1-4	10 GbE ou 25 GbE, com base no tipo de transcetor de cabo ou SFP, na velocidade do switch e na velocidade do link configurada	Conete-se à rede de grade e à rede de cliente para StorageGRID.
3	Porta de gerenciamento de BMC	1 GbE (RJ-45)	Conete-se ao controlador de gerenciamento de placa base SG6000-CN.
4	Portas de diagnóstico e suporte	• VGA • Série, 115200 8-N-1 • USB	Reservado para uso de suporte técnico.
5	Admin Network port 1	1 GbE (RJ-45)	Ligue o SG6000-CN à rede de administração para StorageGRID.

	Porta	Tipo	Utilização
6	Admin Network port 2	1 GbE (RJ-45)	Opções: • Vincular com a porta de gerenciamento 1 para uma conexão redundante com a rede de administração para StorageGRID. • Deixe desconetado e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, utilize a porta 2 para a configuração IP se os endereços IP atribuídos pelo DHCP não estiverem disponíveis.

SG6060: E2800 controladoras de storage

- Duas controladoras para suporte a failover.
- Gerenciar o armazenamento de dados nas unidades.
- Funciona como controladores padrão da série e em uma configuração duplex.
- Inclua o software SANtricity os (firmware do controlador).
- Inclua o Gerenciador do sistema do SANtricity para monitorar o hardware de armazenamento e gerenciar alertas, o recurso AutoSupport e o recurso de segurança da unidade.
- Conete-se ao controlador SG6000-CN e forneça acesso ao armazenamento.

Esta figura mostra os conetores na parte de trás de cada um dos E2800 controladores.

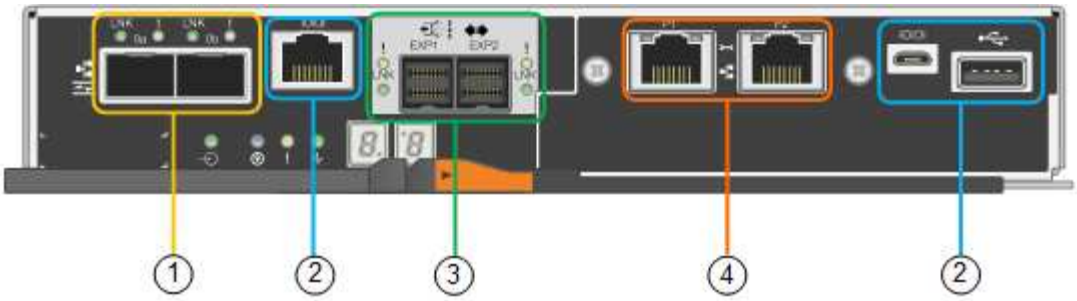


	Porta	Tipo	Utilização
1	Portas de interconexão 1 e 2	SFPa ótico FC de 16 GB/s	Ligue cada um dos controladores E2800 ao controlador SG6000-CN. Existem quatro ligações ao controlador SG6000-CN (duas de cada E2800).
2	Portas de gerenciamento 1 e 2	Ethernet de 1 GB (RJ-45)	• A porta 1 coneta-se à rede onde você acessa o Gerenciador de sistema do SANtricity em um navegador. • A porta 2 está reservada para uso de suporte técnico.
3	Portas de diagnóstico e suporte	• Porta serial RJ-45 • Porta serial micro USB • Porta de USB	Reservado para uso de suporte técnico.
4	Portas de expansão da unidade 1 e 2	SAS de 12GB GB/s.	Conete as portas às portas de expansão da unidade nas IOMs no compartimento de expansão.

SGF6024: EF570 controladoras de storage

- Duas controladoras para suporte a failover.
- Gerenciar o armazenamento de dados nas unidades.
- Funciona como controladores padrão da série e em uma configuração duplex.
- Inclua o software SANtricity os (firmware do controlador).
- Inclua o Gerenciador do sistema do SANtricity para monitorar o hardware de armazenamento e gerenciar alertas, o recurso AutoSupport e o recurso de segurança da unidade.
- Conete-se ao controlador SG6000-CN e forneça acesso ao armazenamento flash.

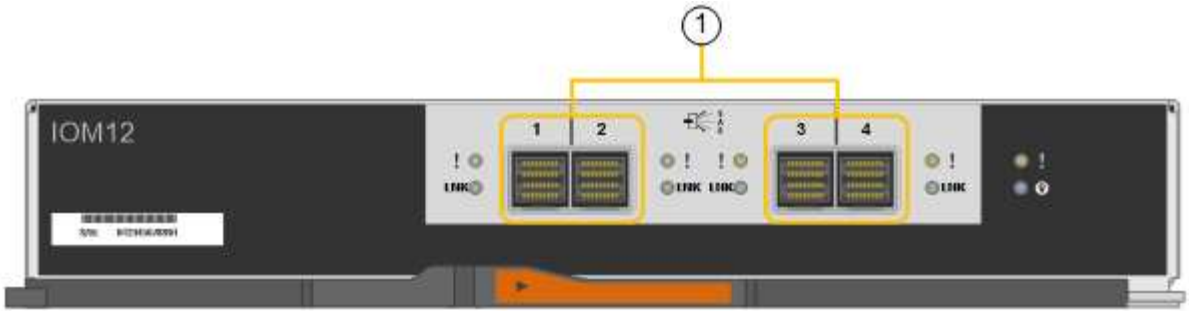
Esta figura mostra os conetores na parte de trás de cada um dos EF570 controladores.



	Porta	Tipo	Utilização
1	Portas de interconexão 1 e 2	SFPa ótico FC de 16 GB/s	Ligue cada um dos controladores EF570 ao controlador SG6000-CN. Existem quatro ligações ao controlador SG6000-CN (duas de cada EF570).
2	Portas de diagnóstico e suporte	• Porta serial RJ-45 • Porta serial micro USB • Porta de USB	Reservado para uso de suporte técnico.
3	Portas de expansão da unidade	SAS de 12GB GB/s.	Não utilizado. O dispositivo SGF6024 não é compatível com compartimentos de unidades de expansão.
4	Portas de gerenciamento 1 e 2	Ethernet de 1 GB (RJ-45)	• A porta 1 coneta-se à rede onde você acessa o Gerenciador de sistema do SANtricity em um navegador. • A porta 2 está reservada para uso de suporte técnico.

SG6060: Módulos de entrada/saída para prateleiras de expansão opcionais

O compartimento de expansão contém dois módulos de entrada/saída (IOMs) que se conectam aos controladores de storage ou a outros compartimentos de expansão.



	Porta	Tipo	Utilização
1	Portas de expansão da unidade 1-4	SAS de 12GB GB/s.	Conecte cada porta aos controladores de storage ou ao compartimento de expansão adicional (se houver).

Visão geral da instalação e implantação

Você pode instalar um ou mais dispositivos de storage do StorageGRID quando implantar o StorageGRID pela primeira vez ou adicionar nós de storage do dispositivo posteriormente como parte de uma expansão. Você também pode precisar instalar um nó de armazenamento de dispositivos como parte de uma operação de recuperação.

O que você vai precisar

O seu sistema StorageGRID está a utilizar a versão necessária do software StorageGRID.

Aparelho	Versão StorageGRID necessária
SG6060 sem compartimentos de expansão	11.1.1 ou posterior
SG6060 PB com compartimentos de expansão (uma ou duas)	11,3 ou posterior **Observação:** se você adicionar compartimentos de expansão após a implantação inicial, use a versão 11,4 ou posterior.
SGF6024	11,3 ou posterior

Tarefas de instalação e implantação

Adicionar um dispositivo de storage StorageGRID a um sistema StorageGRID inclui quatro etapas principais:

1. Preparação para a instalação:
   - Preparar o local de instalação
   - Desembalar as caixas e verificar o conteúdo
   - Obtenção de equipamentos e ferramentas adicionais

- Recolha de endereços IP e informações de rede
- Opcional: Configurando um servidor de gerenciamento de chaves externo (KMS) se você planeja criptografar todos os dados do dispositivo. Consulte detalhes sobre o gerenciamento de chaves externas nas instruções de administração do StorageGRID.

2. Instalar o hardware:
   - Registar o hardware
   - Instalar o aparelho num armário ou num rack
   - Instalar as unidades
   - Instalação das gavetas de expansão opcionais (somente modelo SG6060; máximo de duas gavetas de expansão)
   - Fazer o cabeamento do dispositivo
   - Conexão dos cabos de energia e alimentação
   - Exibindo códigos de status de inicialização
3. Configurar o hardware:
   - Acessando o Gerenciador do sistema do SANtricity para configurar as configurações do Gerenciador do sistema do SANtricity
   - Acessando o Instalador de dispositivos StorageGRID, definindo um endereço IP estático para a porta de gerenciamento 1 no controlador de armazenamento e configurando as configurações de IP de rede e link necessárias para se conetar a redes StorageGRID
   - Aceder à interface do controlador de gestão de base (BMC) no controlador SG6000-CN
   - Opcional: Habilitando a criptografia de nó se você planeja usar um KMS externo para criptografar dados do dispositivo.
   - Opcional: Alterar o modo RAID.
4. Implantando o dispositivo como nó de storage:

Tarefa	Instruções
Implantando um nó de storage de dispositivos em um novo sistema StorageGRID	"Implantando um nó de storage de dispositivos"
Adicionando um nó de storage de dispositivo a um sistema StorageGRID existente	Instruções para expandir um sistema StorageGRID
Implantando um nó de storage de dispositivos como parte de uma operação de recuperação de nó de storage	Instruções para recuperação e manutenção

Informações relacionadas

"Preparando-se para a instalação"

"Instalar o hardware"

"Configurar o hardware"

"Expanda sua grade"

"Manter recuperar"

"Administrar o StorageGRID"

Preparando-se para a instalação

Preparar a instalação de um dispositivo StorageGRID implica preparar o local e obter todo o hardware, cabos e ferramentas necessários. Você também deve coletar endereços IP e informações de rede.

Passos

- "Preparação do local (SG6000)"
- "Desembalar as caixas (SG6000)"
- "Obtenção de equipamentos e ferramentas adicionais (SG6000)"
- "Requisitos do navegador da Web"
- "Rever as ligações de rede do dispositivo"
- "Recolha de informações de instalação (SG6000)"

Preparação do local (SG6000)

Antes de instalar o aparelho, certifique-se de que o local e o gabinete ou rack que pretende utilizar cumprem as especificações de um dispositivo StorageGRID.

Passos

1. Confirme se o local atende aos requisitos de temperatura, umidade, faixa de altitude, fluxo de ar, dissipação de calor, fiação, energia e aterramento. Consulte o NetApp Hardware Universe para obter mais informações.
2. Confirme se a sua localização fornece alimentação CA de 240 volts para a alimentação CA de SG6060 ou 120 volts para o SGF6024.
3. Obtenha um gabinete ou rack de 19 polegadas (48,3 cm) para encaixar prateleiras deste tamanho (sem cabos):

Tipo de prateleira	Altura	Largura	Profundidade	Peso máximo
• E2860 compartimento do controlador* para SG6060	6,87 pol. (17,46 cm)	17,66 pol. (44,86 cm)	38,25 pol. (97,16 cm)	13 250 lb. (113 kg)
• Prateleira de expansão opcional* para SG6060 (um ou dois)	6,87 pol. (17,46 cm)	17,66 pol. (44,86 cm)	38,25 pol. (97,16 cm)	13 250 lb. (113 kg)

Tipo de prateleira	Altura	Largura	Profundidade	Peso máximo
• EF570 compartimento do controlador* para SGF6024	3,35 pol. (8,50 cm)	17,66 pol. (44,86 cm)	19,00 pol. (48,26 cm)	13 51,74 lb. (23,47 kg)
Controlador SG6000-CN para cada aparelho	1,70 pol. (4,32 cm)	17,32 pol. (44,0 cm)	32,0 pol. (81,3 cm)	13 39 lb. (17,7 kg)

4. Decida onde vai instalar o aparelho.

> Ao instalar o compartimento do controlador E2860 ou as prateleiras de expansão opcionais, instale o hardware da parte inferior para a parte superior do rack ou gabinete para evitar que o equipamento tombe. Para garantir que o equipamento mais pesado esteja na parte inferior do gabinete ou rack, instale o controlador SG6000-CN acima da prateleira do controlador E2860 e das prateleiras de expansão.

> Antes de se comprometer com a instalação, verifique se os 0,5m cabos óticos fornecidos com o aparelho, ou os cabos que você fornecer, são longos o suficiente para o layout planejado.

Informações relacionadas

"NetApp Hardware Universe"

"Ferramenta de Matriz de interoperabilidade do NetApp"

Desembalar as caixas (SG6000)

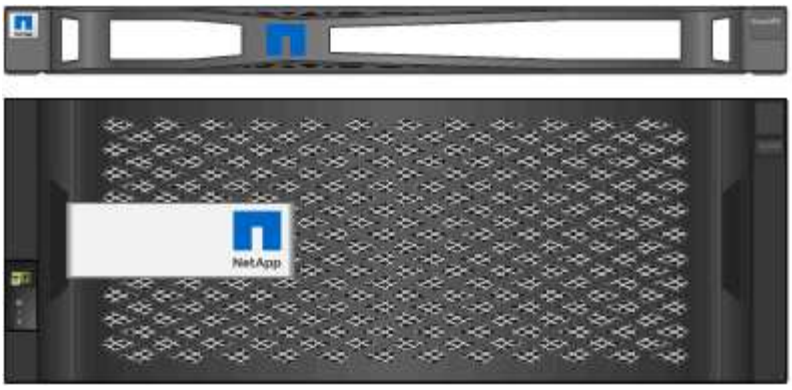
Antes de instalar o dispositivo StorageGRID, desembale todas as caixas e compare o conteúdo com os itens no saco de embalagem.

SG6060

- **Controlador SG6000-CN**

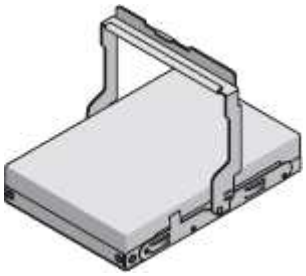
- * Compartimento do controlador E2860 sem unidades instaladas*

- * Duas molduras frontais*

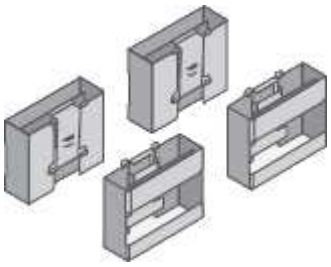


- * Dois kits de trilho com instruções*

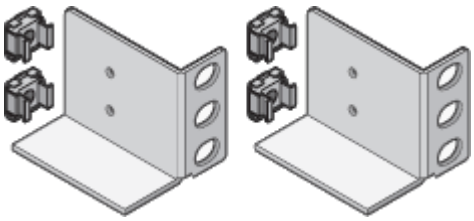
- **Unidades de 60 TB (SSD de 2 TB e NL-SAS de 58 TB)**



- * Quatro alças*



- * Suportes traseiros e porcas de gaiola para instalação de rack de furo quadrado *

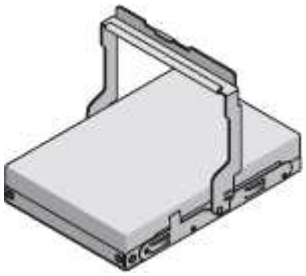


Compartimento de expansão do SG6060

- **Compartimento de expansão sem unidades instaladas**

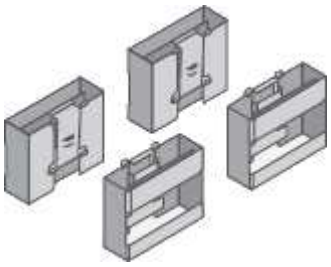
- * Moldura frontal*

- **Unidades NL-SAS de 60 TB**

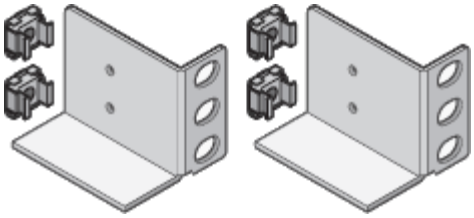


- **Um kit de trilho com instruções**

- * Quatro alças*



- * Suportes traseiros e porcas de gaiola para instalação de rack de furo quadrado *



SGF6024

- **Controlador SG6000-CN**

- * EF570 flash array com 24 unidades de estado sólido (flash) instaladas*

- * Duas molduras frontais*

- * Dois kits de trilho com instruções*

- * Tampas de prateleira*

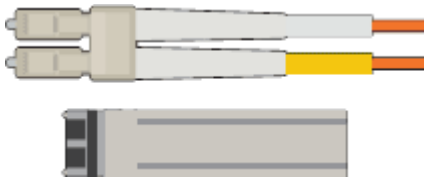
Cabos e conetores

O envio para o dispositivo StorageGRID inclui os seguintes cabos e conetores:

- **Quatro cabos de alimentação para o seu país**

O gabinete pode ter cabos de alimentação especiais que você usa em vez dos cabos de alimentação fornecidos com o aparelho.

- * Cabos óticos e transcetores SFP*



Quatro cabos óticos para as portas de interconexão FC

Quatro transcetores SFP mais, que suportam FC de 16 GB/s

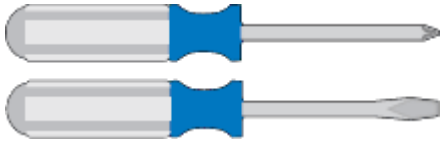
- *Opcional: Dois cabos SAS para conetar cada prateleira de expansão SG6060 *

Obtenção de equipamentos e ferramentas adicionais (SG6000)

Antes de instalar o dispositivo StorageGRID, confirme se tem todo o equipamento e ferramentas adicionais de que necessita.

Você precisa do seguinte equipamento adicional para instalar e configurar o hardware:

- **Chaves de fenda**

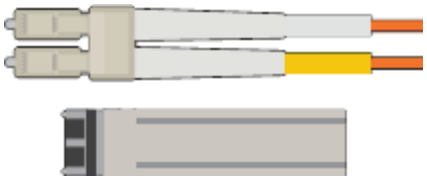


Chave de fendas Phillips n.o 2

Chave de parafusos plana média

- * Pulseira antiestática*

- * Cabos óticos e transcetores SFP*



Você precisa de uma das seguintes opções:

- Um a quatro cabos Twinax ou cabos óticos para as portas 10/25-GbE que você planeja usar no controlador SG6000-CN
- Um a quatro transcetores SFP mais para as portas de 10/25 GbE se você usar cabos óticos e velocidade de link de 10 GbE
- Um a quatro transcetores SFP28 para as portas de 10/25 GbE se você usar cabos óticos e velocidade de link de 25 GbE

- **Cabos Ethernet RJ-45 (Cat5/Cat5e/Cat6)**

- * Serviço de laptop*

Navegador da Web suportado

Porta de 1 GbE (RJ-45)

- **Ferramentas opcionais**

Broca elétrica com ponta Phillips

Lanterna

Elevador mecanizado para prateleiras de 60 unidades

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Rever as ligações de rede do dispositivo

Antes de instalar o dispositivo StorageGRID, você deve entender quais redes podem ser conetadas ao dispositivo.

Ao implantar um dispositivo StorageGRID como nó de storage em um sistema StorageGRID, você pode conectá-lo às seguintes redes:

- **Rede de grade para StorageGRID**: A rede de grade é usada para todo o tráfego interno de StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes. A rede de Grade é necessária.
- **Rede de administração para StorageGRID**: A rede de administração é uma rede fechada usada para administração e manutenção do sistema. A rede Admin é normalmente uma rede privada e não precisa ser roteável entre sites. A rede de administração é opcional.
- **Rede de clientes para StorageGRID:** a rede de clientes é uma rede aberta usada para fornecer acesso a aplicativos clientes, incluindo S3 e Swift. A rede do cliente fornece acesso ao protocolo do cliente à grade, de modo que a rede da grade possa ser isolada e protegida. A rede do cliente é opcional.
- **Rede de gerenciamento para o Gerenciador de sistema SANtricity**: Essa rede fornece acesso ao Gerenciador de sistema SANtricity no controlador de armazenamento, permitindo que você monitore e gerencie os componentes de hardware no compartimento do controlador de armazenamento. Essa rede de gerenciamento pode ser a mesma rede de administração para StorageGRID ou pode ser uma rede de gerenciamento independente.
- **Rede de gerenciamento BMC para o controlador SG6000-CN:** esta rede fornece acesso ao controlador de gerenciamento de placa base no SG6000-CN, permitindo que você monitore e gerencie os componentes de hardware no controlador SG6000-CN. Essa rede de gerenciamento pode ser a mesma rede de administração para StorageGRID ou pode ser uma rede de gerenciamento independente.

Para obter informações detalhadas sobre redes StorageGRID, consulte *Primer*.

Informações relacionadas

"Recolha de informações de instalação (SG6000)"

"Cabeamento do aparelho (SG6000)"

"Modos de ligação de porta para o controlador SG6000-CN"

"Diretrizes de rede"

Modos de ligação de porta para o controlador SG6000-CN

Ao configurar links de rede para o SG6000-CN, você pode usar a ligação de porta para as portas 10/25-GbE que se conetam à rede de Grade e à rede de cliente opcional, e as portas de gerenciamento de 1 GbE que se conetam à rede de administração opcional. A ligação de portas ajuda a proteger os seus dados fornecendo caminhos redundantes entre as redes StorageGRID e o dispositivo.

Informações relacionadas

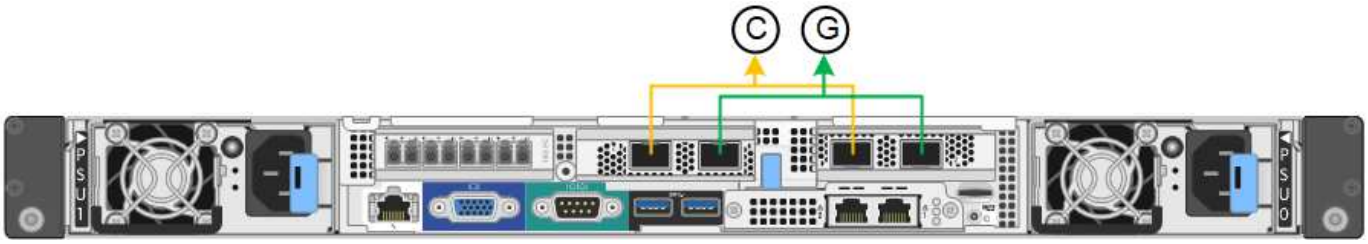
"Configurando links de rede (SG6000)"

Modos de ligação de rede para as portas 10/25-GbE

As portas de rede 10/25-GbE no controlador SG6000-CN suportam o modo de ligação de porta fixa ou modo de ligação de porta agregada para as conexões de rede de Grade e rede de cliente.

Modo de ligação de porta fixa

O modo fixo é a configuração padrão para as portas de rede 10/25-GbE.



	Quais portas estão coladas
C	As portas 1 e 3 são Unidas para a rede do cliente, se esta rede for utilizada.
G	As portas 2 e 4 são Unidas para a rede de Grade.

Ao usar o modo de ligação de porta fixa, as portas podem ser coladas usando o modo de backup ativo ou o modo de protocolo de controle de agregação de link (LACP 802,3ad).

- No modo de backup ativo (padrão), apenas uma porta está ativa por vez. Se a porta ativa falhar, sua porta de backup fornecerá automaticamente uma conexão de failover. A porta 4 fornece um caminho de backup para a porta 2 (rede de Grade) e a porta 3 fornece um caminho de backup para a porta 1 (rede de cliente).
- No modo LACP, cada par de portas forma um canal lógico entre o controlador e a rede, permitindo maior

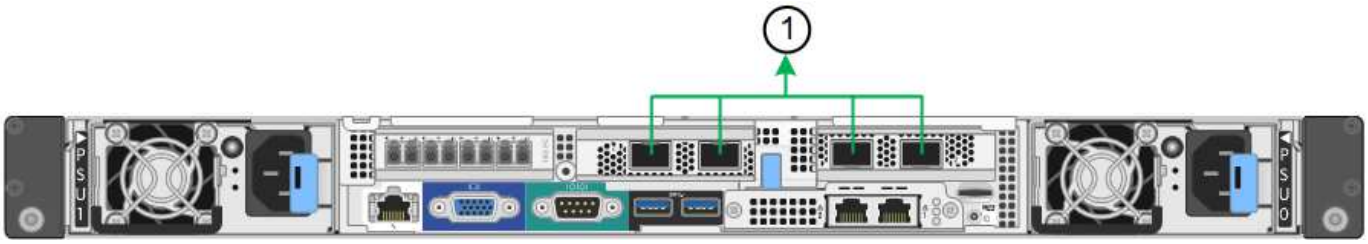
produtividade. Se uma porta falhar, a outra continua a fornecer o canal. A taxa de transferência é reduzida, mas a conetividade não é afetada.

> Se não precisar de ligações redundantes, pode utilizar apenas uma porta para cada rede. No entanto, esteja ciente de que um alerta será acionado no Gerenciador de Grade após a instalação do StorageGRID, indicando que o link está inativo. Uma vez que esta porta está desligada de propósito, pode desativar este alerta com segurança.

No Gerenciador de Grade, selecione **Alerta regras**, selecione a regra e clique em **Editar regra**. Em seguida, desmarque a caixa de seleção **Enabled**.

Modo de ligação de porta agregada

O modo de ligação de porta agregada aumenta significativamente o em toda a rede StorageGRID e fornece caminhos de failover adicionais.



	Quais portas estão coladas
1	Todas as portas conetadas são agrupadas em uma única ligação LACP, permitindo que todas as portas sejam usadas para o tráfego de rede de Grade e rede de Cliente.

Se você planeja usar o modo de ligação de porta agregada:

- Você deve usar o modo de ligação de rede LACP.
- Você deve especificar uma tag VLAN exclusiva para cada rede. Essa tag VLAN será adicionada a cada pacote de rede para garantir que o tráfego de rede seja roteado para a rede correta.
- As portas devem ser conetadas a switches que possam suportar VLAN e LACP. Se vários switches estiverem participando da ligação LACP, os switches devem suportar grupos de agregação de links de vários gabinetes (MLAG) ou equivalente.
- Você deve entender como configurar os switches para usar VLAN, LACP e MLAG, ou equivalente.

Se você não quiser usar todas as quatro portas 10/25 GbE, poderá usar uma, duas ou três portas. O uso de mais de uma porta maximiza a chance de que alguma conetividade de rede permaneça disponível se uma das portas 10/25-GbE falhar.

> Se você optar por usar menos de quatro portas, esteja ciente de que um ou mais alarmes serão levantados no Gerenciador de Grade após a instalação do StorageGRID, indicando que os cabos estão desconetados. Você pode reconhecer os alarmes com segurança para limpá-los.

Modos de ligação de rede para as portas de gerenciamento de 1 GbE

Para as duas portas de gerenciamento de 1 GbE no controlador SG6000-CN, você pode escolher o modo de ligação de rede independente ou o modo de ligação de rede ative-

Backup para se conetar à rede Admin opcional.

No modo independente, apenas a porta de gerenciamento à esquerda está conetada à rede de administração. Este modo não fornece um caminho redundante. A porta de gerenciamento à direita está desconetada e disponível para conexões locais temporárias (usa o endereço IP 169.254.0.1)

No modo ative-Backup, ambas as portas de gerenciamento estão conetadas à rede Admin. Apenas uma porta está ativa de cada vez. Se a porta ativa falhar, sua porta de backup fornecerá automaticamente uma conexão de failover. A ligação dessas duas portas físicas em uma porta de gerenciamento lógico fornece um caminho redundante para a rede de administração.

Se você precisar fazer uma conexão local temporária com o controlador SG6000-CN quando as portas de gerenciamento de 1 GbE estiverem configuradas para o modo ative-Backup, remova os cabos de ambas as portas de gerenciamento, conete o cabo temporário à porta de gerenciamento à direita e acesse o dispositivo usando o endereço IP 169.254.0.1.

	Modo de ligação de rede
A	Ambas as portas de gerenciamento são ligadas a uma porta de gerenciamento lógico conetada à rede de administração.
I	A porta à esquerda está ligada à rede de administração. A porta à direita está disponível para conexões locais temporárias (endereço IP 169.254.0.1).

Recolha de informações de instalação (SG6000)

À medida que você instala e configura o dispositivo StorageGRID, você deve tomar decisões e coletar informações sobre portas de switch Ethernet, endereços IP e modos de ligação de porta e rede.

Sobre esta tarefa

Você pode usar as tabelas a seguir para gravar as informações necessárias para cada rede conetada ao aparelho. Esses valores são necessários para instalar e configurar o hardware.

Informações necessárias para se conectar ao Gerenciador de sistema do SANtricity nos controladores de storage

Você deve conectar ambas as controladoras de storage no dispositivo (controladoras E2800 ou controladoras EF570) à rede de gerenciamento que usará no Gerenciador de sistemas do SANtricity. Os controladores estão localizados em cada dispositivo da seguinte forma:

- SG6060: O controlador A está na parte superior e o controlador B está na parte inferior.
- SGF6024: O controlador A está à esquerda e o controlador B está à direita.

Informações necessárias	O seu valor para o controlador A	O seu valor para o controlador B
Porta do switch Ethernet você conetará à porta de gerenciamento 1 (identificada como P1 no controlador)		
Endereço MAC da porta de gerenciamento 1 (impresso em uma etiqueta próxima à porta P1)		
Endereço IP atribuído pelo DHCP para a porta de gerenciamento 1, se disponível após a ativação **Observação:** se a rede que você se conetará ao controlador de armazenamento incluir um servidor DHCP, o administrador de rede poderá usar o endereço MAC para determinar o endereço IP atribuído pelo servidor DHCP.		
Endereço IP estático que pretende utilizar para o dispositivo na rede de gestão	Para IPv4: • Endereço IPv4: • Máscara de sub-rede: • Gateway: Para IPv6: • Endereço IPv6: • Endereço IP roteável: • Endereço IP do router do controlador de armazenamento:	Para IPv4: • Endereço IPv4: • Máscara de sub-rede: • Gateway: Para IPv6: • Endereço IPv6: • Endereço IP roteável: • Endereço IP do router do controlador de armazenamento:
Formato do endereço IP	Escolha uma: • IPv4 • IPv6	Escolha uma: • IPv4 • IPv6

Informações necessárias	O seu valor para o controlador A	O seu valor para o controlador B
Velocidade e modo duplex **Observação:** você deve certificar-se de que o switch Ethernet da rede de gerenciamento do Gerenciador de sistema do SANtricity esteja definido como negociação automática.	Deve ser: • Negociação automática (padrão)	Deve ser: • Negociação automática (padrão)

Informações necessárias para conetar o controlador SG6000-CN à rede Admin

A rede de administração para StorageGRID é uma rede opcional, usada para administração e manutenção do sistema. O dispositivo se coneta à rede Admin usando as seguintes portas de gerenciamento de 1 GbE no controlador SG6000-CN.

Informações necessárias	O seu valor
Rede de administração ativada	Escolha uma: • Não • Sim (predefinição)
Modo de ligação de rede	Escolha uma: • Independente (predefinição) • Ative-Backup
Porta do switch para a porta esquerda no círculo vermelho no diagrama (porta ativa padrão para o modo de ligação de rede independente)	
Porta do switch para a porta direita no círculo vermelho no diagrama (apenas modo de ligação de rede ative-Backup)	

Informações necessárias	O seu valor
Endereço MAC para a porta Admin Network **Nota:** a etiqueta de endereço MAC na parte frontal do controlador SG6000-CN lista o endereço MAC da porta de gerenciamento BMC. Para determinar o endereço MAC da porta Admin Network, você deve adicionar **2** ao número hexadecimal na etiqueta. Por exemplo, se o endereço MAC na etiqueta terminar em **09**, o endereço MAC da porta Admin terminaria em **0B**. Se o endereço MAC na etiqueta terminar em **(*y*)FF**, o endereço MAC da porta Admin terminaria em **(*y*(1)01**. Você pode facilmente fazer esse cálculo abrindo o Calculator no Windows, definindo-o para o modo Programador, selecionando Hex, digitando o endereço MAC e, em seguida, digitando * 2 *.	
Endereço IP atribuído pelo DHCP para a porta Admin Network, se disponível após a ativação **Observação:** você pode determinar o endereço IP atribuído pelo DHCP usando o endereço MAC para procurar o IP atribuído.	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede de administração **Nota:** se a rede não tiver um gateway, especifique o mesmo endereço IPv4 estático para o gateway.	• Endereço IPv4 (CIDR): • Gateway:
Sub-redes de rede Admin (CIDR)	

Informações necessárias para conetar e configurar as portas 10/25-GbE no controlador SG6000-CN

As quatro portas 10/25-GbE no controlador SG6000-CN conetam-se à rede de Grade StorageGRID e à rede de Cliente opcional.

Informações necessárias	O seu valor
Velocidade da ligação	Escolha uma: • Auto (predefinição) • 10 GbE • 25 GbE

Informações necessárias	O seu valor
Modo de ligação da porta	Escolha uma: • Fixo (padrão) • Agregado
Porta do switch para a porta 1 (rede do cliente para o modo fixo)	
Porta do switch para a porta 2 (rede de grade para modo fixo)	
Porta do switch para a porta 3 (rede do cliente para o modo fixo)	
Porta do switch para a porta 4 (rede de grade para modo fixo)	

Informações necessárias para conetar o controlador SG6000-CN à rede de Grade

A rede de Grade para StorageGRID é uma rede necessária, usada para todo o tráfego interno de StorageGRID. O dispositivo se coneta à rede de Grade usando as portas 10/25-GbE no controlador SG6000-CN.

Informações necessárias	O seu valor
Modo de ligação de rede	Escolha uma: • Ative-Backup (padrão) • Bola de Futsal (802,3ad)
Marcação de VLAN ativada	Escolha uma: • Não (predefinição) • Sim
Tag VLAN (se a marcação VLAN estiver ativada)	Introduza um valor entre 0 e 4095:
Endereço IP atribuído pelo DHCP para a rede de Grade, se disponível após a ativação	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede de grelha **Nota:** se a rede não tiver um gateway, especifique o mesmo endereço IPv4 estático para o gateway.	• Endereço IPv4 (CIDR): • Gateway:

Informações necessárias	O seu valor
Sub-redes de rede de rede (CIDR)	

Informações necessárias para conetar o controlador SG6000-CN à rede do cliente

A rede de cliente para StorageGRID é uma rede opcional, normalmente usada para fornecer acesso de protocolo de cliente à grade. O dispositivo se coneta à rede do cliente usando as portas 10/25-GbE no controlador SG6000-CN.

Informações necessárias	O seu valor
Rede cliente ativada	Escolha uma: • Não (predefinição) • Sim
Modo de ligação de rede	Escolha uma: • Ative-Backup (padrão) • Bola de Futsal (802,3ad)
Marcação de VLAN ativada	Escolha uma: • Não (predefinição) • Sim
Tag VLAN (se a marcação VLAN estiver ativada)	Introduza um valor entre 0 e 4095:
Endereço IP atribuído pelo DHCP para a rede do cliente, se disponível após a ligação	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede do cliente **Nota:** se a rede do cliente estiver ativada, a rota padrão no controlador usará o gateway especificado aqui.	• Endereço IPv4 (CIDR): • Gateway:

Informações necessárias para conetar o controlador SG6000-CN à rede de gerenciamento BMC

Você pode acessar a interface BMC no controlador SG6000-CN usando a seguinte porta de gerenciamento de 1 GbE. Esta porta suporta a gestão remota do hardware do controlador através de Ethernet, utilizando a norma IPMI (Intelligent Platform Management Interface).

Informações necessárias	O seu valor
Porta do switch Ethernet, você se conetará à porta de gerenciamento BMC (circulada no diagrama)	
Endereço IP atribuído por DHCP para a rede de gerenciamento BMC, se disponível após a inicialização	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para a porta de gestão BMC	• Endereço IPv4 (CIDR): • Gateway:

Informações relacionadas

"Controladores nos dispositivos SG6000"

"Rever as ligações de rede do dispositivo"

"Modos de ligação de porta para o controlador SG6000-CN"

"Cabeamento do aparelho (SG6000)"

"Configurando endereços IP do StorageGRID"

Instalar o hardware

A instalação de hardware implica a instalação do controlador SG6000-CN e da prateleira do controlador de armazenamento em um gabinete ou rack, conetando os cabos e aplicando energia.

Passos

- "Registar o hardware"
- "SG6060: Instalação de compartimentos de 60 unidades em um gabinete ou rack"
- "SG6060: Instalar as unidades"
- "SGF6024: Instalação de compartimentos de 24 unidades em um gabinete ou rack"
- "SG6000-CN: Instalação em um gabinete ou rack"
- "Cabeamento do aparelho (SG6000)"
- "SG6060: Cabeamento das gavetas de expansão opcionais"
- "Conexão dos cabos de alimentação e alimentação de energia (SG6000)"
- "Visualizar indicadores de estado e botões no controlador SG6000-CN"
- "Exibindo códigos de status de inicialização para os controladores de storage SG6000"

Registar o hardware

Registrar o hardware do aparelho fornece benefícios de suporte.

Passos

1. Localize o número de série do chassi do compartimento do controlador de armazenamento.

   Pode encontrar o número no folheto de embalagem, no seu e-mail de confirmação ou no aparelho depois de o desembalar.

   Existem vários números de série no dispositivo de armazenamento. O número de série no compartimento do controlador de armazenamento é aquele que deve ser registrado e usado se você chamar para assistência ou suporte no dispositivo.

2. Vá para o site de suporte da NetApp em "mysupport.NetApp.com".
3. Determine se você precisa Registrar o hardware:

Se você é um…	Siga estes passos…
Cliente NetApp existente	a. Inicie sessão com o seu nome de utilizador e palavra-passe. b. Selecione **Produtos Meus Produtos**. c. Confirme se o novo número de série está listado. d. Se não estiver, siga as instruções para novos clientes NetApp.
Novo cliente da NetApp	a. Clique em **Registe-se agora** e crie uma conta. b. Selecione **Produtos Registe produtos**. c. Insira o número de série do produto e os detalhes solicitados. Após a aprovação do seu registo, pode transferir qualquer software necessário. O processo de aprovação pode demorar até 24 horas.

SG6060: Instalação de compartimentos de 60 unidades em um gabinete ou rack

Você deve instalar um conjunto de trilhos para o compartimento do controlador E2860 em seu gabinete ou rack e, em seguida, deslizar a prateleira do controlador para os trilhos. Se você estiver instalando compartimentos de expansão de 60 unidades, o mesmo procedimento será aplicado.

O que você vai precisar

- Você revisou o documento de Avisos de segurança incluído na caixa e entendeu as precauções para mover e instalar hardware.
- Você tem as instruções fornecidas com o kit de trilho.

Cada compartimento de 60 unidades pesa aproximadamente 132 lb (60 kg) sem unidades instaladas. Quatro pessoas ou um elevador mecanizado são necessários para mover a prateleira com segurança.

Para evitar danificar o hardware, nunca mova a gaveta se as unidades estiverem instaladas. É necessário remover todas as unidades antes de mover a gaveta.

Ao instalar o compartimento do controlador E2860 ou as prateleiras de expansão opcionais, instale o hardware da parte inferior para a parte superior do rack ou gabinete para evitar que o equipamento tombe. Para garantir que o equipamento mais pesado esteja na parte inferior do gabinete ou rack, instale o controlador SG6000-CN acima da prateleira do controlador E2860 e das prateleiras de expansão.

Antes de se comprometer com a instalação, verifique se os 0,5m cabos óticos fornecidos com o aparelho, ou os cabos que você fornecer, são longos o suficiente para o layout planejado.

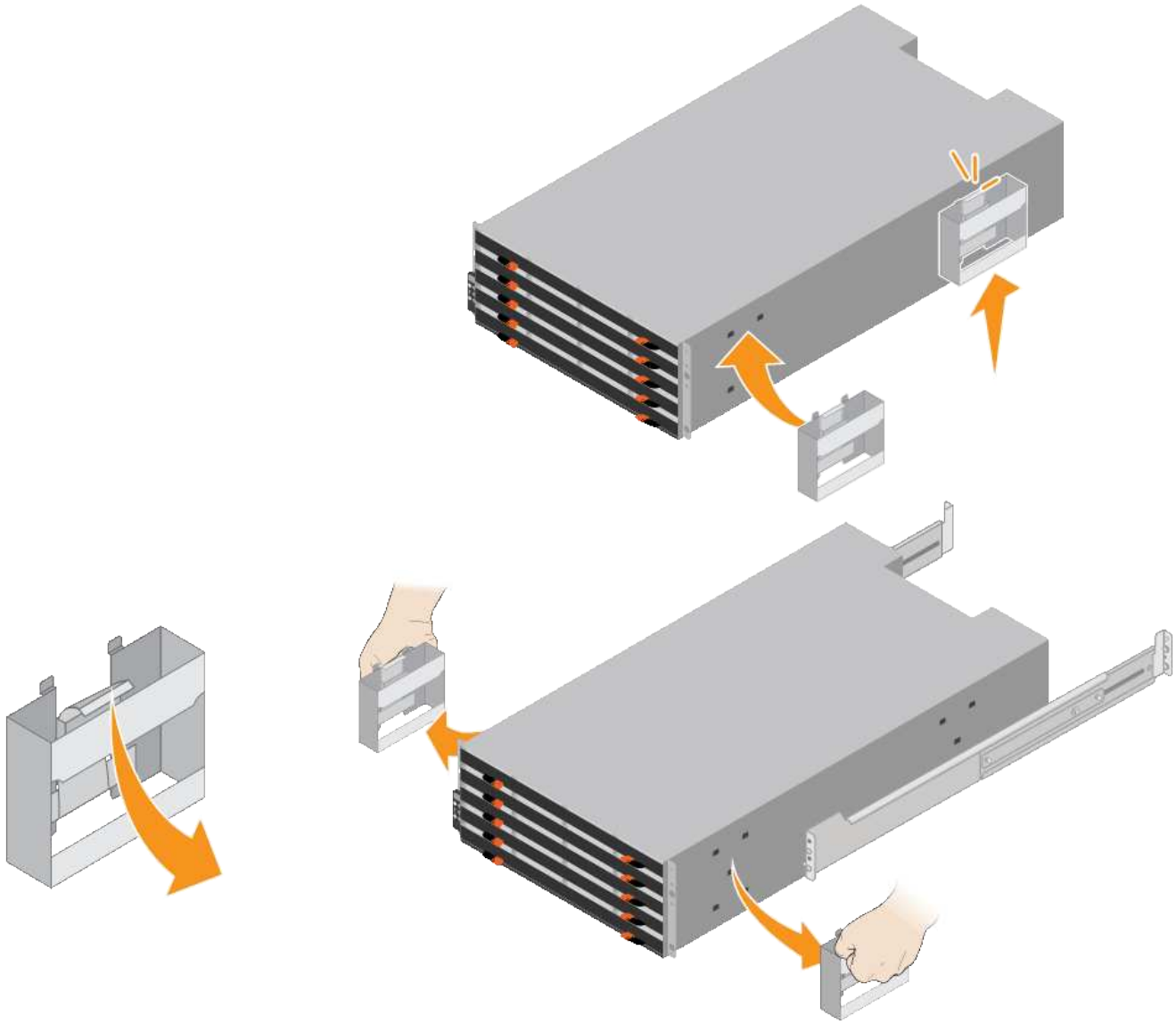
Passos

1. Siga cuidadosamente as instruções para o kit de trilho para instalar os trilhos em seu gabinete ou rack.

   Para armários de orifício quadrado, primeiro você deve instalar as porcas de gaiola fornecidas para fixar a parte frontal e traseira da prateleira com parafusos.

2. Retire a caixa de embalagem exterior do aparelho. Em seguida, dobre as abas na caixa interna.
3. Se estiver a levantar o aparelho à mão, fixe as quatro pegas nas laterais do chassis.

   Empurre cada alça para cima até que ela se encaixe no lugar.



4. Coloque a parte de trás da prateleira (a extremidade com os conetores) nos trilhos.
5. Apoiando a prateleira de baixo, deslize-a para dentro do gabinete. Se você estiver usando as alças, use as travas para soltar uma alça de cada vez enquanto você desliza a prateleira para dentro.

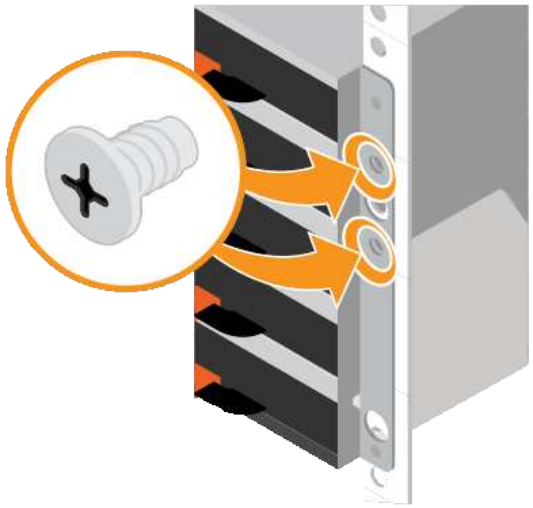
   Para remover as pegas, puxe para trás o trinco de desbloqueio, empurre-o para baixo e, em seguida, puxe-o para fora da prateleira.

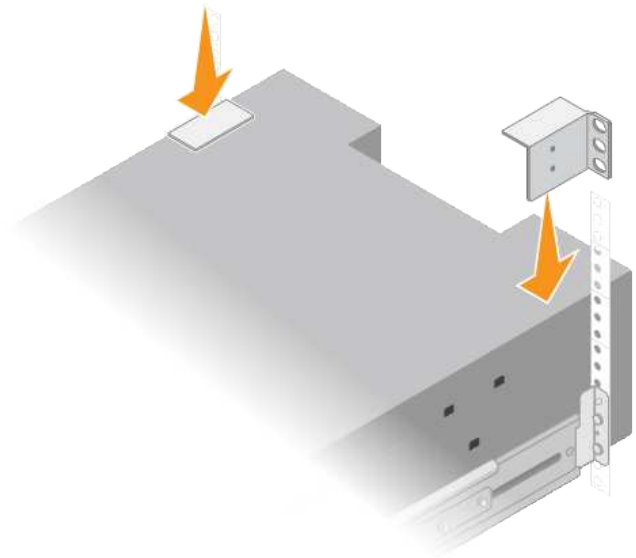
6. Fixe a prateleira na parte frontal do gabinete.

   Insira os parafusos no primeiro e terceiro orifícios a partir da parte superior da prateleira em ambos os lados.

7. Fixe a prateleira na parte de trás do armário.

   Coloque dois suportes traseiros em cada lado da secção traseira superior da prateleira. Insira os parafusos no primeiro e terceiro orifícios de cada suporte.





8. Repita essas etapas para qualquer gaveta de expansão.

SG6060: Instalar as unidades

Depois de instalar o compartimento de 60 unidades em um gabinete ou rack, você deve instalar todas as unidades 60 na gaveta. O envio para o compartimento de controladora E2860 inclui duas unidades SSD, que devem ser instaladas na gaveta superior do compartimento de controladora. Cada compartimento de expansão opcional inclui 60 unidades HDD e nenhuma unidade SSD.

O que você vai precisar

Você instalou o compartimento de controladora E2860 ou as gavetas de expansão opcionais (uma ou duas) no gabinete ou no rack.

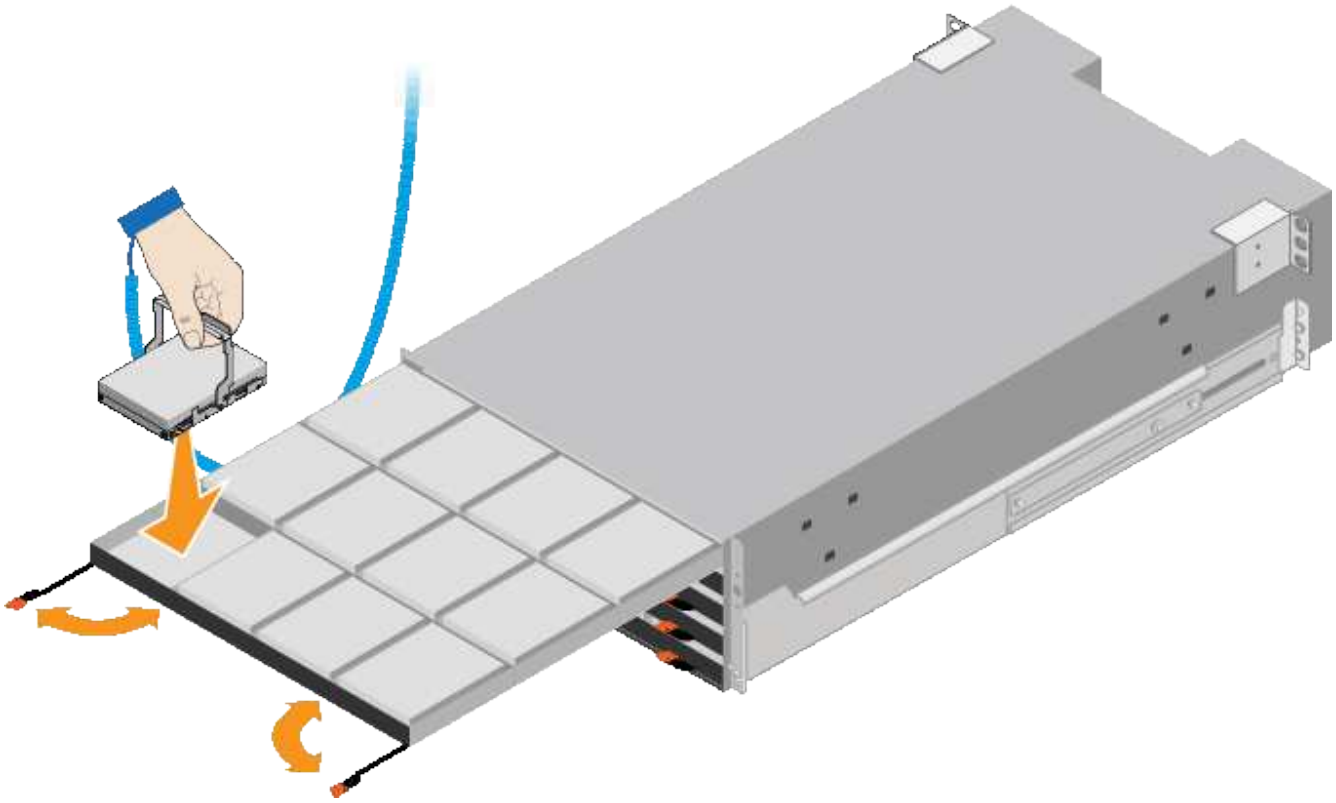
> Para evitar danificar o hardware, nunca mova a gaveta se as unidades estiverem instaladas. É necessário remover todas as unidades antes de mover a gaveta.

Passos

1. Enrole a extremidade da correia da pulseira ESD à volta do pulso e fixe a extremidade do clipe a um solo metálico para evitar descargas estáticas.
2. Remova as unidades da embalagem.
3. Solte as alavancas na gaveta superior da unidade e deslize a gaveta para fora usando as alavancas.
4. Localize as duas unidades SSD.

   > Os compartimentos de expansão não usam unidades SSD.

5. Levante cada manípulo de acionamento para uma posição vertical.
6. Instale as duas unidades SSD nos slots 0 e 1 (os dois primeiros slots ao longo do lado esquerdo da gaveta).
7. Posicione cuidadosamente cada unidade na respetiva ranhura e baixe a pega da unidade levantada até encaixar.



8. Instale 10 unidades HDD na gaveta superior.
9. Deslize a gaveta para dentro novamente empurrando o centro e fechando ambas as alavancas com cuidado.

> Pare de empurrar a gaveta se sentir preso. Use as alavancas de liberação na parte frontal da gaveta para deslizar a gaveta para fora. Em seguida, reinsira cuidadosamente a gaveta na ranhura.

10. Repita estes passos para instalar unidades HDD nas outras quatro gavetas.

> Você deve instalar todas as unidades 60 para garantir o funcionamento correto.

11. Fixe a moldura frontal à prateleira.
12. Se você tiver compartimentos de expansão, repita estas etapas para instalar 12 unidades HDD em cada gaveta de cada gaveta de expansão.
13. Avance para as instruções de instalação do SG6000-CN em um gabinete ou rack.

SGF6024: Instalação de compartimentos de 24 unidades em um gabinete ou rack

Você deve instalar um conjunto de trilhos para o compartimento do controlador EF570 em seu gabinete ou rack e, em seguida, deslizar o array para os trilhos.

O que você vai precisar

- Você revisou o documento de Avisos de segurança incluído na caixa e entendeu as precauções para mover e instalar hardware.
- Você tem as instruções fornecidas com o kit de trilho.

Passos

1. Siga cuidadosamente as instruções para o kit de trilho para instalar os trilhos em seu gabinete ou rack.

   Para armários de orifício quadrado, primeiro você deve instalar as porcas de gaiola fornecidas para fixar a parte frontal e traseira da prateleira com parafusos.

2. Retire a caixa de embalagem exterior do aparelho. Em seguida, dobre as abas na caixa interna.
3. Coloque a parte de trás da prateleira (a extremidade com os conetores) nos trilhos.

   Uma prateleira totalmente carregada pesa aproximadamente 52 lb (24 kg). São necessárias duas pessoas para mover o armário com segurança.

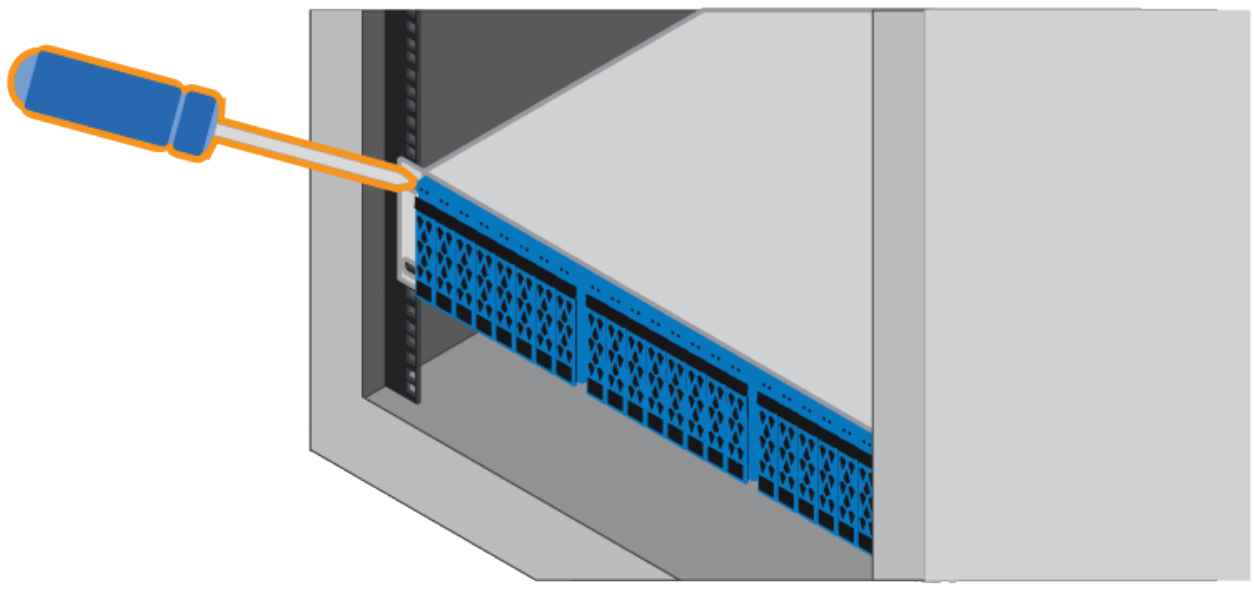
4. Deslize cuidadosamente o compartimento até os trilhos.

   Talvez seja necessário ajustar os trilhos para garantir que o gabinete deslize totalmente para os trilhos.

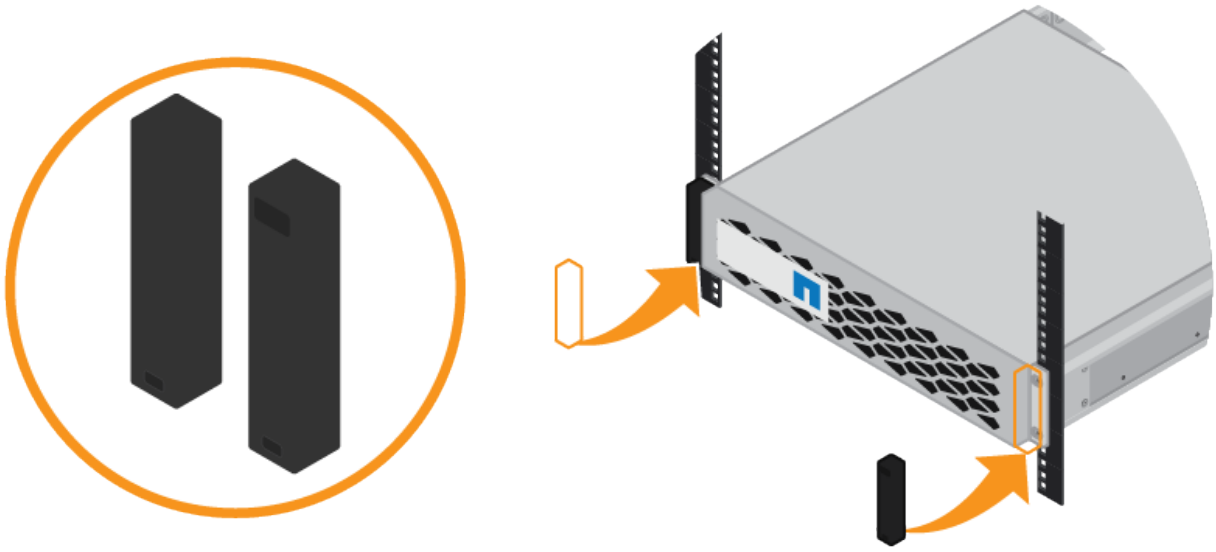
   Não coloque equipamento adicional nos trilhos depois de concluir a instalação do compartimento. Os trilhos não são projetados para suportar peso adicional.

   Se aplicável, talvez seja necessário remover as tampas da extremidade da prateleira ou a moldura do sistema para fixar o compartimento ao poste do rack; se for o caso, você precisará substituir as tampas da extremidade ou a moldura quando terminar.

5. Prenda o gabinete à parte frontal do gabinete ou rack e trilhos inserindo dois parafusos M5 através dos suportes de montagem (pré-instalados em ambos os lados da parte frontal do gabinete), os orifícios no rack ou no gabinete do sistema e os orifícios na parte frontal dos trilhos.



6. Fixe o compartimento na parte de trás dos trilhos inserindo dois parafusos M5 através dos suportes no compartimento e no suporte do kit de trilho.
7. Se aplicável, substitua as tampas da extremidade da prateleira ou a moldura do sistema.



SG6000-CN: Instalação em um gabinete ou rack

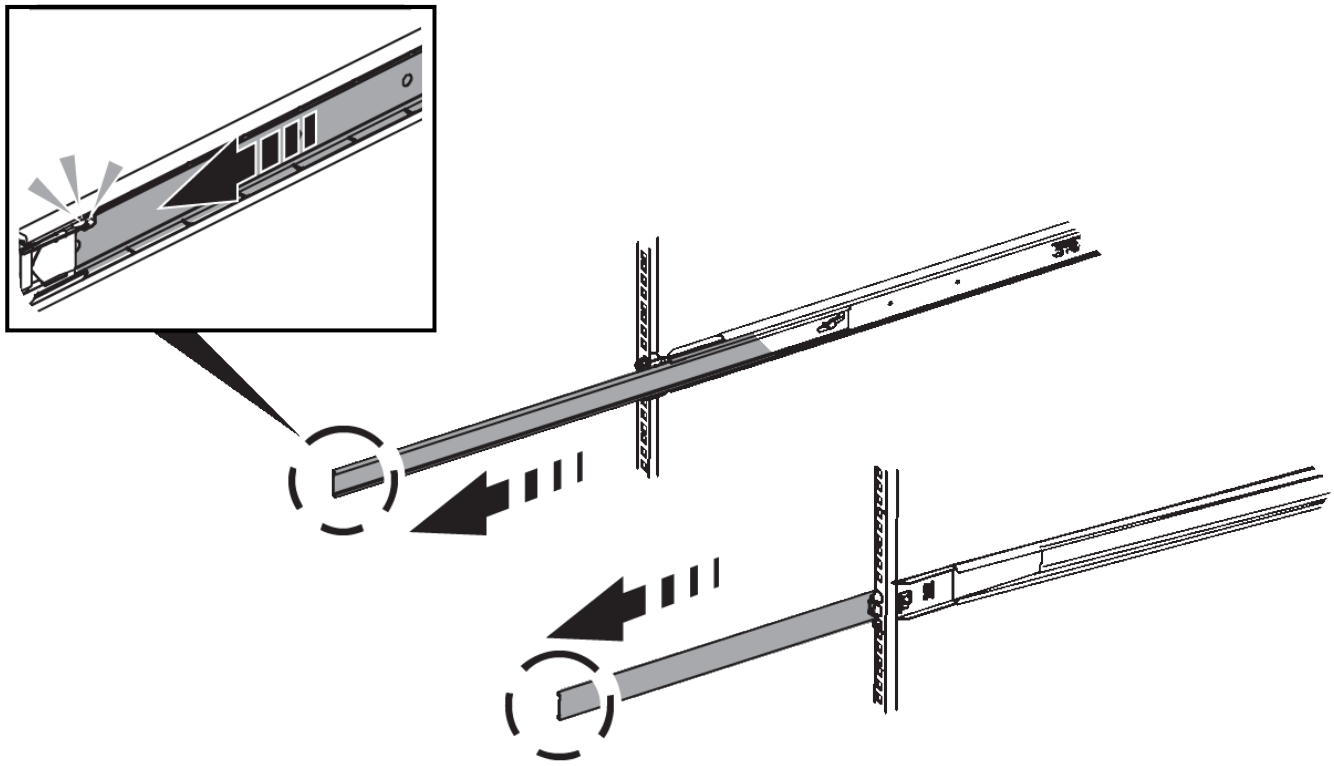
Você deve instalar um conjunto de trilhos para o controlador SG6000-CN em seu gabinete ou rack e, em seguida, deslizar o controlador para os trilhos.

O que você vai precisar

- Você revisou o documento de Avisos de segurança incluído na caixa e entendeu as precauções para mover e instalar hardware.
- Você tem as instruções fornecidas com o kit de trilho.
- Você instalou o compartimento de controladora e as unidades E2860 ou o compartimento de controladora EF570.

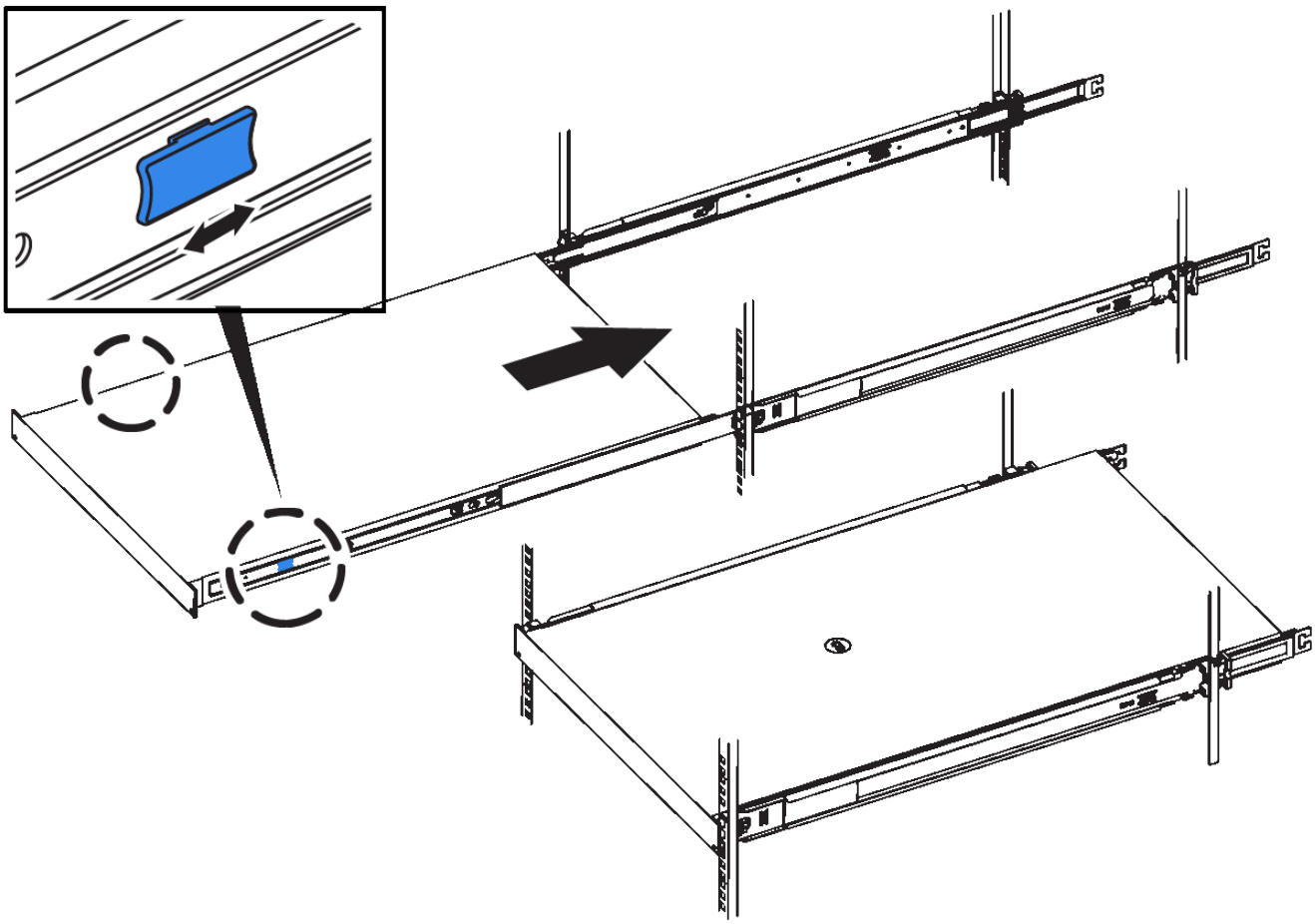
Passos

1. Siga cuidadosamente as instruções para o kit de trilho para instalar os trilhos em seu gabinete ou rack.
2. Nos dois trilhos instalados no gabinete ou rack, estenda as partes móveis dos trilhos até ouvir um clique.



3. Insira o controlador SG6000-CN nos trilhos.
4. Deslize o controlador para dentro do gabinete ou rack.

   Quando não conseguir mover o controlador mais, puxe os trincos azuis em ambos os lados do chassis para deslizar o controlador até ao fim.



Não conete a moldura frontal até que você ligue o controlador.

5. Aperte os parafusos integrados no painel frontal do controlador para fixar o controlador no rack.

Cabeamento do aparelho (SG6000)

Você deve conetar os controladores de armazenamento ao controlador SG6000-CN, conetar as portas de gerenciamento em todos os três controladores e conetar as portas de rede no controlador SG6000-CN à rede de grade e à rede cliente opcional para StorageGRID.

O que você vai precisar

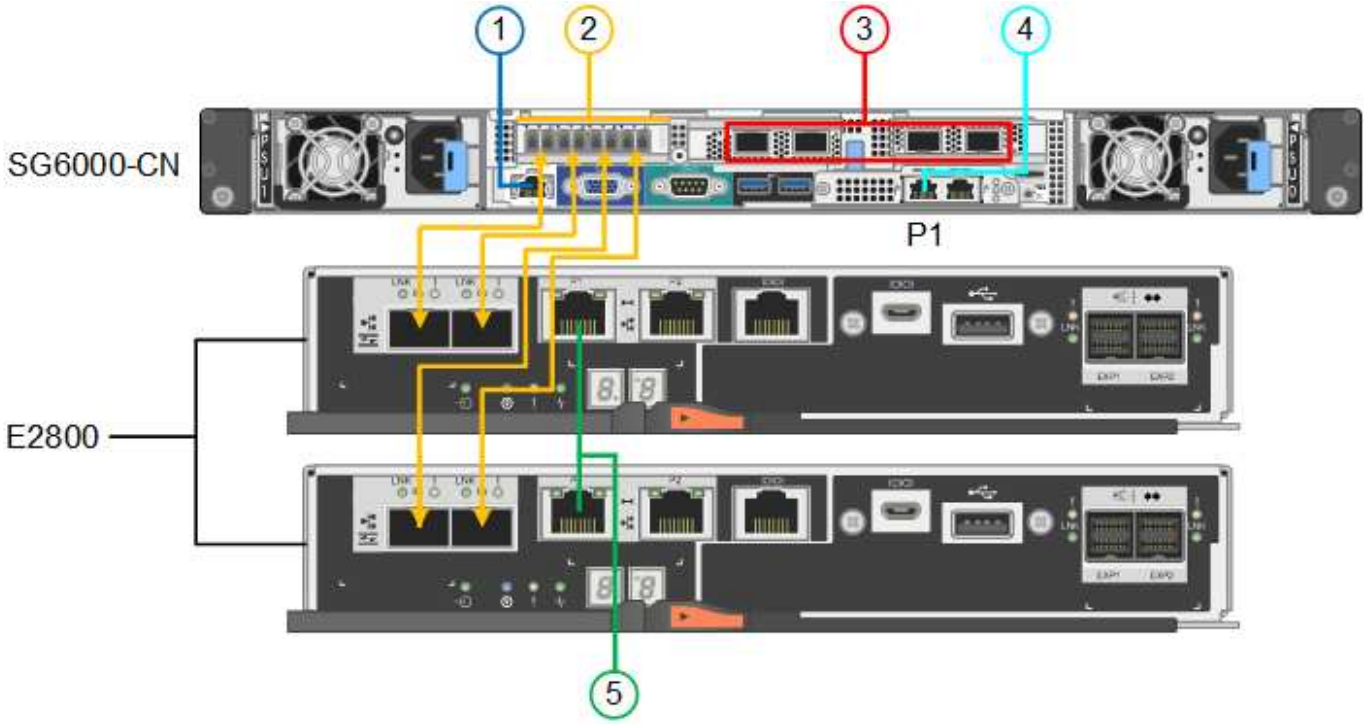
- Você tem os quatro cabos óticos fornecidos com o aparelho para conetar os dois controladores de armazenamento ao controlador SG6000-CN.
- Você tem cabos Ethernet RJ-45 (quatro no mínimo) para conetar as portas de gerenciamento.
- Tem uma das seguintes opções para as portas de rede. Estes itens não são fornecidos com o aparelho.
  - Um a quatro cabos Twinax para ligar as quatro portas de rede.

◦ Um a quatro transcetores SFP ou SFP28G se você planeja usar cabos óticos para as portas.

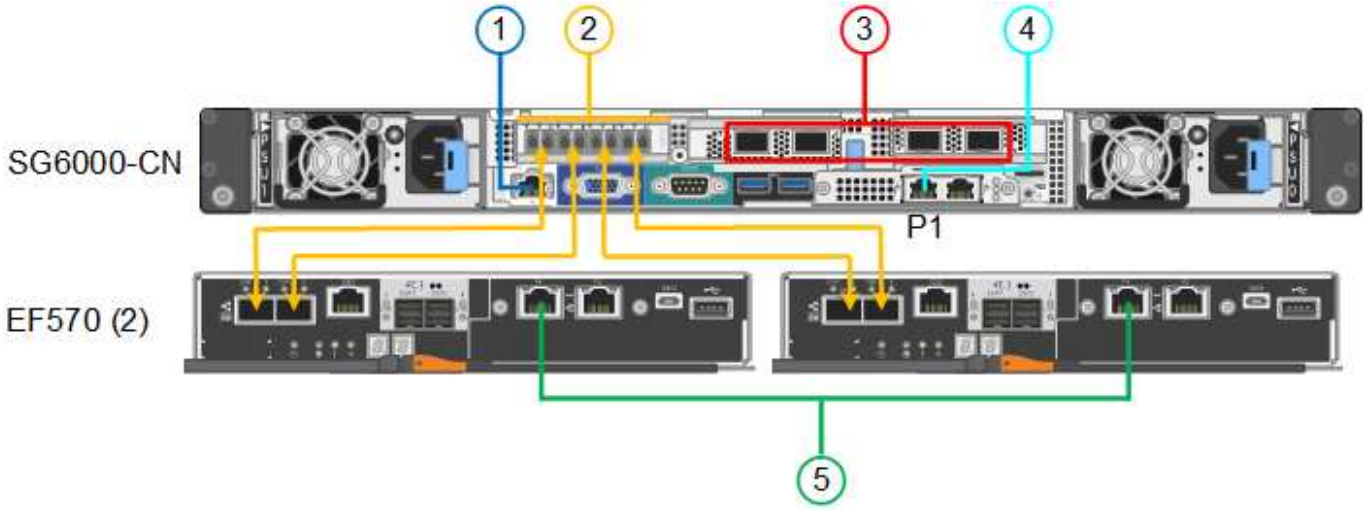
Risco de exposição à radiação laser — não desmonte nem remova qualquer parte de um transcetor SFP. Você pode estar exposto à radiação laser.

Sobre esta tarefa

A figura a seguir mostra os três controladores no dispositivo SG6060, com o controlador de computação SG6000-CN na parte superior e os dois controladores de storage E2800 na parte inferior.



A figura a seguir mostra as três controladoras no dispositivo SGF6024, com o controlador de computação SG6000-CN na parte superior e as duas controladoras de storage EF570 lado a lado abaixo do controlador de computação.



	Porta	Tipo de porta	Função
1	Porta de gerenciamento BMC no controlador SG6000-CN	1 GbE (RJ-45)	Liga-se à rede onde acede à interface BMC.
2	Portas de conexão FC: • 4 no controlador SG6000-CN • 2 em cada controlador de storage	SFP ótico FC de 16 GB/s.	Ligue cada controlador de armazenamento ao controlador SG6000-CN.
3	Quatro portas de rede no controlador SG6000-CN	10/25-GbE	Conete-se à rede de grade e à rede de cliente para StorageGRID.
4	Porta Admin Network no controlador SG6000-CN (identificada como P1 na figura)	1 GbE (RJ-45) **Importante:** esta porta funciona apenas a 1000 BaseT/full e não suporta velocidades de 10 ou 100 megabits.	Liga o controlador SG6000-CN à rede de administração para StorageGRID.
4	Porta RJ-45 mais à direita no controlador SG6000-CN	1 GbE (RJ-45) **Importante:** esta porta funciona apenas a 1000 BaseT/full e não suporta velocidades de 10 ou 100 megabits.	• Pode ser ligado com a porta de gerenciamento 1 se você quiser uma conexão redundante com a rede de administração. • Pode ser deixado sem fios e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, pode ser utilizado para ligar o controlador SG6000-CN a um computador portátil de serviço se os endereços IP atribuídos por DHCP não estiverem disponíveis.

	Porta	Tipo de porta	Função
5	Porta de gerenciamento 1 em cada controlador de storage	1 GbE (RJ-45)	Liga-se à rede onde acede ao Gestor de sistema SANtricity.
5	Porta de gerenciamento 2 em cada controlador de storage	1 GbE (RJ-45)	Reservado para suporte técnico.

Passos

1. Conete a porta de gerenciamento BMC no controlador SG6000-CN à rede de gerenciamento, usando um cabo Ethernet.

   Embora essa conexão seja opcional, recomenda-se facilitar o suporte.

2. Conete as duas portas FC em cada controlador de storage às portas FC no controlador SG6000-CN, usando quatro cabos óticos e quatro transcetores SFP mais para os controladores de storage.
3. Conete as portas de rede do controlador SG6000-CN aos switches de rede apropriados, usando cabos Twinax ou cabos óticos e transcetores SFP ou SFP28.

   > As quatro portas de rede devem usar a mesma velocidade de link. Instale transcetores SFP se você planeja usar velocidades de link de 10 GbE. Instale os transcetores SFP28 se você planeja usar velocidades de link de 25 GbE.

   - Se você planeja usar o modo de ligação de porta fixa (padrão), conete as portas à rede StorageGRID e às redes de clientes, conforme mostrado na tabela.

Porta	Liga a…
Porta 1	Rede cliente (opcional)
Porta 2	Rede de rede
Porta 3	Rede cliente (opcional)
Porta 4	Rede de rede

   - Se você planeja usar o modo de ligação de porta agregada, conete uma ou mais portas de rede a um ou mais switches. Você deve conetar pelo menos duas das quatro portas para evitar ter um único ponto de falha. Se você usar mais de um switch para uma única ligação LACP, os switches devem suportar MLAG ou equivalente.
4. Se pretender utilizar a rede de administração para StorageGRID, ligue a porta de rede de administração do controlador SG6000-CN à rede de administração, utilizando um cabo Ethernet.
5. Conete a porta de gerenciamento 1 (P1) em cada controlador de storage (a porta RJ-45 à esquerda) à rede de gerenciamento do Gerenciador de sistemas SANtricity, usando um cabo Ethernet.

   Não use a porta de gerenciamento 2 (P2) nos controladores de storage (a porta RJ-45 à direita). Esta porta está reservada para suporte técnico.

Informações relacionadas

"Modos de ligação de porta para o controlador SG6000-CN"

"Reinstalar o controlador SG6000-CN em um gabinete ou rack"

SG6060: Cabeamento das gavetas de expansão opcionais

Se você estiver usando gavetas de expansão, será necessário conectá-los ao compartimento de controladora E2860. Você pode ter no máximo duas gavetas de expansão para cada dispositivo SG6060.

O que você vai precisar

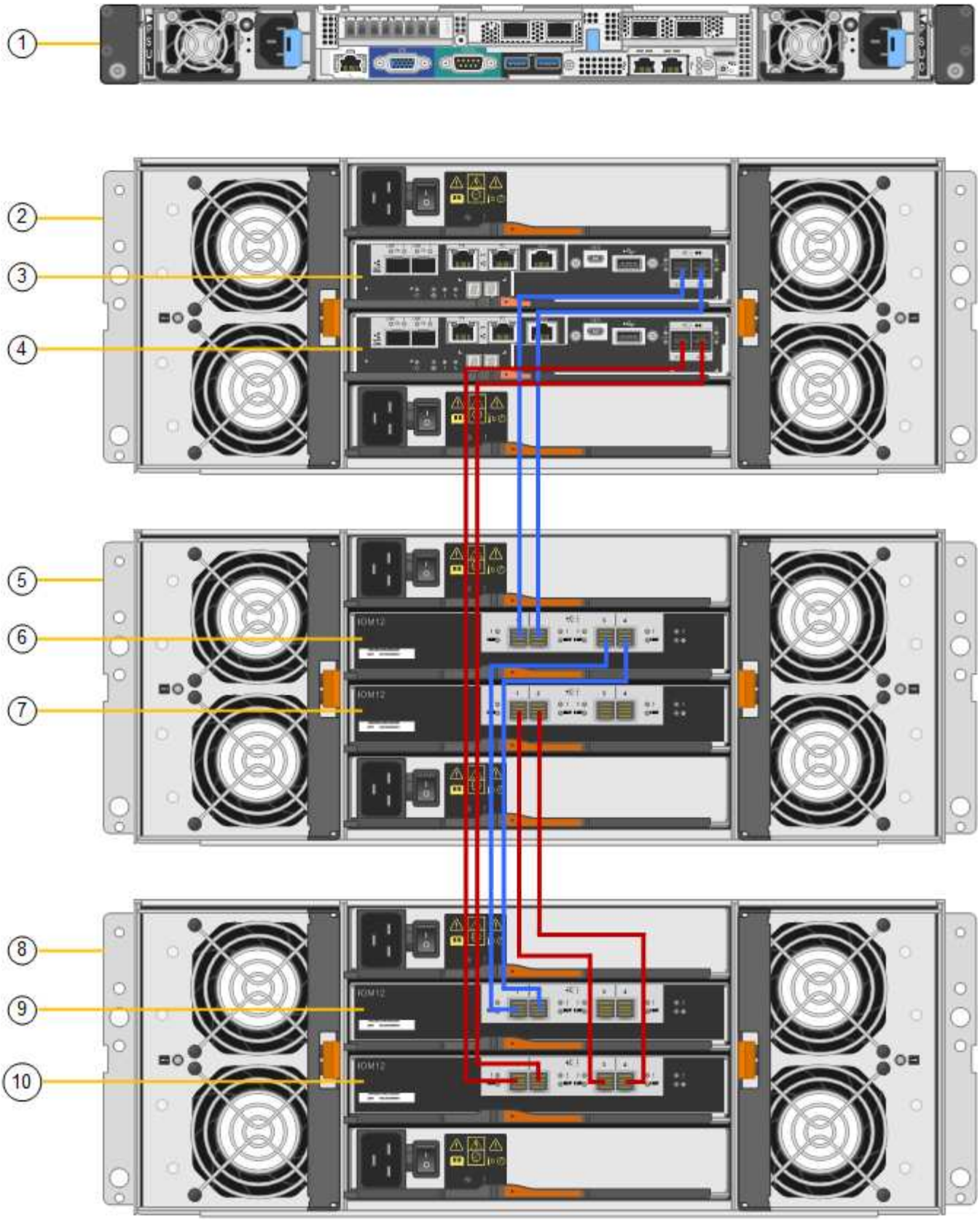
- Você tem os dois cabos SAS fornecidos com cada compartimento de expansão.
- Você instalou as gavetas de expansão no gabinete ou rack que contém o compartimento de controladora E2860.

  "SG6060: Instalação de compartimentos de 60 unidades em um gabinete ou rack"

Passo

Conete cada compartimento de expansão ao compartimento de controladora E2860, conforme mostrado no diagrama.

Este desenho mostra duas prateleiras de expansão. Se tiver apenas uma, ligue a IOM A ao controlador A e ligue a IOM B ao controlador B.



	Descrição
1	SG6000-CN

	Descrição
2	Compartimento do controlador de E2860 TB
3	Controlador A
4	Controlador B
5	Compartimento de expansão 1
6	IOM A para compartimento de expansão 1
7	IOM B para compartimento de expansão 1
8	Compartimento de expansão 2
9	IOM A para compartimento de expansão 2
10	IOM B para compartimento de expansão 2

Conexão dos cabos de alimentação e alimentação de energia (SG6000)

Depois de conetar os cabos de rede, você estará pronto para aplicar energia ao controlador SG6000-CN e aos dois controladores de armazenamento ou compartimentos de expansão opcionais.

Passos

1. Confirme se as duas controladoras no compartimento de controladora de storage estão desligadas.

> **Risco de choque elétrico** — antes de ligar os cabos de alimentação, certifique-se de que os interrutores de alimentação de cada um dos dois controladores de armazenamento estão desligados.

2. Se você tiver gavetas de expansão, confirme se ambos os interruptores de energia da IOM estão desligados.

> **Risco de choque elétrico** — antes de conetar os cabos de alimentação, certifique-se de que os dois interrutores de alimentação de cada uma das prateleiras de expansão estão desligados.

3. Ligue um cabo de alimentação a cada uma das duas unidades de alimentação do controlador SG6000-CN.
4. Conete esses dois cabos de alimentação a duas unidades de distribuição de energia (PDUs) diferentes no gabinete ou no rack.
5. Conete um cabo de alimentação a cada uma das duas unidades de fonte de alimentação no compartimento do controlador de armazenamento.
6. Se você tiver compartimentos de expansão, conete um cabo de alimentação a cada uma das duas

unidades de fonte de alimentação em cada compartimento de expansão.

7. Conete os dois cabos de energia em cada compartimento de armazenamento (incluindo as gavetas de expansão opcionais) a duas PDUs diferentes no gabinete ou no rack.
8. Se o botão liga/desliga na parte frontal do controlador SG6000-CN não estiver aceso a azul, prima o botão para ligar o controlador.

   Não volte a premir o botão de alimentação durante o processo de ativação.

9. Ligue os dois interruptores de energia na parte de trás do compartimento do controlador de armazenamento. Se você tiver compartimentos de expansão, ligue os dois interruptores de energia para cada compartimento.
   - Não desligue os interrutores de alimentação durante o processo de ativação.
   - Os ventiladores na gaveta do controlador de storage e nas gavetas de expansão opcionais podem ser muito altos quando são iniciados pela primeira vez. O ruído alto durante o arranque é normal.
10. Depois que os componentes iniciarem, verifique seu status.
    - Verifique o visor de sete segmentos na parte de trás de cada controlador de armazenamento. Consulte o artigo sobre como visualizar códigos de status de inicialização para obter mais informações.
    - Verifique se o botão de alimentação na parte frontal do controlador SG6000-CN está aceso.
11. Se ocorrerem erros, corrija quaisquer problemas.
12. Fixe a moldura frontal ao controlador SG6000-CN.

Informações relacionadas

"Exibindo códigos de status de inicialização para os controladores de storage SG6000"

"Visualizar indicadores de estado e botões no controlador SG6000-CN"

"Reinstalar o controlador SG6000-CN em um gabinete ou rack"

Visualizar indicadores de estado e botões no controlador SG6000-CN

O controlador SG6000-CN inclui indicadores que o ajudam a determinar o estado do controlador, incluindo os seguintes indicadores e botões.

	Visor	Descrição
1	Botão de alimentação	• Azul: O controlador está ligado. • Desligado: O controlador está desligado.

	Visor	Descrição
2	Botão Reset (Repor)	*Nenhum indicador* Utilize este botão para executar uma reinicialização total do controlador.
3	Botão identificar	• Azul intermitente ou contínuo: Identifica o controlador no gabinete ou rack. • Desligado: O controlador não é visualmente identificável no gabinete ou rack. Este botão pode ser definido como intermitente, ligado (sólido) ou desligado.
4	LED de alarme	• Âmbar: Ocorreu um erro. **Nota:** para visualizar os códigos de inicialização e erro, você deve acessar a interface do BMC. • Desligado: Nenhum erro está presente.

Códigos gerais de arranque

Durante a inicialização ou após uma reinicialização forçada do controlador SG6000-CN, ocorre o seguinte:

1. O controlador de gerenciamento de placa base (BMC) Registra códigos para a sequência de inicialização, incluindo quaisquer erros que ocorram.
2. O botão liga/desliga acende-se.
3. Se ocorrerem erros durante a inicialização, o LED de alarme acende-se.

   Para exibir os códigos de inicialização e erro, você deve acessar a interface do BMC.

Informações relacionadas

"Solução de problemas da instalação do hardware"

"Configurando a interface BMC"

"Ligar o controlador SG6000-CN e verificar a operação"

Exibindo códigos de status de inicialização para os controladores de storage SG6000

Cada controlador de storage tem uma tela de sete segmentos que fornece códigos de status à medida que o controlador liga. Os códigos de status são os mesmos para o

controlador E2800 e o controlador EF570.

Sobre esta tarefa

Para obter descrições desses códigos, consulte as informações de monitoramento do sistema e-Series para o tipo de controlador de storage.

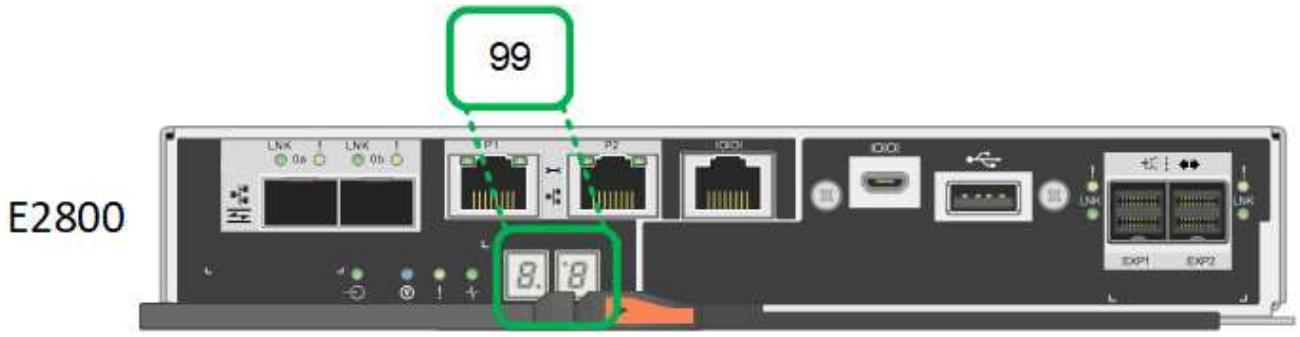
Passos

1. Durante a inicialização, monitore o progresso visualizando os códigos mostrados no visor de sete segmentos para cada controlador de armazenamento.

   A exibição de sete segmentos em cada controlador de armazenamento mostra a sequência repetida **os**, **SD**, ***blank*** para indicar que o controlador está executando o processamento de início do dia.

2. Após a inicialização dos controladores, confirme se cada controlador de armazenamento mostra 99, que é o ID padrão para um compartimento de controladora e-Series.

   Certifique-se de que esse valor seja exibido em ambos os controladores de storage, como mostrado neste exemplo E2800 controlador.



3. Se um ou ambos os controladores mostrarem outros valores, consulte as informações sobre como solucionar problemas da instalação do hardware e confirme que você concluiu as etapas de instalação corretamente. Se não conseguir resolver o problema, contacte o suporte técnico.

Informações relacionadas

"Guia de monitorização do sistema E5700 e E2800"

"Solução de problemas da instalação do hardware"

"Suporte à NetApp"

"Ligar o controlador SG6000-CN e verificar a operação"

Configurar o hardware

Depois de aplicar energia ao aparelho, você deve configurar as conexões de rede que serão usadas pelo StorageGRID. É necessário configurar o Gerenciador de sistemas do SANtricity, que é o software que você usará para monitorar as controladoras de storage e outro hardware no compartimento da controladora. Você também deve garantir que você pode acessar a interface BMC para o controlador SG6000-CN.

Passos

- "Configurando conexões StorageGRID"

- "Acessando e configurando o Gerenciador do sistema do SANtricity"
- "Configurando a interface BMC"
- "Opcional: Habilitando a criptografia de nó"
- "Opcional: Alterar o modo RAID (apenas SG6000)"
- "Opcional: Remapeamento de portas de rede para o dispositivo"

Configurando conexões StorageGRID

Antes de implantar um dispositivo StorageGRID como nó de armazenamento em um sistema StorageGRID, você deve configurar as conexões entre o dispositivo e as redes que você planeja usar. Você pode configurar a rede navegando até o Instalador de dispositivos StorageGRID, que é pré-instalado no controlador SG6000-CN (o controlador de computação).

Passos

- "Acessando o instalador do StorageGRID Appliance"
- "Verificando e atualizando a versão do Instalador de dispositivos StorageGRID"
- "Configurando links de rede (SG6000)"
- "Configurando endereços IP do StorageGRID"
- "Verificando conexões de rede"
- "Verificando conexões de rede no nível da porta"

Acessando o instalador do StorageGRID Appliance

Você deve acessar o Instalador do StorageGRID Appliance para verificar a versão do instalador e configurar as conexões entre o appliance e as três redes StorageGRID: A rede de grade, a rede de administração (opcional) e a rede de cliente (opcional).

O que você vai precisar

- Você está usando qualquer cliente de gerenciamento que possa se conetar à rede de administração do StorageGRID ou tem um laptop de serviço.
- O cliente ou laptop de serviço tem um navegador da Web suportado.
- O controlador SG6000-CN está ligado a todas as redes StorageGRID que pretende utilizar.
- Você conhece o endereço IP, o gateway e a sub-rede do controlador SG6000-CN nessas redes.
- Configurou os comutadores de rede que pretende utilizar.

Sobre esta tarefa

Para acessar inicialmente o Instalador de dispositivos StorageGRID, você pode usar o endereço IP atribuído pelo DHCP para a porta de rede Admin no controlador SG6000-CN (assumindo que o controlador esteja conetado à rede Admin) ou conetar um laptop de serviço diretamente ao controlador SG6000-CN.

Passos

1. Se possível, use o endereço DHCP para a porta de rede de administração no controlador SG6000-CN para acessar o Instalador de dispositivos StorageGRID.

a. Localize a etiqueta de endereço MAC na parte frontal do controlador SG6000-CN e determine o endereço MAC da porta Admin Network.

   O rótulo de endereço MAC lista o endereço MAC da porta de gerenciamento BMC.

   Para determinar o endereço MAC da porta Admin Network, você deve adicionar **2** ao número hexadecimal na etiqueta. Por exemplo, se o endereço MAC na etiqueta terminar em **09**, o endereço MAC da porta Admin terminaria em **0B**. Se o endereço MAC na etiqueta terminar em **(*y*)FF**, o endereço MAC da porta Admin terminaria em **(*y*(1)01**. Você pode facilmente fazer esse cálculo abrindo o Calculator no Windows, definindo-o para o modo Programador, selecionando Hex, digitando o endereço MAC e, em seguida, digitando * 2 *.

b. Forneça o endereço MAC ao administrador da rede para que ele possa procurar o endereço DHCP do dispositivo na rede Admin.

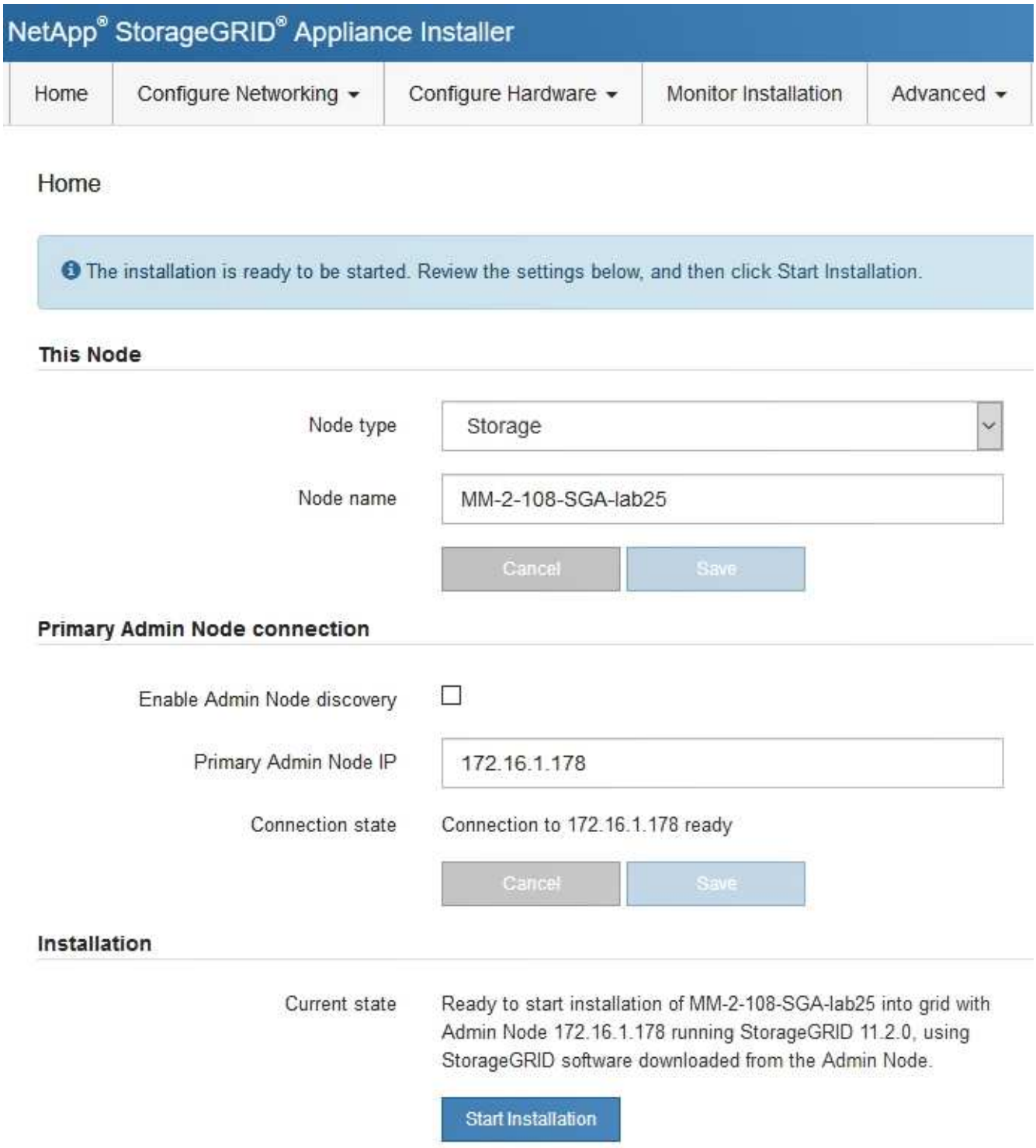
c. No cliente, insira esta URL para o instalador do StorageGRID Appliance
   `https://Appliance_Controller_IP:8443`

   Para *`SG6000-CN_Controller_IP`*, utilize o endereço DHCP.

d. Se for solicitado um alerta de segurança, exiba e instale o certificado usando o assistente de instalação do navegador.

   O alerta não aparecerá na próxima vez que você acessar este URL.

   A página inicial do instalador do dispositivo StorageGRID é exibida. As informações e as mensagens mostradas quando você acessa esta página pela primeira vez dependem de como o dispositivo está conetado atualmente às redes StorageGRID. Podem aparecer mensagens de erro que serão resolvidas em etapas posteriores.



2. Se não conseguir obter um endereço IP utilizando DHCP, pode utilizar uma ligação local.

   a. Conete um laptop de serviço diretamente à porta RJ-45 mais à direita do controlador SG6000-CN, usando um cabo Ethernet.

   b. Abra um navegador da Web no laptop de serviço.

c. Digite este URL para o instalador do StorageGRID Appliance
`https://169.254.0.1:8443`

A página inicial do instalador do dispositivo StorageGRID é exibida. As informações e as mensagens apresentadas quando acede pela primeira vez a esta página dependem da forma como o seu aparelho está atualmente ligado.

> Se não conseguir aceder à página inicial através de uma ligação local, configure o endereço IP do computador portátil de serviço como `169.254.0.2`, e tente novamente.

Depois de terminar

Depois de acessar o Instalador de dispositivos StorageGRID:

- Verifique se a versão do Instalador de dispositivos StorageGRID no dispositivo corresponde à versão de software instalada no sistema StorageGRID. Atualize o Instalador de dispositivos StorageGRID, se necessário.

  "Verificando e atualizando a versão do Instalador de dispositivos StorageGRID"

- Revise todas as mensagens exibidas na página inicial do Instalador do StorageGRID Appliance e configure a configuração do link e a configuração do IP, conforme necessário.

Informações relacionadas

"Requisitos do navegador da Web"

Verificando e atualizando a versão do Instalador de dispositivos StorageGRID

A versão do Instalador de dispositivos StorageGRID no dispositivo deve corresponder à versão de software instalada no sistema StorageGRID para garantir que todos os recursos do StorageGRID sejam suportados.

O que você vai precisar

Você acessou o Instalador de dispositivos StorageGRID.

Sobre esta tarefa

Os dispositivos StorageGRID vêm da fábrica pré-instalados com o Instalador de dispositivos StorageGRID. Se você estiver adicionando um dispositivo a um sistema StorageGRID atualizado recentemente, talvez seja necessário atualizar manualmente o Instalador de dispositivos StorageGRID antes de instalar o dispositivo como um novo nó.

O Instalador de dispositivos StorageGRID é atualizado automaticamente quando você atualiza para uma nova versão do StorageGRID. Não é necessário atualizar o Instalador de dispositivos StorageGRID nos nós de dispositivos instalados. Este procedimento só é necessário quando estiver a instalar um dispositivo que contenha uma versão anterior do Instalador de dispositivos StorageGRID.

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Avançado Atualização de firmware**.
2. Compare a versão atual do firmware com a versão de software instalada no seu sistema StorageGRID (no Gerenciador de Grade, selecione **Ajuda sobre**).

   O segundo dígito nas duas versões deve corresponder. Por exemplo, se o seu sistema StorageGRID

estiver executando a versão 11.**5**.*x*.*y*, a versão do Instalador de dispositivos StorageGRID deve ser 3.**5**.*z*.

3. Se o aparelho tiver uma versão de nível inferior do instalador do dispositivo StorageGRID, vá para a página de downloads do NetApp para StorageGRID.

   "NetApp Downloads: StorageGRID"

   Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.

4. Baixe a versão apropriada do arquivo **suporte para dispositivos StorageGRID** e o arquivo de checksum correspondente.

   O arquivo de suporte para dispositivos StorageGRID é um `.zip` arquivo que contém as versões de firmware atuais e anteriores para todos os modelos de dispositivos StorageGRID, em subdiretórios para cada tipo de controlador.

   Depois de baixar o arquivo de suporte para o arquivo de dispositivos StorageGRID, extraia o `.zip` arquivo e consulte o arquivo README para obter informações importantes sobre a instalação do Instalador de dispositivos StorageGRID.

5. Siga as instruções na página Atualizar firmware do Instalador de dispositivos StorageGRID para executar estas etapas:
   a. Carregue o ficheiro de suporte apropriado (imagem de firmware) para o seu tipo de controlador e o ficheiro de checksum.
   b. Atualize a partição inativa.
   c. Reinicie e troque partições.
   d. Atualize a segunda partição.

Informações relacionadas

"Acessando o instalador do StorageGRID Appliance"

Configurando links de rede (SG6000)

Você pode configurar links de rede para as portas usadas para conetar o dispositivo à rede de Grade, à rede de cliente e à rede de administração. Você pode definir a velocidade do link, bem como os modos de ligação de porta e rede.

O que você vai precisar

Se você estiver clonando um nó de dispositivo, configure links de rede para o dispositivo de destino para todos os links usados pelo nó do dispositivo de origem.

Se você planeja usar a velocidade de link de 25 GbE:

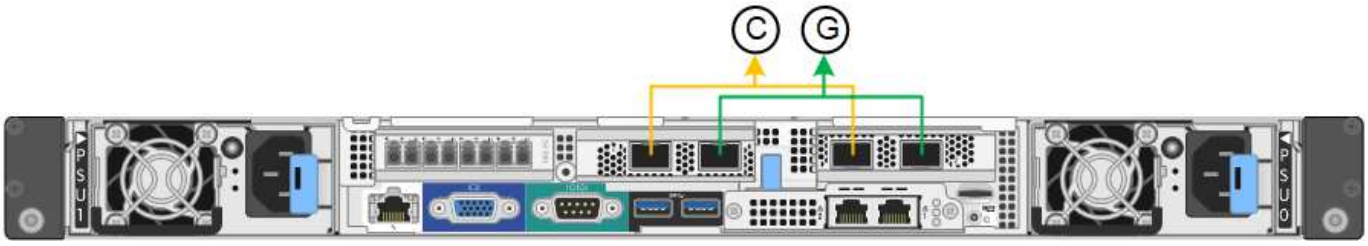
- Você está usando cabos SFP28 Twinax ou instalou transcetores SFP28 nas portas de rede que você planeja usar.
- Você conetou as portas de rede a switches que podem suportar esses recursos.
- Você entende como configurar os interrutores para usar essa velocidade mais alta.

Se você planeja usar o modo de ligação de porta agregada, o modo de ligação de rede LACP ou a marcação de VLAN:

- Você conetou as portas de rede do dispositivo a switches que podem suportar VLAN e LACP.
- Se vários switches estiverem participando da ligação LACP, os switches suportam grupos de agregação de links de vários gabinetes (MLAG) ou equivalente.
- Você entende como configurar os switches para usar VLAN, LACP e MLAG ou equivalente.
- Você conhece a tag VLAN exclusiva a ser usada para cada rede. Essa tag VLAN será adicionada a cada pacote de rede para garantir que o tráfego de rede seja roteado para a rede correta.

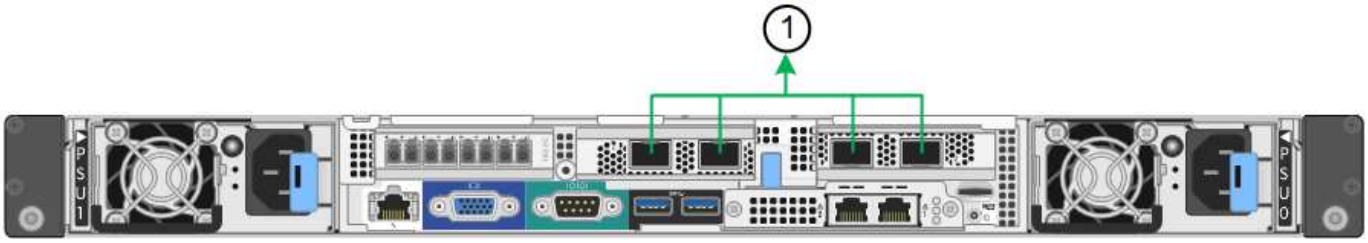
Sobre esta tarefa

Esta figura mostra como as quatro portas de rede são ligadas no modo de ligação de porta fixa (configuração padrão).



	Quais portas estão coladas
C	As portas 1 e 3 são Unidas para a rede do cliente, se esta rede for utilizada.
G	As portas 2 e 4 são Unidas para a rede de Grade.

Esta figura mostra como as quatro portas de rede são ligadas no modo de ligação de porta agregada.



	Quais portas estão coladas
1	Todas as quatro portas são agrupadas em uma única ligação LACP, permitindo que todas as portas sejam usadas para o tráfego de rede de Grade e rede de Cliente.

A tabela resume as opções de configuração das quatro portas de rede. As predefinições são apresentadas a negrito. Só é necessário configurar as definições na página Configuração de ligação se pretender utilizar uma definição não predefinida.

- **Modo de ligação de porta fixo (padrão)**

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Ative-Backup (padrão)	• As portas 2 e 4 usam uma ligação de backup ativo para a rede de Grade. • As portas 1 e 3 não são usadas. • Uma etiqueta VLAN é opcional.	• As portas 2 e 4 usam uma ligação de backup ativo para a rede de Grade. • As portas 1 e 3 usam uma ligação de backup ativo para a rede do cliente. • Tags VLAN podem ser especificadas para ambas as redes para a conveniência do administrador de rede.
Bola de Futsal (802,3ad)	• As portas 2 e 4 usam uma ligação LACP para a rede de Grade. • As portas 1 e 3 não são usadas. • Uma etiqueta VLAN é opcional.	• As portas 2 e 4 usam uma ligação LACP para a rede de Grade. • As portas 1 e 3 usam uma ligação LACP para a rede de clientes. • Tags VLAN podem ser especificadas para ambas as redes para a conveniência do administrador de rede.

- **Modo de ligação de porta agregada**

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Apenas LACP (802,3ad)	• As portas 1-4 usam uma única ligação LACP para a rede de Grade. • Uma única etiqueta VLAN identifica pacotes de rede de Grade.	• As portas 1-4 usam uma única ligação LACP para a rede de Grade e a rede do Cliente. • Duas etiquetas VLAN permitem que os pacotes de rede de Grade sejam segregados dos pacotes de rede de Cliente.

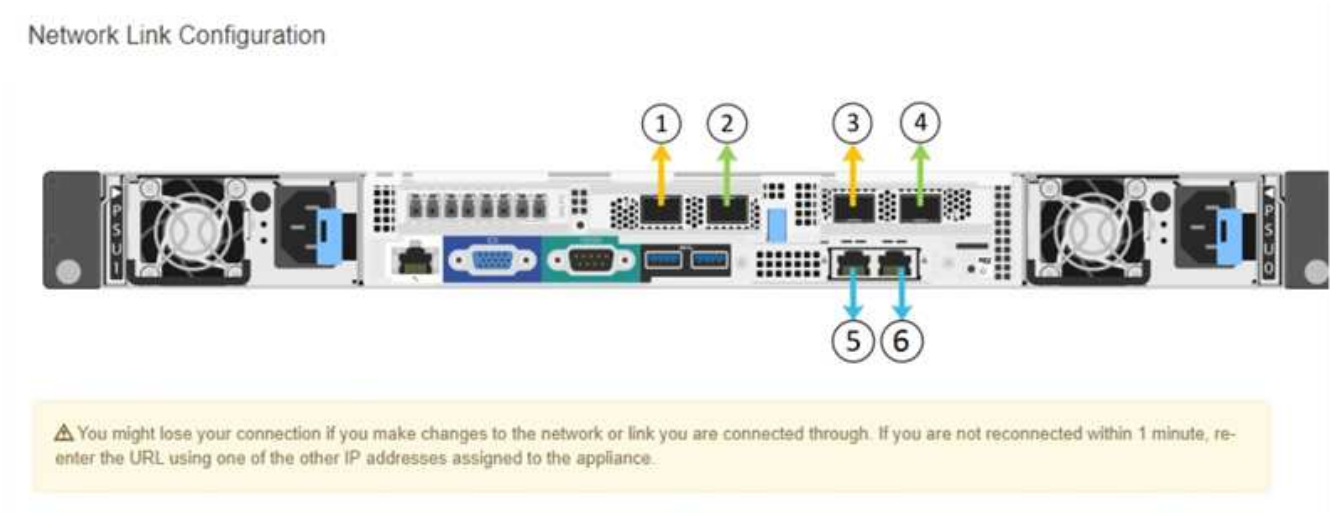
Consulte ""conexões de porta de rede para o controlador SG6000-CN"" para obter mais informações sobre os modos de ligação de porta e ligação de rede.

Esta figura mostra como as duas portas de gerenciamento de 1 GbE no controlador SG6000-CN são ligadas no modo de ligação de rede ative-Backup para a rede Admin.

Passos

1. No Instalador de dispositivos StorageGRID, clique em **Configurar rede Configuração de ligação**.

A página Network Link Configuration (Configuração da ligação de rede) apresenta um diagrama do seu dispositivo com as portas de rede e de gestão numeradas.



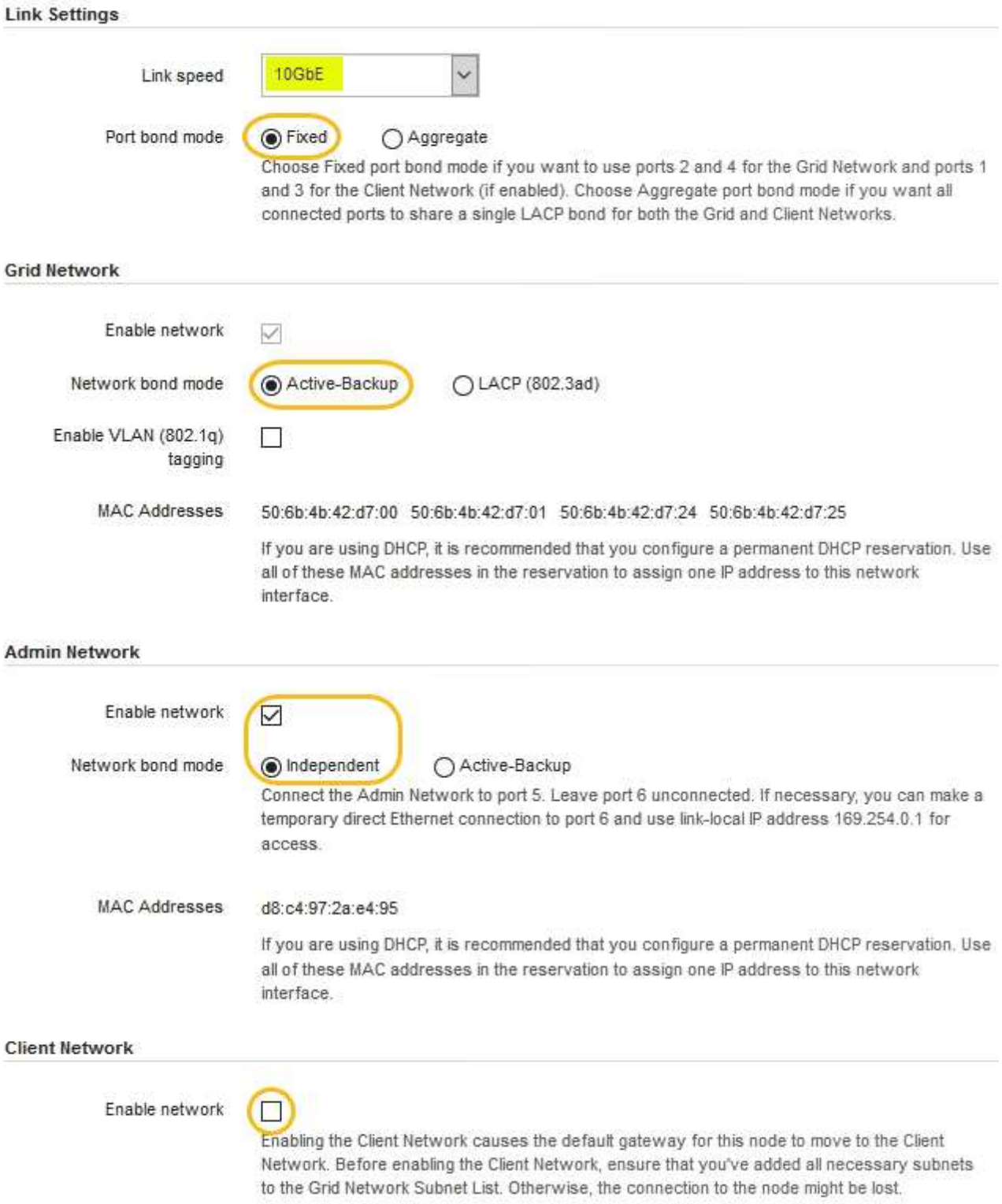
A tabela Status da ligação lista o estado da ligação (para cima/para baixo) e a velocidade (1/10/25/40/100 Gbps) das portas numeradas.

Link Status

Link	State	Speed (Gbps)
1	Up	10
2	Up	10
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

A primeira vez que aceder a esta página:

- **Link Speed** está definido para **10GbE**.
- **Port bond mode** está definido como **Fixed**.
- **O modo de ligação de rede** está definido como **ative-Backup** para a rede de Grade.
- A **Admin Network** está ativada e o modo de ligação de rede está definido como **Independent**.
- A **rede do cliente** está desativada.



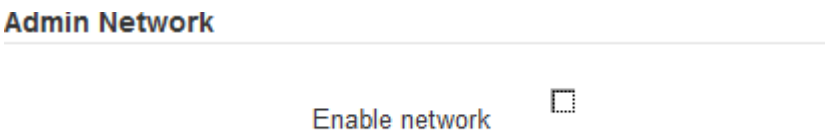
2. Se você planeja usar a velocidade de link de 25 GbE para as portas de rede, selecione **25GbE** na lista suspensa velocidade de link.

   Os switches de rede que você está usando para a rede de Grade e a rede do cliente também devem suportar e ser configurados para essa velocidade. Você deve usar cabos SFP28 Twinax ou cabos óticos e transcetores SFP28.

3. Ative ou desative as redes StorageGRID que pretende utilizar.

A rede de Grade é necessária. Não é possível desativar esta rede.

a. Se o dispositivo não estiver conetado à rede Admin, desmarque a caixa de seleção **Ativar rede** para a rede Admin.



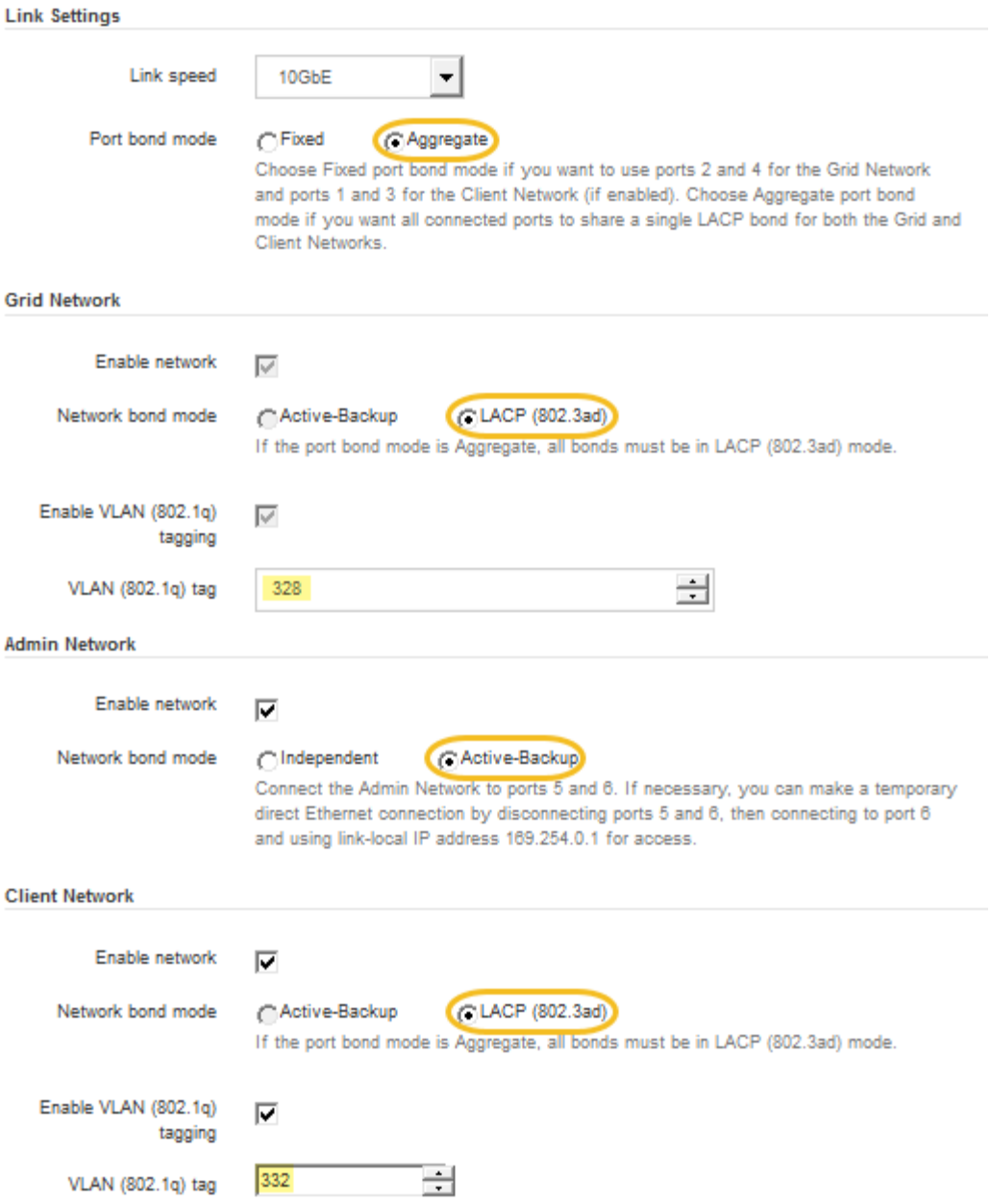
b. Se o dispositivo estiver conetado à rede do cliente, marque a caixa de seleção **Ativar rede** para a rede do cliente.

As definições de rede do cliente para as portas de rede são agora apresentadas.

4. Consulte a tabela e configure o modo de ligação de porta e o modo de ligação de rede.

Este exemplo mostra:

- **Aggregate** e **LACP** selecionados para as redes Grid e Client. Você deve especificar uma tag VLAN exclusiva para cada rede. Pode selecionar valores entre 0 e 4095.
- **Ative-Backup** selecionado para a rede Admin.



5. Quando estiver satisfeito com suas seleções, clique em **Salvar**.

> Poderá perder a ligação se tiver efetuado alterações à rede ou à ligação através da qual está ligado. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do Instalador de appliance StorageGRID usando um dos outros endereços IP atribuídos ao appliance
> **`https://SG6000-CN_Controller_IP:8443`**

Informações relacionadas

"Modos de ligação de porta para o controlador SG6000-CN"

"Configurando endereços IP do StorageGRID"

Você usa o Instalador de dispositivos StorageGRID para configurar os endereços IP e as informações de roteamento usados para o nó de armazenamento de dispositivos nas redes StorageGRID, Admin e cliente.

Sobre esta tarefa

Você deve atribuir um IP estático para o dispositivo em cada rede conetada ou atribuir uma concessão permanente para o endereço no servidor DHCP.

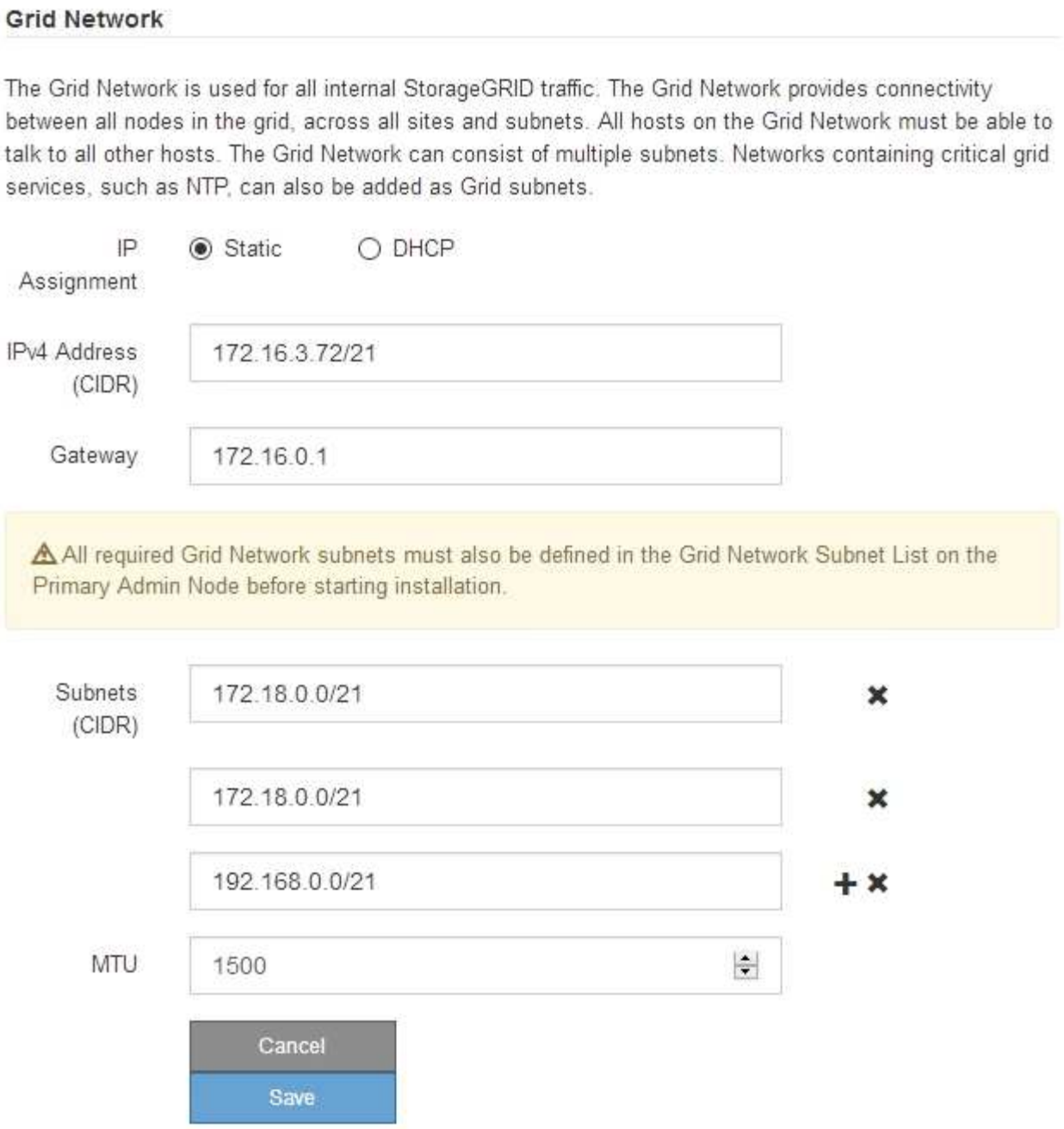
Se você quiser alterar a configuração do link, consulte as instruções para alterar a configuração do link do controlador SG6000-CN.

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração IP**.

   É apresentada a página Configuração IP.

2. Para configurar a rede de Grade, selecione **Static** ou **DHCP** na seção **Grid Network** da página.



3. Se você selecionou **Static**, siga estas etapas para configurar a rede de Grade:
   a. Insira o endereço IPv4 estático, usando a notação CIDR.
   b. Entre no gateway.

      Se a rede não tiver um gateway, insira novamente o mesmo endereço IPv4 estático.

   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

      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.

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.

d. Clique em **Salvar**.

Quando você altera o endereço IP, o gateway e a lista de sub-redes também podem mudar.

Se você perder a conexão com o Instalador do StorageGRID Appliance, insira novamente o URL usando o novo endereço IP estático que você acabou de atribuir. Por exemplo `https://services_appliance_IP:8443`

e. Confirme se a lista de sub-redes da rede de Grade está correta.

Se você tiver 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. Essas sub-redes de rede de grade também devem ser definidas na lista de sub-redes de rede de grade no nó de administração principal quando você iniciar a instalação do StorageGRID.

A rota padrão não está listada. Se a rede do cliente não estiver ativada, a rota padrão usará o gateway de rede de grade.

- Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
- Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

f. Clique em **Salvar**.

4. Se você selecionou **DHCP**, siga estas etapas para configurar a rede de Grade:

a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

Os campos **IPv4 Address**, **Gateway** e **sub-redes** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

b. Confirme se a lista de sub-redes da rede de Grade está correta.

Se você tiver 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. Essas sub-redes de rede de grade também devem ser definidas na lista de sub-redes de rede de grade no nó de administração principal quando você iniciar a instalação do StorageGRID.

A rota padrão não está listada. Se a rede do cliente não estiver ativada, a rota padrão usará o gateway de rede de grade.

- Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
- Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros

jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

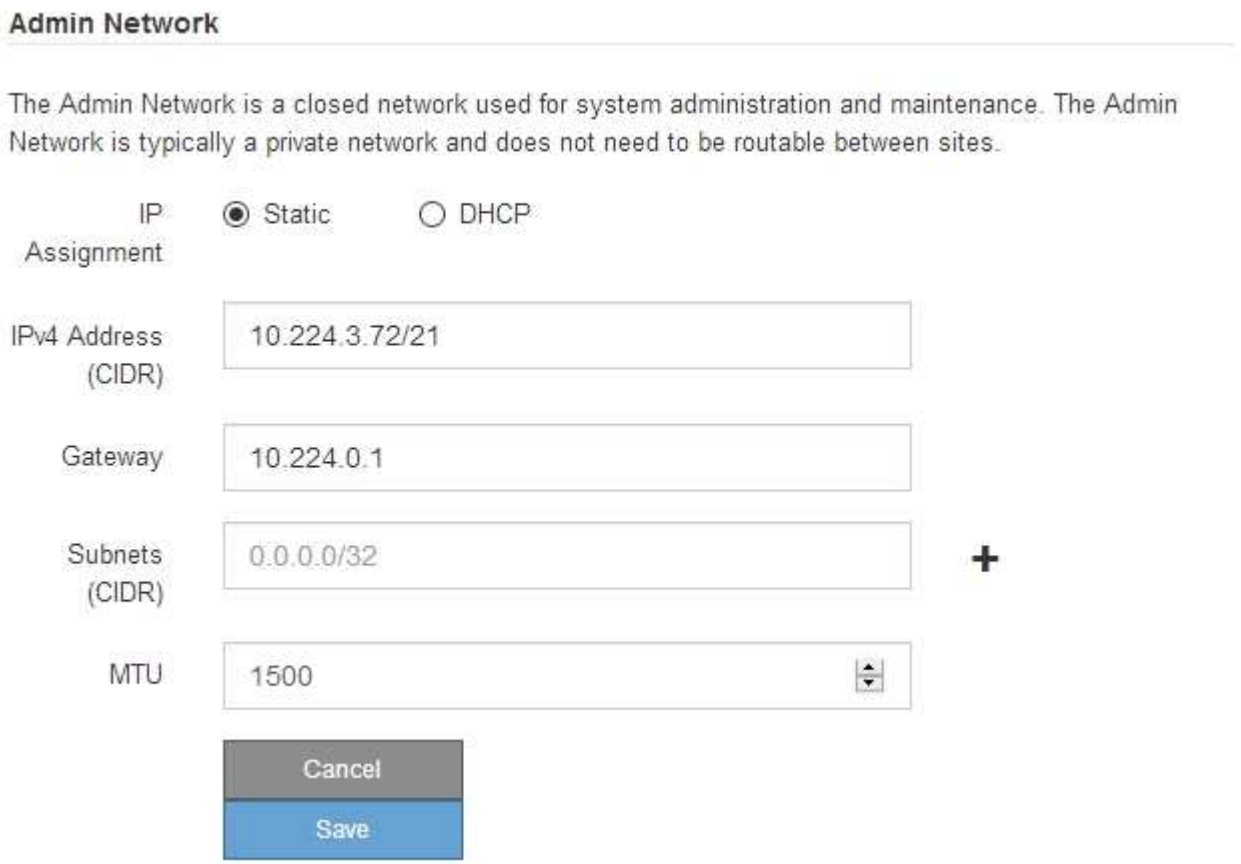
> O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

> 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.

a. Clique em **Salvar**.

5. Para configurar a rede Admin, selecione **Static** (estático) ou **DHCP** (DHCP) na secção **Admin Network** (rede Admin) da página.

> Para configurar a rede de administração, você deve ativar a rede de administração na página Configuração de ligação.



6. Se você selecionou **Static**, siga estas etapas para configurar a rede Admin:

a. Introduza o endereço IPv4 estático, utilizando a notação CIDR, para a porta de gestão 1 no dispositivo.

A porta de gerenciamento 1 fica à esquerda das duas portas RJ45 de 1 GbE na extremidade direita do dispositivo.

b. Entre no gateway.

   Se a rede não tiver um gateway, insira novamente o mesmo endereço IPv4 estático.

c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

   > 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.

d. Clique em **Salvar**.

   Quando você altera o endereço IP, o gateway e a lista de sub-redes também podem mudar.

   Se você perder a conexão com o Instalador do StorageGRID Appliance, insira novamente o URL usando o novo endereço IP estático que você acabou de atribuir. Por exemplo `https://services_appliance:8443`

e. Confirme se a lista de sub-redes Admin Network está correta.

   Você deve verificar se todas as sub-redes podem ser alcançadas usando o gateway fornecido.

   > A rota padrão não pode ser feita para usar o gateway de rede Admin.

   - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
   - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

f. Clique em **Salvar**.

7. Se você selecionou **DHCP**, siga estas etapas para configurar a rede Admin:

   a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

      Os campos **IPv4 Address**, **Gateway** e **sub-redes** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

      O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

   b. Confirme se a lista de sub-redes Admin Network está correta.

      Você deve verificar se todas as sub-redes podem ser alcançadas usando o gateway fornecido.

      > A rota padrão não pode ser feita para usar o gateway de rede Admin.

      - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
      - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

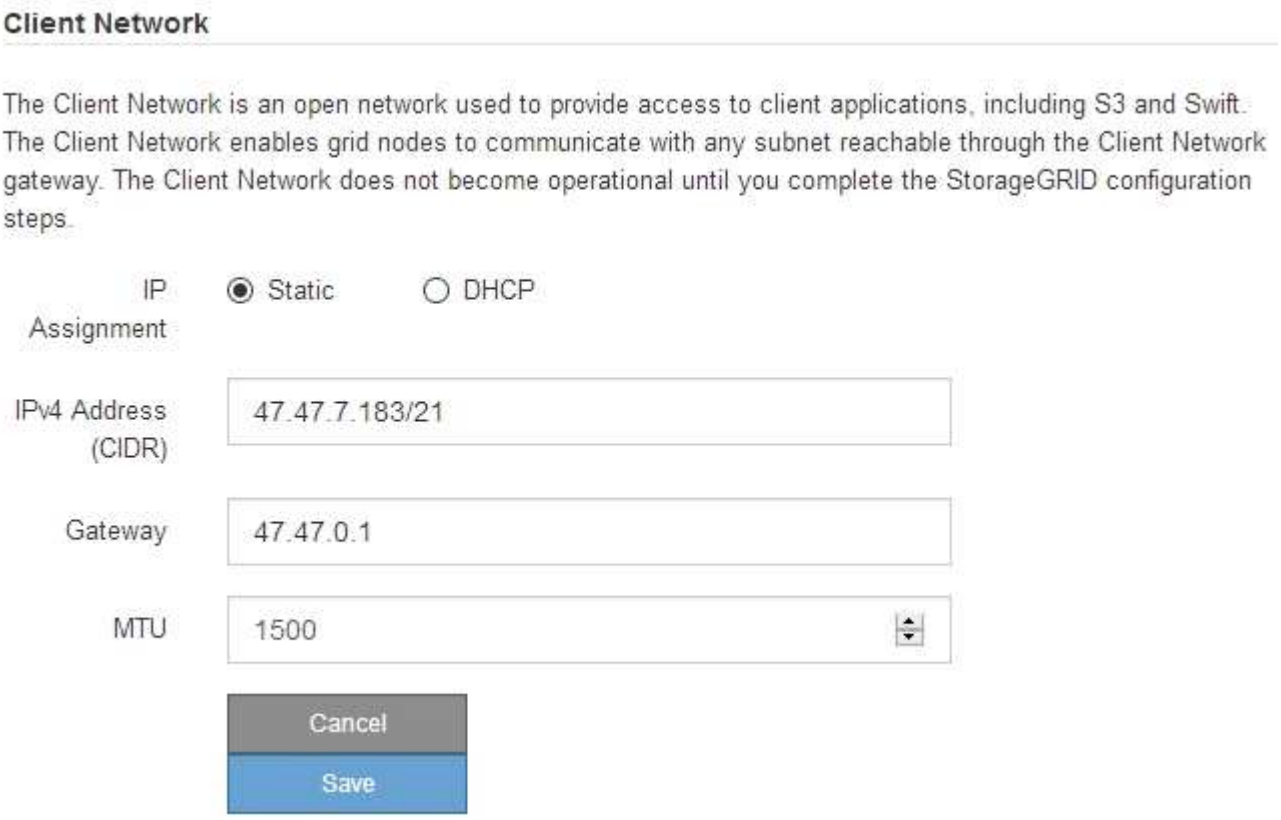
   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

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.

d. Clique em **Salvar**.

8. Para configurar a rede do cliente, selecione **estático** ou **DHCP** na seção **rede do cliente** da página.

Para configurar a rede do cliente, tem de ativar a rede do cliente na página Configuração da ligação.



9. Se você selecionou **Static**, siga estas etapas para configurar a rede do cliente:

a. Insira o endereço IPv4 estático, usando a notação CIDR.

b. Clique em **Salvar**.

c. Confirme se o endereço IP do gateway de rede do cliente está correto.

Se a rede do cliente estiver ativada, é apresentada a rota predefinida. A rota padrão usa o gateway de rede do cliente e não pode ser movida para outra interface enquanto a rede do cliente está ativada.

d. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

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.

e. Clique em **Salvar**.

10. Se você selecionou **DHCP**, siga estas etapas para configurar a rede do cliente:

    a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

       Os campos **IPv4 Address** e **Gateway** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

    O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

    a. Confirme se o gateway está correto.

       > ⓘ Se a rede do cliente estiver ativada, é apresentada a rota predefinida. A rota padrão usa o gateway de rede do cliente e não pode ser movida para outra interface enquanto a rede do cliente está ativada.

    b. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

       > ⓘ 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.

Informações relacionadas

"Alterar a configuração do link do controlador SG6000-CN"

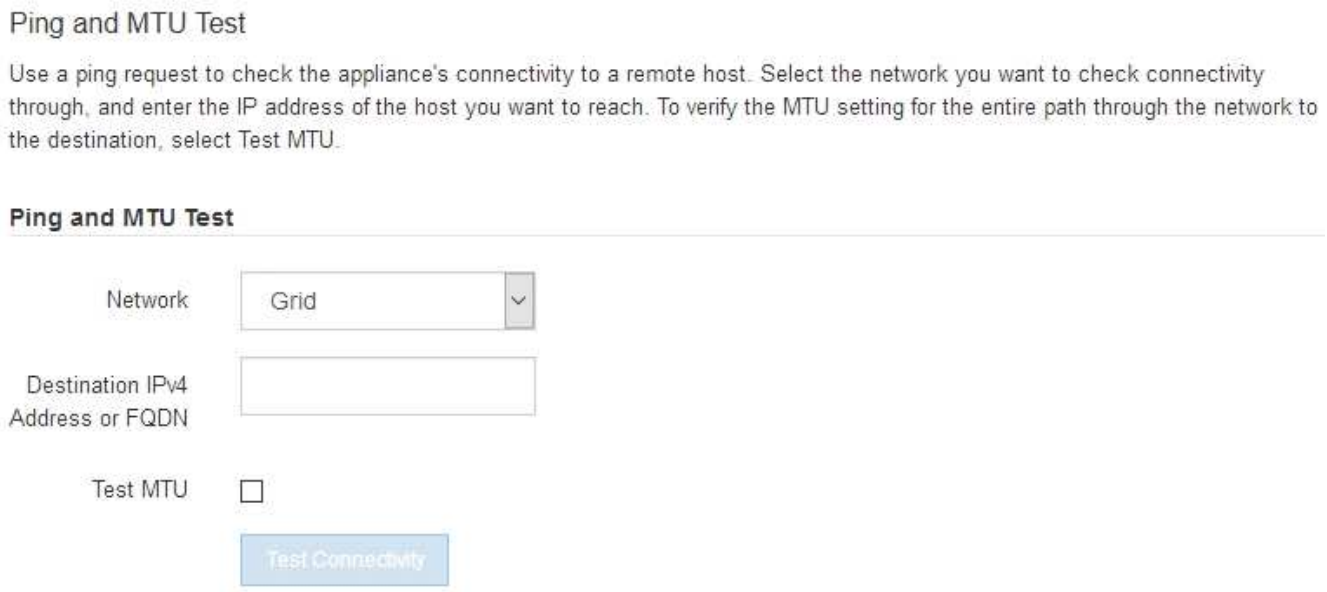
Verificando conexões de rede

Confirme que pode aceder às redes StorageGRID que está a utilizar a partir do dispositivo. Para validar o roteamento por meio de gateways de rede, você deve testar a conetividade entre o Instalador de dispositivos StorageGRID e endereços IP em diferentes sub-redes. Você também pode verificar a configuração MTU.

Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Teste de Ping e MTU**.

   A página Ping e MTU Test (Teste de Ping e MTU) é exibida.



2. Na caixa suspensa **rede**, selecione a rede que deseja testar: Grade, Admin ou Cliente.
3. Insira o endereço IPv4 ou o nome de domínio totalmente qualificado (FQDN) para um host nessa rede.

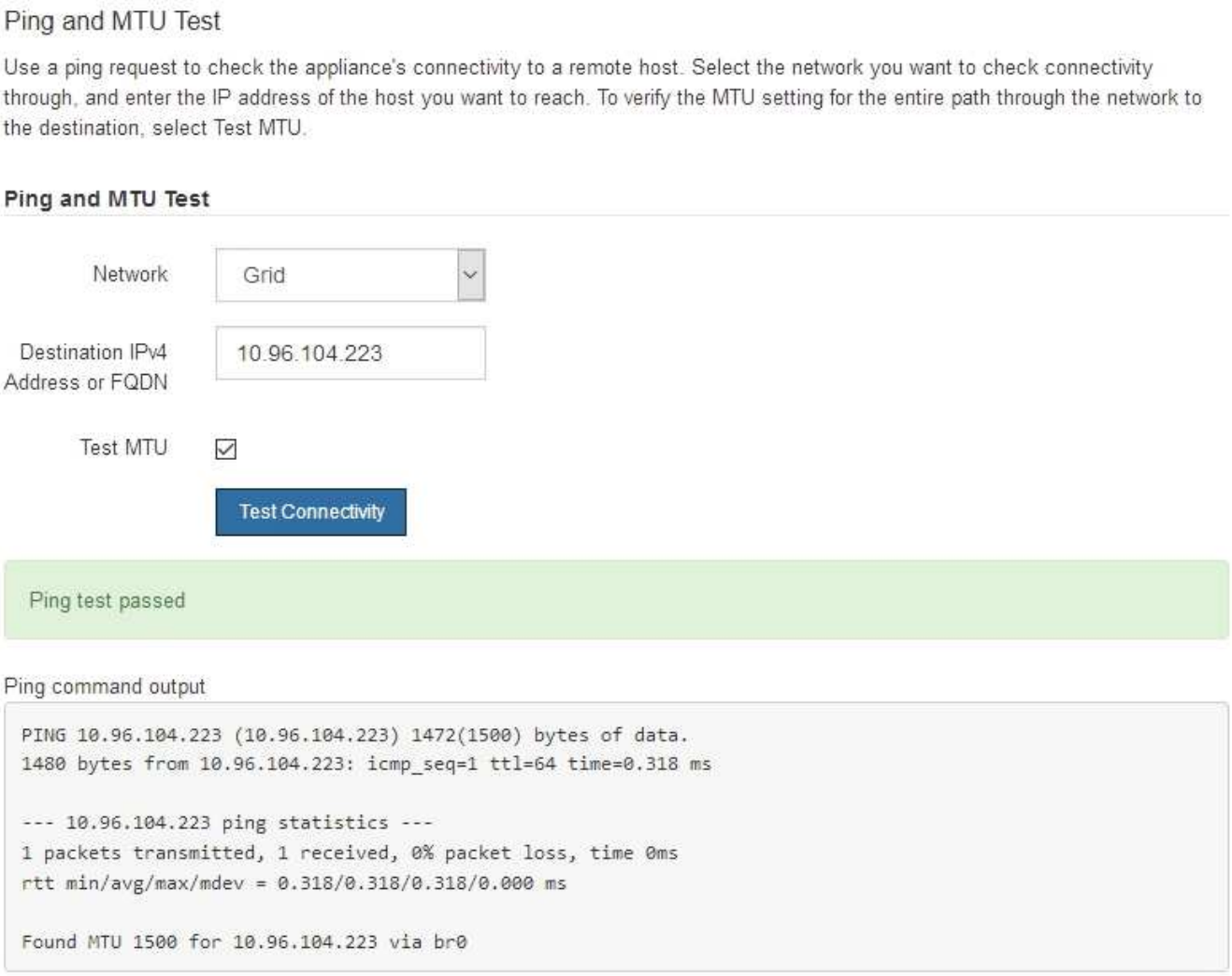
   Por exemplo, você pode querer fazer ping no gateway na rede ou no nó de administração principal.

4. Opcionalmente, marque a caixa de seleção **Test MTU** para verificar a configuração de MTU para todo o caminho através da rede até o destino.

   Por exemplo, você pode testar o caminho entre o nó do dispositivo e um nó em um local diferente.

5. Clique em **testar conetividade**.

   Se a conexão de rede for válida, a mensagem "Teste de ping aprovado" será exibida, com a saída do comando ping listada.



Informações relacionadas

"Configurando links de rede (SG6000)"

"Alterar a definição MTU"

Verificando conexões de rede no nível da porta

Para garantir que o acesso entre o Instalador de dispositivos StorageGRID e outros nós não esteja obstruído por firewalls, confirme se o Instalador de dispositivos StorageGRID pode se conetar a uma porta TCP específica ou conjunto de portas no endereço IP ou intervalo de endereços especificado.

Sobre esta tarefa

Usando a lista de portas fornecida no Instalador de dispositivos StorageGRID, você pode testar a conetividade entre o dispositivo e os outros nós da rede de Grade.

Além disso, você pode testar a conetividade nas redes Admin e Client e nas portas UDP, como as usadas para servidores NFS ou DNS externos. Para obter uma lista dessas portas, consulte a referência de porta nas diretrizes de rede do StorageGRID.

As portas de rede de grade listadas na tabela de conetividade de portas são válidas apenas para o StorageGRID versão 11,5.0. Para verificar quais portas estão corretas para cada tipo de nó, você deve sempre consultar as diretrizes de rede para sua versão do StorageGRID.

Passos

1. No Instalador de dispositivos StorageGRID, clique em **Configurar rede Teste de conetividade de porta (nmap)**.

   A página Teste de conetividade de porta é exibida.

   A tabela de conetividade de porta lista os tipos de nós que exigem conetividade TCP na rede de Grade. Para cada tipo de nó, a tabela lista as portas de rede de Grade que devem ser acessíveis ao seu dispositivo.

   The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

   Você pode testar a conetividade entre as portas do dispositivo listadas na tabela e os outros nós da rede de Grade.

2. Na lista suspensa **Network**, selecione a rede que deseja testar: **Grid**, **Admin** ou **Client**.
3. Especifique um intervalo de endereços IPv4 para os hosts nessa rede.

   Por exemplo, você pode querer pesquisar o gateway na rede ou no nó de administração principal.

   Especifique um intervalo usando um hífen, como mostrado no exemplo.

4. Insira um número de porta TCP, uma lista de portas separadas por vírgulas ou um intervalo de portas.

The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

Port Connectivity Test

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: TCP UDP

Test Connectivity

5. Clique em **testar conetividade**.

   - Se as conexões de rede no nível da porta selecionadas forem válidas, a mensagem ""Teste de conetividade de porta aprovado"" aparecerá em um banner verde. A saída do comando nmap está listada abaixo do banner.

     Port connectivity test passed

     Nmap command output. Note: Unreachable hosts will not appear in the output.

     ```
     # Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
     Nmap scan report for 10.224.6.160
     Host is up (0.00072s latency).

     PORT     STATE SERVICE
     22/tcp   open  ssh
     2022/tcp open  down

     Nmap scan report for 10.224.6.161
     Host is up (0.00060s latency).

     PORT     STATE SERVICE
     22/tcp   open  ssh
     2022/tcp open  down

     # Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
     ```

   - Se uma conexão de rede no nível da porta for feita ao host remoto, mas o host não estiver ouvindo em uma ou mais das portas selecionadas, a mensagem ""Falha no teste de conetividade da porta"" aparecerá em um banner amarelo. A saída do comando nmap está listada abaixo do banner.

     Qualquer porta remota que o host não esteja ouvindo tem um estado de "fechado". Por exemplo, você pode ver esse banner amarelo quando o nó ao qual você está tentando se conetar estiver em um estado pré-instalado e o serviço StorageGRID NMS ainda não estiver sendo executado nesse nó.

- Se uma conexão de rede no nível de porta não puder ser feita para uma ou mais portas selecionadas, a mensagem "Falha no teste de conetividade de porta" aparecerá em um banner vermelho. A saída do comando nmap está listada abaixo do banner.

  O banner vermelho indica que uma tentativa de conexão TCP para uma porta no host remoto foi feita, mas nada foi retornado ao remetente. Quando nenhuma resposta é retornada, a porta tem um estado de "filtrada" e é provavelmente bloqueada por um firewall.

  Os portos com "fechado" também são listados.

Informações relacionadas

"Diretrizes de rede"

Acessando e configurando o Gerenciador do sistema do SANtricity

Você pode usar o Gerenciador de sistemas do SANtricity para monitorar o status das

controladoras de storage, discos de storage e outros componentes de hardware no compartimento de controladora de storage. Você também pode configurar um proxy para o e-Series AutoSupport que permite enviar mensagens AutoSupport do dispositivo sem o uso da porta de gerenciamento.

Passos

- "Configuração e acesso ao Gerenciador de sistema do SANtricity"
- "Analisando o status do hardware no Gerenciador do sistema do SANtricity"
- "Definir os endereços IP dos controladores de armazenamento utilizando o Instalador de dispositivos StorageGRID"

Configuração e acesso ao Gerenciador de sistema do SANtricity

Talvez seja necessário acessar o Gerenciador de sistema do SANtricity no controlador de storage para monitorar o hardware no compartimento de controladora de storage ou para configurar o e-Series AutoSupport.

O que você vai precisar

- Você está usando um navegador da Web compatível.
- Para acessar o Gerenciador de sistema do SANtricity por meio do Gerenciador de Grade, você deve ter instalado o StorageGRID e ter a permissão Administrador do dispositivo de armazenamento ou a permissão de acesso à raiz.
- Para acessar o Gerenciador de sistema do SANtricity usando o Instalador de dispositivos do StorageGRID, você deve ter o nome de usuário e a senha do administrador do Gerenciador de sistema do SANtricity.
- Para acessar diretamente o Gerenciador de sistema do SANtricity usando um navegador da Web, você deve ter o nome de usuário e a senha do administrador do Gerenciador de sistema do SANtricity.

> Você deve ter o firmware 8,70 ou superior do SANtricity para acessar o Gerenciador de sistema do SANtricity usando o Gerenciador de Grade ou o Instalador de dispositivos StorageGRID. Você pode verificar a versão do firmware usando o Instalador do StorageGRID Appliance e selecionando **Ajuda sobre**.

> O acesso ao Gerenciador de sistema do SANtricity a partir do Gerenciador de Grade ou do Instalador de dispositivos é geralmente destinado apenas para monitorar seu hardware e configurar o e-Series AutoSupport. Muitos recursos e operações no Gerenciador de sistemas do SANtricity, como atualização de firmware, não se aplicam ao monitoramento do dispositivo StorageGRID. Para evitar problemas, siga sempre as instruções de instalação e manutenção do hardware do seu aparelho.

Sobre esta tarefa

Há três maneiras de acessar o Gerenciador de sistema do SANtricity, dependendo de qual estágio do processo de instalação e configuração você está:

- Se o dispositivo ainda não tiver sido implantado como um nó no sistema StorageGRID, você deve usar a guia Avançado no Instalador de dispositivos StorageGRID.

> Depois que o nó for implantado, você não poderá mais usar o Instalador de dispositivos StorageGRID para acessar o Gerenciador de sistemas do SANtricity.

- Se o dispositivo tiver sido implantado como um nó em seu sistema StorageGRID, use a guia Gerenciador de sistema do SANtricity na página nós no Gerenciador de Grade.
- Se você não puder usar o Instalador de dispositivos StorageGRID ou o Gerenciador de Grade, poderá acessar o Gerenciador de sistema do SANtricity diretamente usando um navegador da Web conetado à porta de gerenciamento.

Este procedimento inclui etapas para o seu acesso inicial ao Gerenciador de sistema do SANtricity. Se você já tiver configurado o Gerenciador de sistema do SANtricity, vá para a configurar alertas de hardware etapa.

> O uso do Gerenciador de Grade ou do Instalador de dispositivos StorageGRID permite que você acesse o Gerenciador de sistema do SANtricity sem ter que configurar ou conetar a porta de gerenciamento do dispositivo.

Você usa o Gerenciador de sistema do SANtricity para monitorar o seguinte:

- Dados de performance, como performance em nível de storage array, latência de e/S, utilização de CPU e taxa de transferência
- Status do componente de hardware
- Funções de suporte, incluindo visualização de dados de diagnóstico

Você pode usar o Gerenciador de sistema do SANtricity para configurar as seguintes configurações:

- Alertas de e-mail, alertas SNMP ou alertas syslog para os componentes no compartimento do controlador de armazenamento
- Configurações do e-Series AutoSupport para os componentes no compartimento do controlador de storage.

  Para obter detalhes adicionais sobre o e-Series AutoSupport, consulte o centro de documentação do e-Series.

  "Site de Documentação de sistemas NetApp e-Series"

- Chaves de segurança da unidade, que são necessárias para desbloquear unidades seguras (esta etapa é necessária se o recurso Segurança da unidade estiver ativado)
- Senha de administrador para acessar o Gerenciador de sistema do SANtricity

Passos

1. Execute um dos seguintes procedimentos:
   - Use o Instalador do StorageGRID Appliance e selecione **Avançado Gerenciador do sistema SANtricity**
   - Use o Gerenciador de Grade e selecione **nós** * `***appliance Storage Node***`Gerenciador de sistema SANtricity*

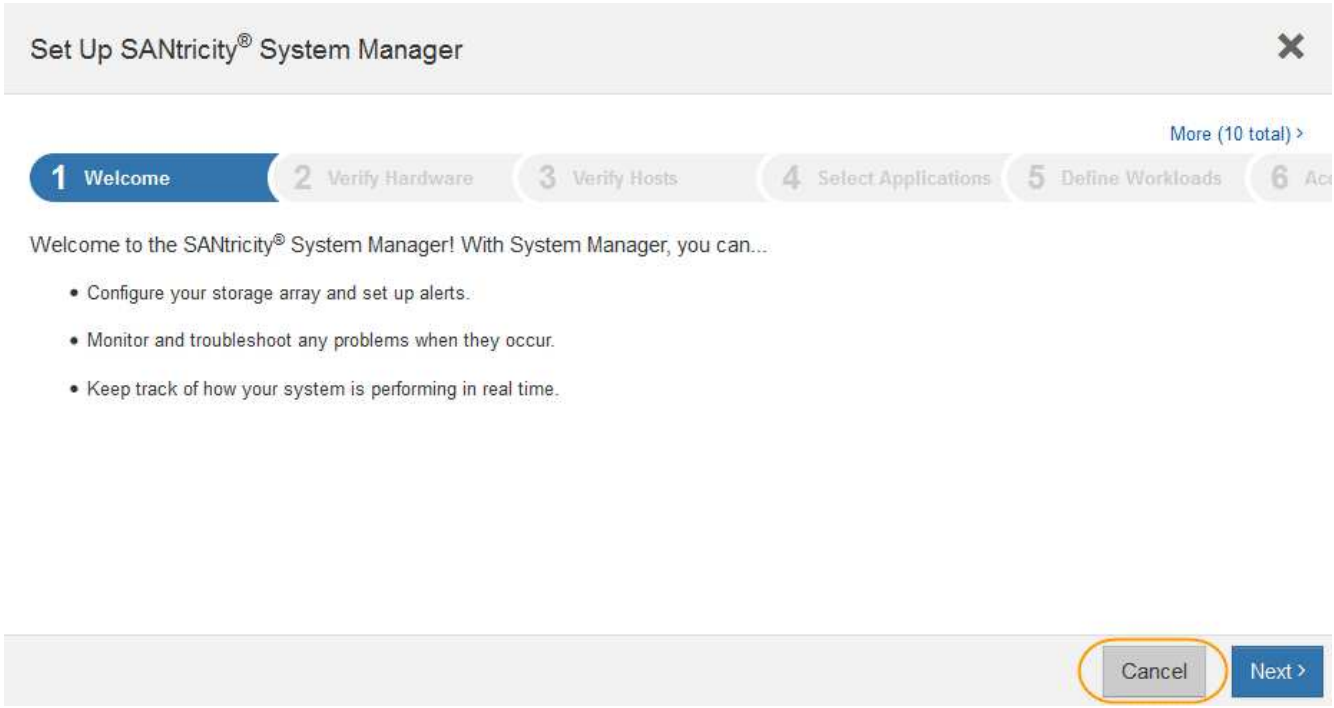
     > Se essas opções não estiverem disponíveis ou a página de login não aparecer, você deverá usar o endereço IP do controlador de armazenamento. Acesse o Gerenciador de sistema do SANtricity navegando para o IP do controlador de armazenamento `https://Storage_Controller_IP`

   É apresentada a página de início de sessão do Gestor do sistema SANtricity.

2. Defina ou introduza a palavra-passe do administrador.

> O Gerenciador de sistema do SANtricity usa uma única senha de administrador que é compartilhada entre todos os usuários.

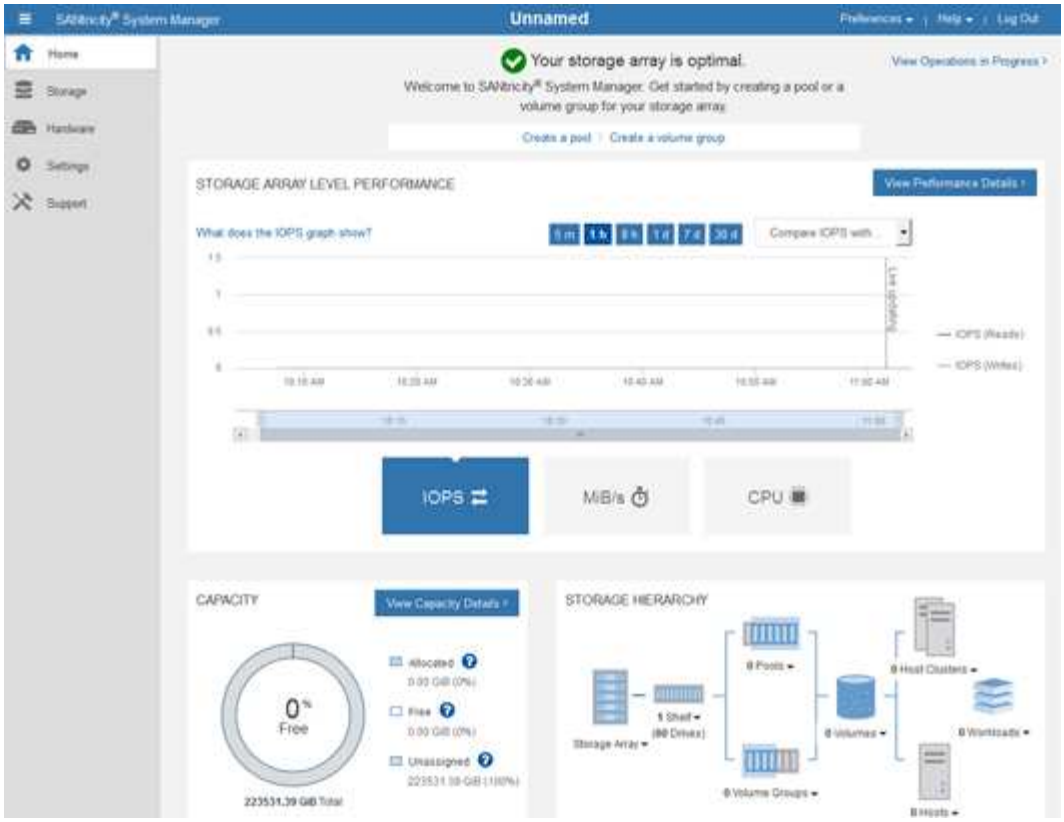
O assistente de configuração é exibido.



3. Selecione **Cancelar** para fechar o assistente.

> Não conclua o assistente de configuração de um dispositivo StorageGRID.

É apresentada a página inicial do Gestor do sistema SANtricity.



1. Configurar alertas de hardware.
   a. Selecione **Ajuda** para acessar a ajuda on-line do Gerenciador de sistemas do SANtricity.
   b. Use a seção **Configurações Alertas** da ajuda on-line para saber mais sobre alertas.
   c. Siga as instruções ""como fazer"" para configurar alertas de e-mail, alertas SNMP ou alertas syslog.
2. Gerenciar o AutoSupport para os componentes no compartimento do controlador de storage.
   a. Selecione **Ajuda** para acessar a ajuda on-line do Gerenciador de sistemas do SANtricity.
   b. Use a seção **suporte Centro de suporte** da ajuda on-line para saber mais sobre o recurso AutoSupport.
   c. Siga as instruções ""como fazer"" para gerenciar o AutoSupport.

      Para obter instruções específicas sobre como configurar um proxy StorageGRID para enviar mensagens AutoSupport da série e sem usar a porta de gerenciamento, vá para as instruções de administração do StorageGRID e procure "configurações de proxy para o e-Series AutoSupport".

   "Administrar o StorageGRID"
3. Se o recurso Segurança da unidade estiver ativado para o dispositivo, crie e gerencie a chave de segurança.
   a. Selecione **Ajuda** para acessar a ajuda on-line do Gerenciador de sistemas do SANtricity.
   b. Use a seção **Configurações sistema Gerenciamento de chaves de segurança** da ajuda on-line para saber mais sobre a segurança da unidade.
   c. Siga as instruções de "como fazer" para criar e gerenciar a chave de segurança.
4. Opcionalmente, altere a senha do administrador.

a. Selecione **Ajuda** para acessar a ajuda on-line do Gerenciador de sistemas do SANtricity.

b. Use a seção **Home Storage array Administration** da ajuda on-line para saber mais sobre a senha do administrador.

c. Siga as instruções "'como fazer'" para alterar a senha.

Informações relacionadas

"Requisitos do navegador da Web"

"Definir os endereços IP dos controladores de armazenamento utilizando o Instalador de dispositivos StorageGRID"

Analisando o status do hardware no Gerenciador do sistema do SANtricity

Você pode usar o Gerenciador de sistema do SANtricity para monitorar e gerenciar componentes de hardware individuais no compartimento de controladora de storage e analisar informações ambientais e de diagnóstico de hardware, como temperaturas dos componentes, bem como problemas relacionados às unidades.

O que você vai precisar

- Você está usando um navegador da Web compatível.
- Para acessar o Gerenciador de sistema do SANtricity por meio do Gerenciador de Grade, você deve ter a permissão Administrador do dispositivo de armazenamento ou a permissão de acesso à raiz.
- Para acessar o Gerenciador de sistema do SANtricity usando o Instalador de dispositivos do StorageGRID, você deve ter o nome de usuário e a senha do administrador do Gerenciador de sistema do SANtricity.
- Para acessar diretamente o Gerenciador de sistema do SANtricity usando um navegador da Web, você deve ter o nome de usuário e a senha do administrador do Gerenciador de sistema do SANtricity.

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

> O acesso ao Gerenciador de sistema do SANtricity a partir do Gerenciador de Grade ou do Instalador de dispositivos é geralmente destinado apenas para monitorar seu hardware e configurar o e-Series AutoSupport. Muitos recursos e operações no Gerenciador de sistemas do SANtricity, como atualização de firmware, não se aplicam ao monitoramento do dispositivo StorageGRID. Para evitar problemas, siga sempre as instruções de instalação e manutenção do hardware do seu aparelho.

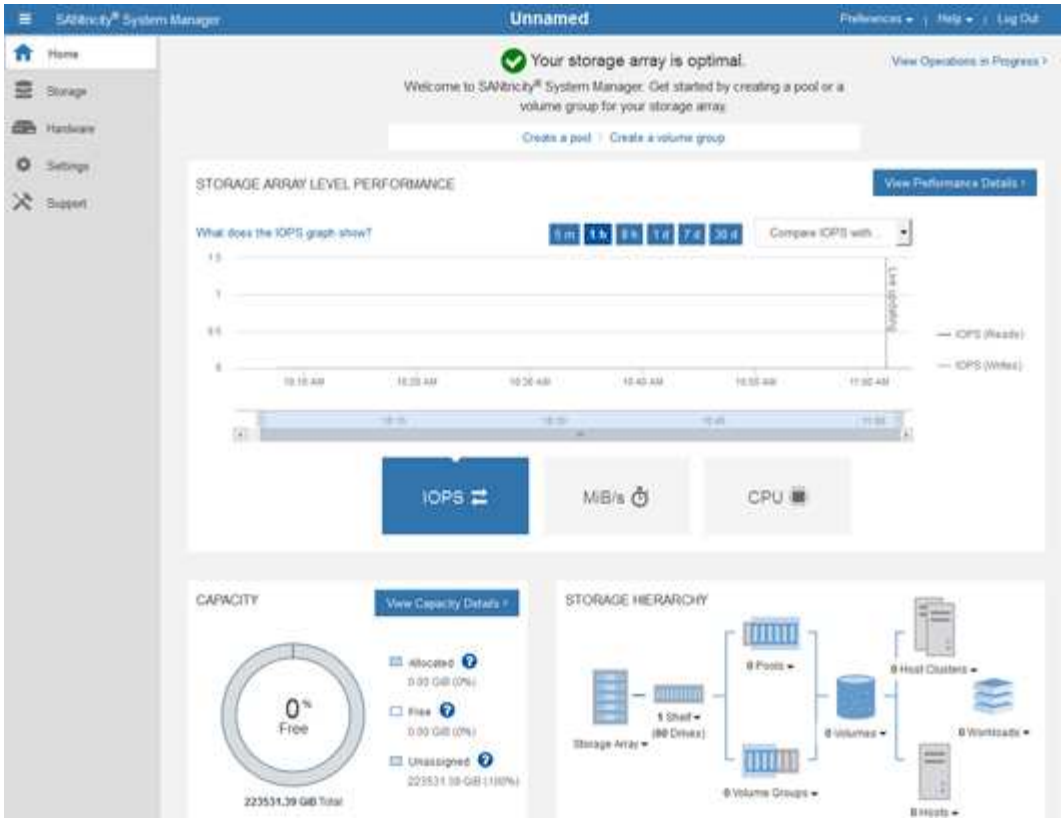
Passos

1. Acesse o Gerenciador do sistema do SANtricity.

   "Configuração e acesso ao Gerenciador de sistema do SANtricity"

2. Introduza o nome de utilizador e a palavra-passe do administrador, se necessário.
3. Clique em **Cancelar** para fechar o assistente de configuração e exibir a página inicial do Gerenciador do sistema SANtricity.

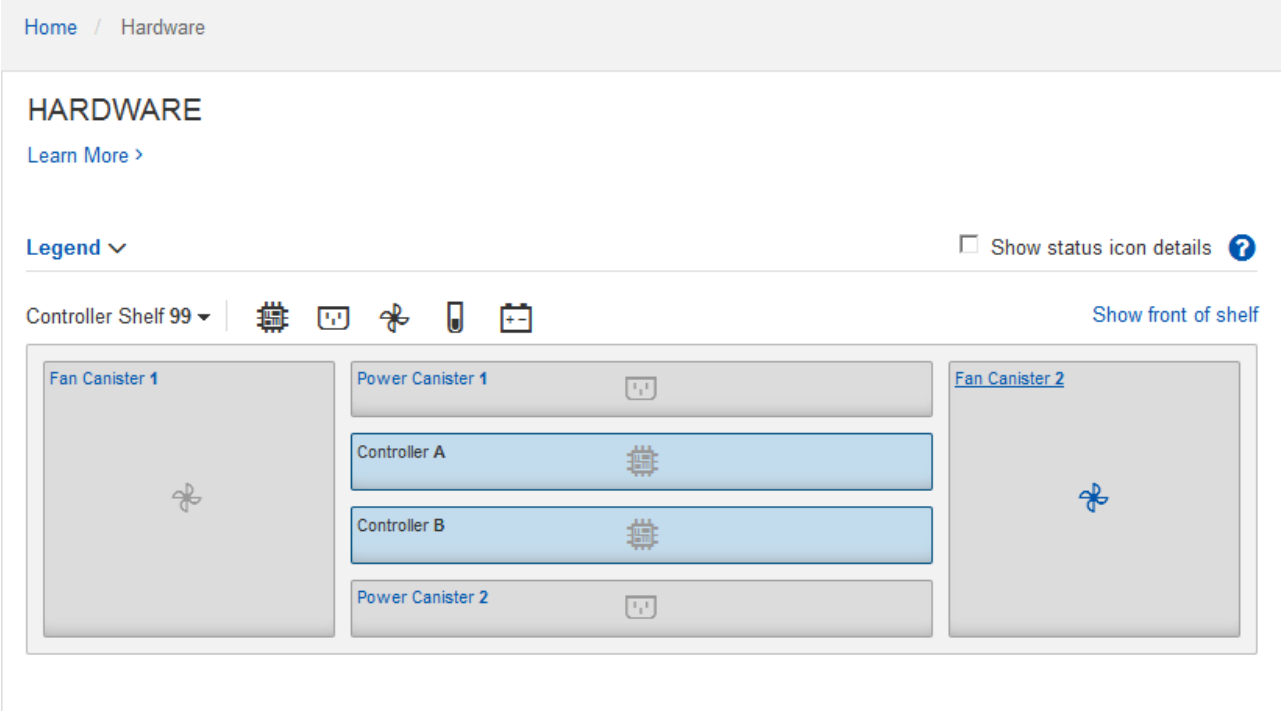
   É apresentada a página inicial do Gestor do sistema SANtricity. No Gerenciador de sistemas do SANtricity, o compartimento de controladora é chamado de storage array.



4. Revise as informações exibidas para o hardware do dispositivo e confirme se todos os componentes de hardware têm o status ideal.

   a. Clique na guia **hardware**.

   b. Clique em **Mostrar parte posterior da prateleira**.



Na parte de trás da gaveta, você pode visualizar os dois controladores de armazenamento, a bateria em cada controlador de armazenamento, os dois coletores de energia, os dois coletores de ventilador e os

compartimentos de expansão (se houver). Também pode visualizar as temperaturas dos componentes.

a. Para ver as configurações de cada controlador de armazenamento, selecione o controlador e selecione **View settings** no menu de contexto.
b. Para ver as configurações de outros componentes na parte de trás da prateleira, selecione o componente que deseja exibir.
c. Clique em **Mostrar frente da prateleira** e selecione o componente que deseja exibir.

   Na parte da frente da gaveta, é possível visualizar as unidades e as gavetas de unidades da gaveta de controladora de armazenamento ou das gavetas de expansão (se houver).

Se o status de qualquer componente for necessário atenção, siga as etapas no Recovery Guru para resolver o problema ou entre em Contato com o suporte técnico.

Definir os endereços IP dos controladores de armazenamento utilizando o Instalador de dispositivos StorageGRID

A porta de gerenciamento 1 em cada controlador de storage coneta o dispositivo à rede de gerenciamento do Gerenciador de sistema do SANtricity. Se você não puder acessar o Gerenciador de sistema do SANtricity pelo Instalador de dispositivos StorageGRID, defina um endereço IP estático para cada controlador de armazenamento para garantir que não perca a conexão de gerenciamento com o hardware e o firmware da controladora no compartimento da controladora.

O que você vai precisar

- Você está usando qualquer cliente de gerenciamento que possa se conetar à rede de administração do StorageGRID ou tem um laptop de serviço.
- O cliente ou laptop de serviço tem um navegador da Web suportado.

Sobre esta tarefa

Os endereços atribuídos pelo DHCP podem ser alterados a qualquer momento. Atribua endereços IP estáticos aos controladores para garantir uma acessibilidade consistente.

> Siga este procedimento somente se você não tiver acesso ao Gerenciador de sistemas SANtricity a partir do Instalador de dispositivos StorageGRID (**Avançado Gerenciador de sistemas SANtricity**) ou Gerenciador de Grade (**nós Gerenciador de sistemas SANtricity**).

Passos

1. No cliente, insira o URL para o instalador do StorageGRID Appliance
   `https://Appliance_Controller_IP:8443`

   Para *`Appliance_Controller_IP`*, use o endereço IP do dispositivo em qualquer rede StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configure hardware Storage Controller Network Configuration**.

   A página Configuração da rede do controlador de armazenamento é exibida.

3. Dependendo da configuração da rede, selecione **Enabled** para IPv4, IPv6 ou ambos.
4. Anote o endereço IPv4 que é exibido automaticamente.

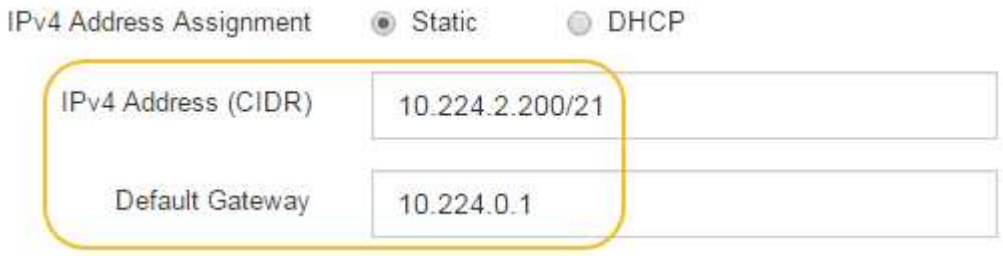
DHCP é o método padrão para atribuir um endereço IP à porta de gerenciamento do controlador de armazenamento.

Pode demorar alguns minutos para que os valores DHCP apareçam.

5. Opcionalmente, defina um endereço IP estático para a porta de gerenciamento do controlador de armazenamento.

Você deve atribuir um IP estático para a porta de gerenciamento ou atribuir uma concessão permanente para o endereço no servidor DHCP.

a. Selecione **estático**.
b. Introduza o endereço IPv4, utilizando a notação CIDR.
c. Introduza o gateway predefinido.



d. Clique em **Salvar**.

Pode levar alguns minutos para que suas alterações sejam aplicadas.

Quando você se conetar ao Gerenciador de sistema do SANtricity, você usará o novo endereço IP estático como URL
`https://Storage_Controller_IP`

Configurando a interface BMC

A interface do usuário do controlador de gerenciamento de placa base (BMC) no controlador SG6000-CN fornece informações de status sobre o hardware e permite configurar configurações SNMP e outras opções para o controlador SG6000-CN.

Passos

- "Alterar a senha raiz da interface BMC"
- "Definir o endereço IP da porta de gerenciamento do BMC"

- "Acessando a interface BMC"
- "Configurar definições SNMP para o controlador SG6000-CN"
- "Configurar notificações por e-mail para alertas"

Alterar a senha raiz da interface BMC

Para segurança, você deve alterar a senha do usuário raiz do BMC.

O que você vai precisar

- O cliente de gerenciamento está usando um navegador da Web compatível.

Sobre esta tarefa

Quando você instala o dispositivo pela primeira vez, o BMC usa uma senha padrão para o usuário raiz (`root/calvin`). Você deve alterar a senha do usuário raiz para proteger seu sistema.

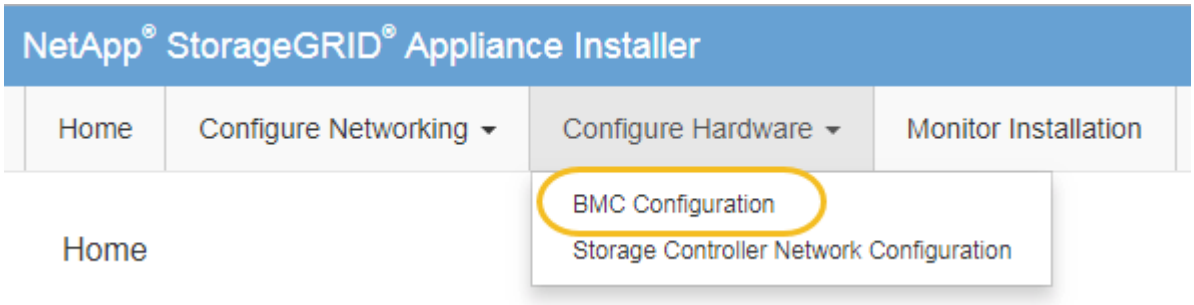
Passos

1. No cliente, insira o URL para o instalador do StorageGRID Appliance
   `https://Appliance_Controller_IP:8443`

   Para *`Appliance_Controller_IP`*, use o endereço IP do dispositivo em qualquer rede StorageGRID.

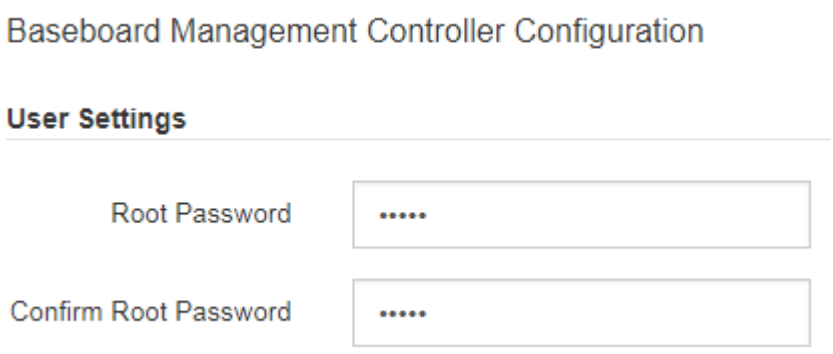
   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configurar hardware Configuração do BMC**.



   É apresentada a página Baseboard Management Controller Configuration (Configuração do controlador de gestão de base).

3. Insira uma nova senha para a conta root nos dois campos fornecidos.



4. Clique em **Salvar**.

Definir o endereço IP da porta de gerenciamento do BMC

Antes de poder aceder à interface BMC, tem de configurar o endereço IP para a porta de gestão BMC no controlador SG6000-CN.

O que você vai precisar

- O cliente de gerenciamento está usando um navegador da Web compatível.
- Você está usando qualquer cliente de gerenciamento que possa se conetar a uma rede StorageGRID.
- A porta de gerenciamento do BMC está conetada à rede de gerenciamento que você planeja usar.

Sobre esta tarefa

Para fins de suporte, a porta de gerenciamento do BMC permite acesso a hardware de baixo nível.

> Só deve ligar esta porta a uma rede de gestão interna segura, fidedigna. Se nenhuma rede estiver disponível, deixe a porta BMC desconetada ou bloqueada, a menos que uma conexão BMC seja solicitada pelo suporte técnico.

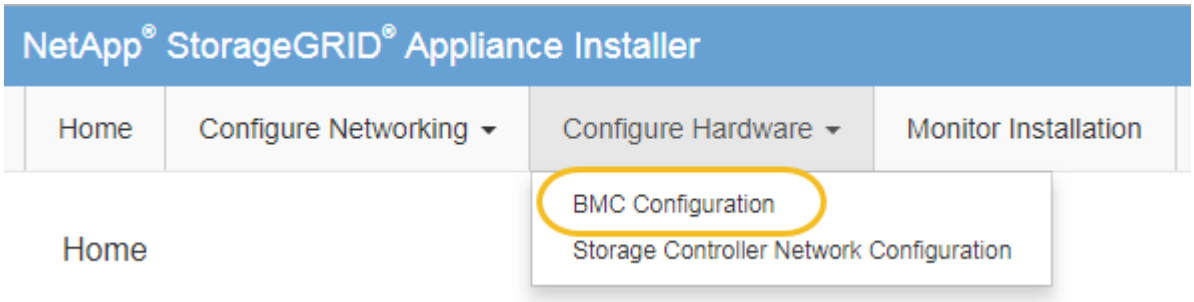
Passos

1. No cliente, insira o URL para o instalador do StorageGRID Appliance
   `https://SG6000-CN_Controller_IP:8443`

   Para `SG6000-CN_Controller_IP`, use o endereço IP do dispositivo em qualquer rede StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configurar hardware Configuração do BMC**.

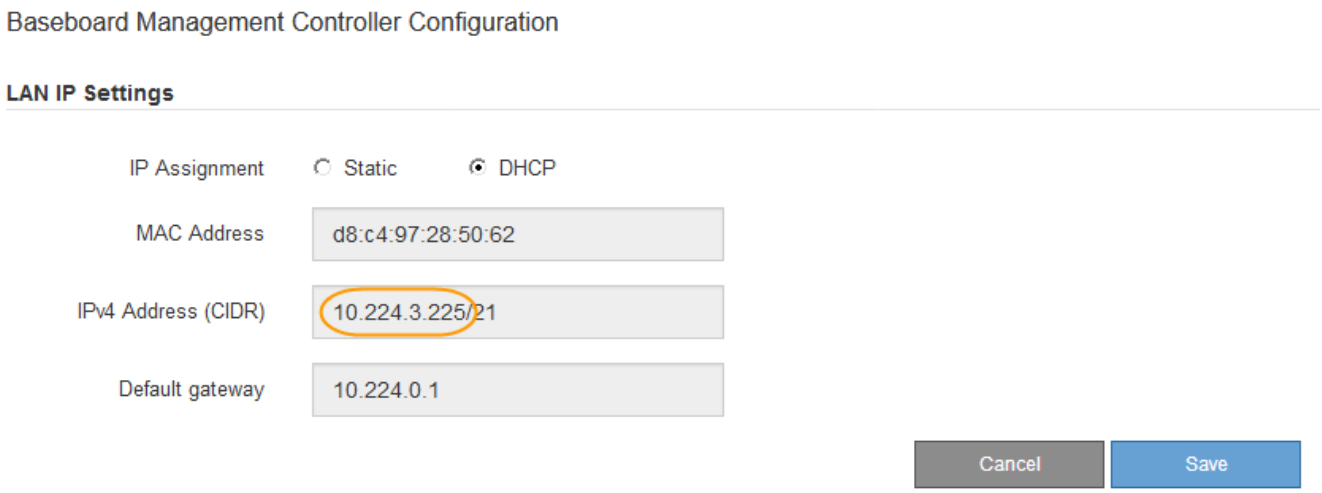


   É apresentada a página Baseboard Management Controller Configuration (Configuração do controlador de gestão de base).

3. Anote o endereço IPv4 que é exibido automaticamente.

   DHCP é o método padrão para atribuir um endereço IP a esta porta.

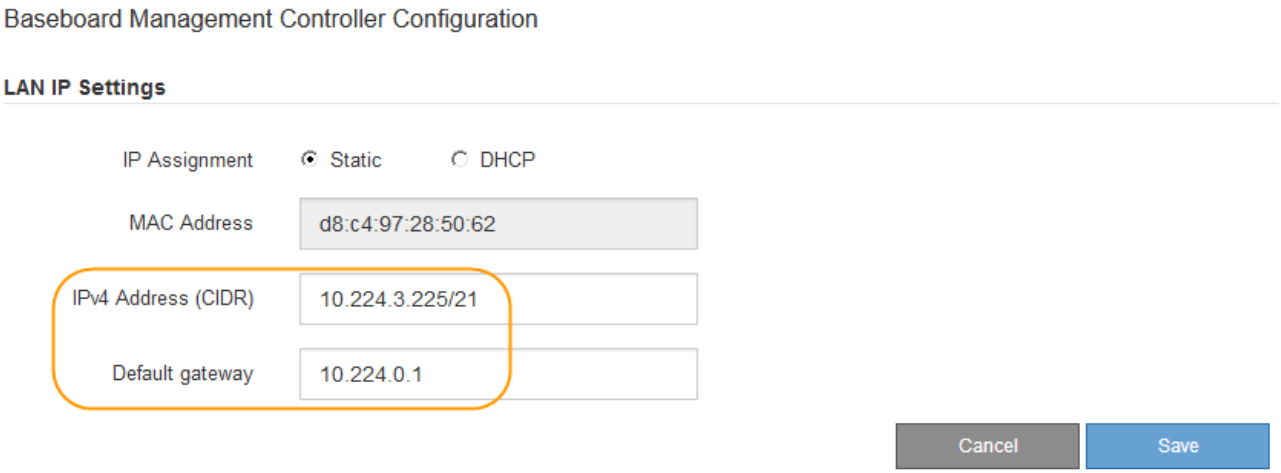
   > Pode demorar alguns minutos para que os valores DHCP apareçam.



4. Opcionalmente, defina um endereço IP estático para a porta de gerenciamento BMC.

> Você deve atribuir um IP estático para a porta de gerenciamento do BMC ou atribuir uma concessão permanente para o endereço no servidor DHCP.

a. Selecione **estático**.
b. Introduza o endereço IPv4, utilizando a notação CIDR.
c. Introduza o gateway predefinido.



d. Clique em **Salvar**.

Pode levar alguns minutos para que suas alterações sejam aplicadas.

Acessando a interface BMC

Você pode acessar a interface BMC no controlador SG6000-CN usando o DHCP ou o endereço IP estático para a porta de gerenciamento BMC.

O que você vai precisar

- A porta de gerenciamento BMC no controlador SG6000-CN está conetada à rede de gerenciamento que você planeja usar.

- O cliente de gerenciamento está usando um navegador da Web compatível.

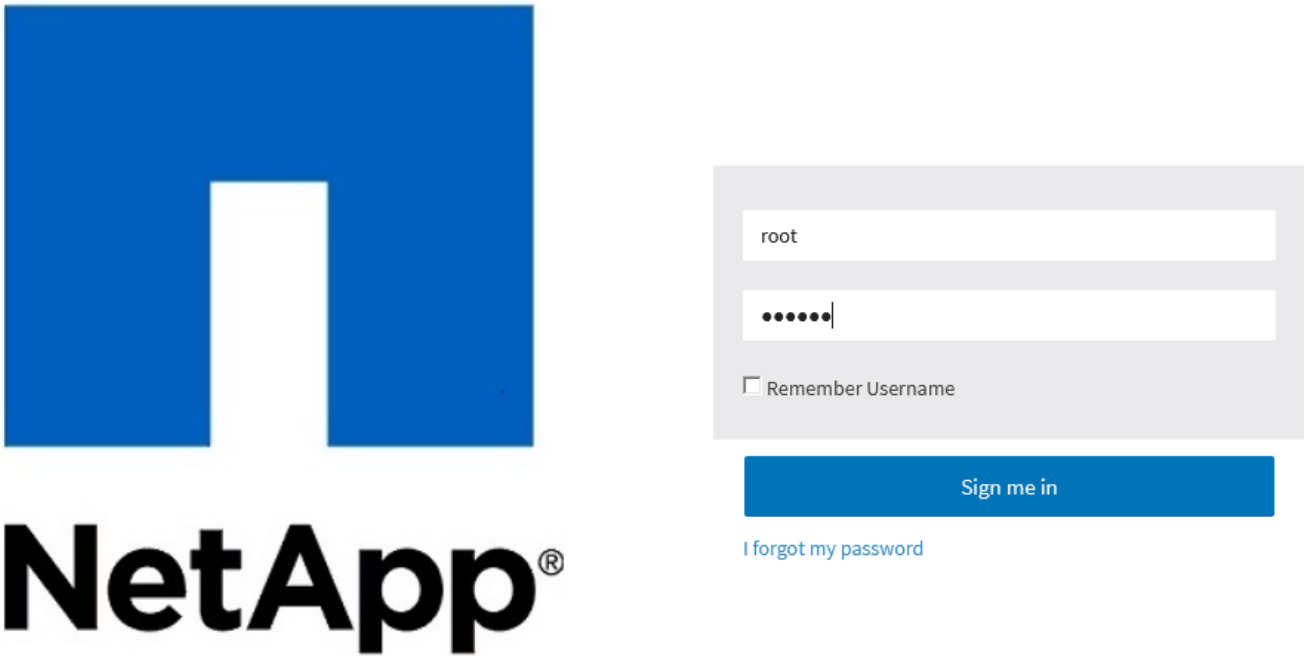
Passos

1. Digite o URL para a interface do BMC
   `https://BMC_Port_IP`

   Para *`BMC_Port_IP`*, utilize o DHCP ou o endereço IP estático para a porta de gestão BMC.

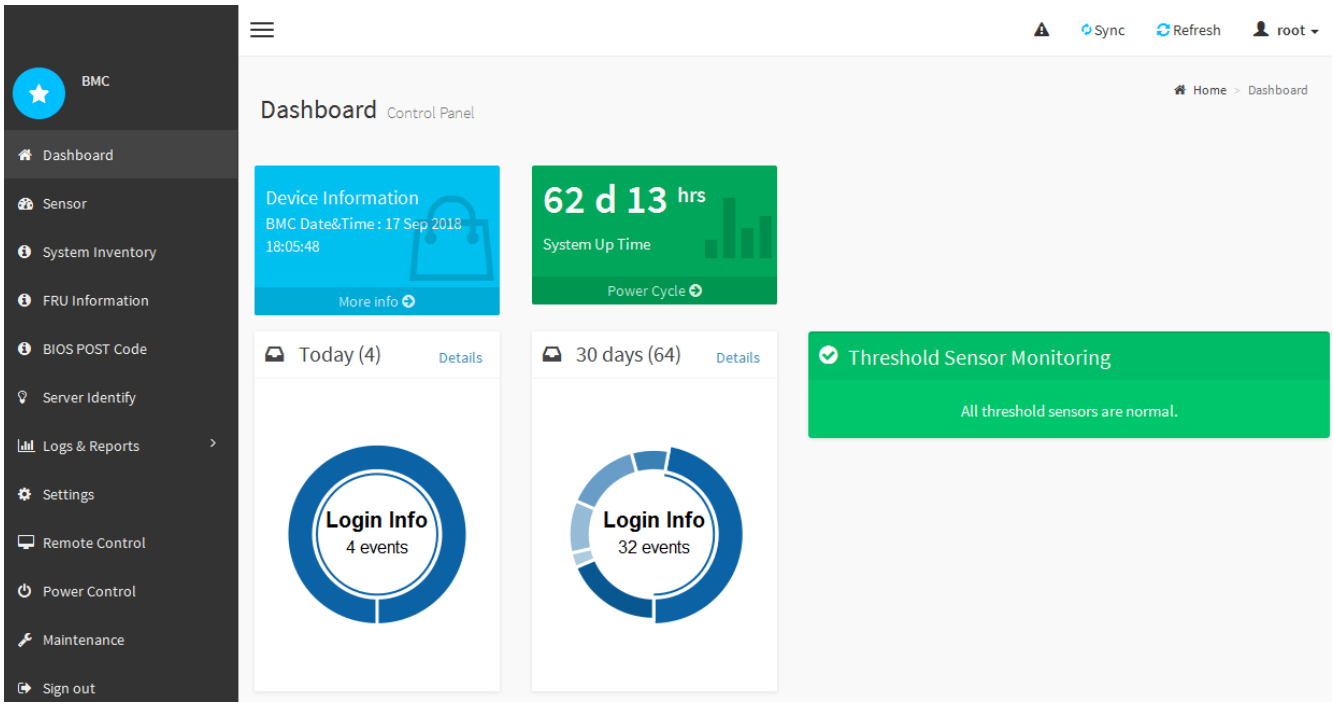
   É apresentada a página de início de sessão do BMC.

2. Digite o nome de usuário e a senha raiz, usando a senha que você definiu quando você alterou a senha padrão do root
   `root`
   `password`



3. Selecione **entrar**.

   O painel BMC é exibido.



4. Opcionalmente, crie usuários adicionais selecionando **Configurações Gerenciamento de usuários** e clicando em qualquer usuário "habilitado".

> Quando os usuários entram pela primeira vez, eles podem ser solicitados a alterar sua senha para aumentar a segurança.

Informações relacionadas

"Alterar a senha raiz da interface BMC"

Configurar definições SNMP para o controlador SG6000-CN

Se estiver familiarizado com a configuração do SNMP para hardware, pode utilizar a interface BMC para configurar as definições SNMP para o controlador SG6000-CN. Você pode fornecer strings de comunidade seguras, ativar Trap SNMP e especificar até cinco destinos SNMP.

O que você vai precisar

- Você sabe como acessar o painel do BMC.
- Tem experiência em configurar definições SNMP para equipamento SNMPv1-v2c.

Passos

1. No painel BMC, selecione **Configurações Configurações Configurações SNMP**.
2. Na página Configurações SNMP, selecione **Ativar SNMP V1/V2** e, em seguida, forneça uma String comunitária somente leitura e uma String Comunidade de leitura-escrita.

   A String da Comunidade somente leitura é como uma ID de usuário ou senha. Você deve alterar esse valor para evitar que intrusos obtenham informações sobre a configuração da rede. A cadeia de Comunidade de leitura-escrita protege o dispositivo contra alterações não autorizadas.

3. Opcionalmente, selecione **Ativar Trap** e insira as informações necessárias.

Introduza o IP de destino para cada trap SNMP utilizando um endereço IP. Nomes de domínio totalmente qualificados não são suportados.

Ative traps se quiser que o controlador SG6000-CN envie notificações imediatas para um console SNMP quando ele estiver em um estado incomum. Os traps podem indicar falhas de hardware de vários componentes ou limites de temperatura que estão sendo excedidos.

4. Opcionalmente, clique em **Send Test Trap** para testar suas configurações.
5. Se as configurações estiverem corretas, clique em **Salvar**.

Configurar notificações por e-mail para alertas

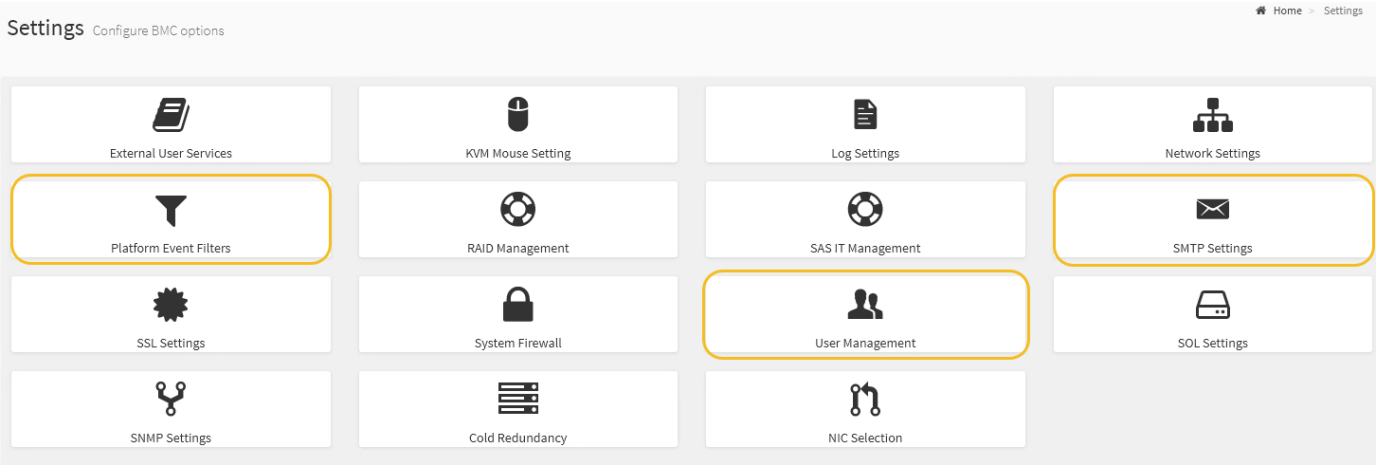
Se você quiser que as notificações por e-mail sejam enviadas quando os alertas ocorrerem, use a interface do BMC para configurar as configurações SMTP, usuários, destinos de LAN, políticas de alerta e filtros de eventos.

O que você vai precisar

Você sabe como acessar o painel do BMC.

Sobre esta tarefa

Na interface do BMC, você usa as opções **Configurações SMTP**, **Gerenciamento de usuários** e **filtros de evento da plataforma** na página Configurações para configurar notificações por e-mail.



Passos

1. Configure as definições SMTP.
   a. Selecione **Configurações Configurações SMTP**.
   b. Para a ID de e-mail do remetente, introduza um endereço de e-mail válido.

      Este endereço de e-mail é fornecido como o endereço de quando o BMC envia e-mail.

2. Configure os usuários para receber alertas.
   a. No painel do BMC, selecione **Configurações Gerenciamento de usuários**.
   b. Adicione pelo menos um usuário para receber notificações de alerta.

      O endereço de e-mail que você configura para um usuário é o endereço para o qual o BMC envia notificações de alerta. Por exemplo, você pode adicionar um usuário genérico, como "usuário de

notificação", e usar o endereço de e-mail de uma lista de distribuição de e-mail da equipe de suporte técnico.

3. Configure o destino da LAN para alertas.
   a. Selecione **Configurações filtros de evento de plataforma Destinos de LAN**.
   b. Configure pelo menos um destino de LAN.
      - Selecione **Email** como tipo de destino.
      - Para Nome de usuário do BMC, selecione um nome de usuário que você adicionou anteriormente.
      - Se você adicionou vários usuários e quer que todos eles recebam e-mails de notificação, você deve adicionar um destino de LAN para cada usuário.
   c. Envie um alerta de teste.
4. Configure políticas de alerta para que você possa definir quando e onde o BMC envia alertas.
   a. Selecione **Configurações filtros de evento da plataforma políticas de alerta**.
   b. Configure pelo menos uma política de alerta para cada destino de LAN.
      - Para número do Grupo de políticas, selecione **1**.
      - Para Ação de Política, selecione **sempre enviar alerta para este destino**.
      - Para Canal LAN, selecione **1**.
      - No Seletor de destinos, selecione o destino da LAN para a política.
5. Configure filtros de eventos para direcionar alertas para diferentes tipos de eventos para os usuários apropriados.
   a. Selecione **Configurações filtros de evento da plataforma filtros de evento**.
   b. Para o número do grupo de políticas de alerta, digite **1**.
   c. Crie filtros para cada evento sobre o qual você deseja que o Grupo de políticas de Alerta seja notificado.
      - Você pode criar filtros de eventos para ações de energia, eventos de sensor específicos ou todos os eventos.
      - Se você não tiver certeza sobre quais eventos monitorar, selecione **todos os sensores** para tipo de sensor e **todos os eventos** para Opções de evento. Se receber notificações indesejadas, pode alterar as suas seleções mais tarde.

Opcional: Habilitando a criptografia de nó

Se você ativar a criptografia de nó, os discos do seu dispositivo podem ser protegidos pela criptografia de servidor de gerenciamento de chaves (KMS) seguro contra perda física ou remoção do site. Você deve selecionar e ativar a criptografia de nó durante a instalação do dispositivo e não pode desmarcar a criptografia de nó depois que o processo de criptografia KMS for iniciado.

O que você vai precisar

Consulte as informações sobre o KMS nas instruções de administração do StorageGRID.

Sobre esta tarefa

Um dispositivo com criptografia de nó ativada se coneta ao servidor de gerenciamento de chaves externas (KMS) configurado para o site StorageGRID. Cada cluster KMS (ou KMS) gerencia as chaves de criptografia

para todos os nós de dispositivo no local. Essas chaves criptografam e descriptografam os dados em cada disco em um dispositivo que tem criptografia de nó ativada.

Um KMS pode ser configurado no Gerenciador de Grade antes ou depois que o dispositivo é instalado no StorageGRID. Consulte as informações sobre a configuração do KMS e do appliance nas instruções de administração do StorageGRID para obter detalhes adicionais.

- Se um KMS for configurado antes de instalar o dispositivo, a criptografia controlada pelo KMS será iniciada quando você ativar a criptografia de nó no dispositivo e adicioná-la a um site do StorageGRID onde o KMS está configurado.
- Se um KMS não for configurado antes de instalar o dispositivo, a criptografia controlada por KMS é executada em cada dispositivo que tem criptografia de nó ativada assim que um KMS é configurado e disponível para o site que contém o nó do dispositivo.

> Todos os dados existentes antes de um dispositivo que tenha criptografia de nó ativada se conetarem ao KMS configurado são criptografados com uma chave temporária que não é segura. O aparelho não está protegido contra remoção ou roubo até que a chave esteja definida para um valor fornecido pelo KMS.

Sem a chave KMS necessária para descriptografar o disco, os dados no dispositivo não podem ser recuperados e são efetivamente perdidos. Este é o caso sempre que a chave de descriptografia não pode ser recuperada do KMS. A chave fica inacessível se um cliente limpar a configuração do KMS, uma chave KMS expira, a conexão com o KMS é perdida ou o dispositivo é removido do sistema StorageGRID onde suas chaves KMS são instaladas.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo.

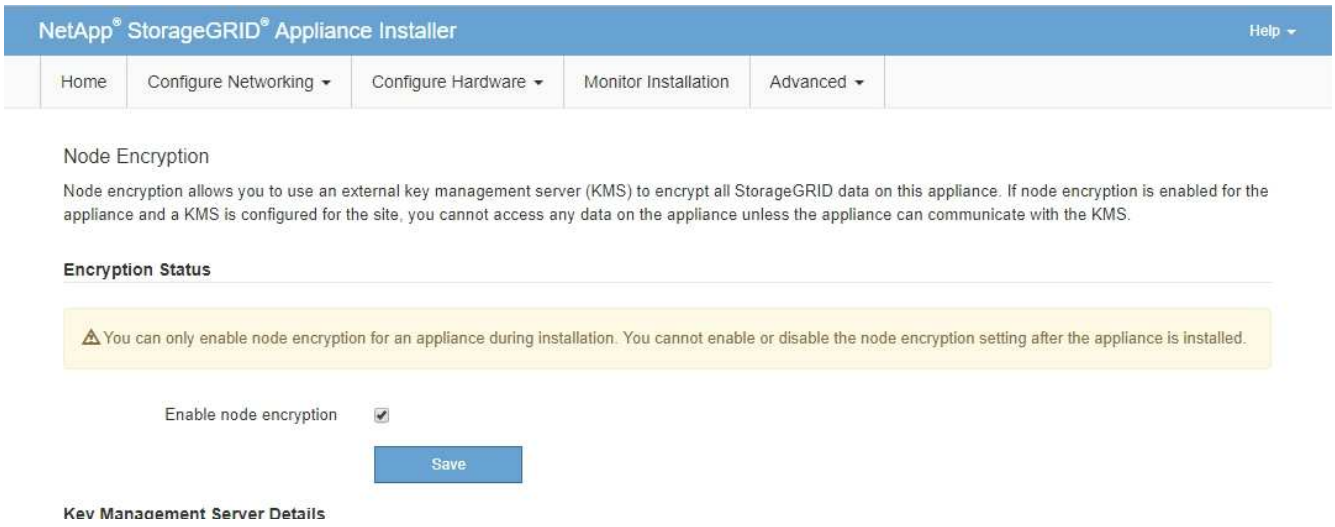
   `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

   > Depois que o dispositivo tiver sido criptografado com uma chave KMS, os discos do appliance não podem ser descriptografados sem usar a mesma chave KMS.

2. Selecione **Configure hardware Node Encryption**.



3. Selecione **Ativar criptografia de nó**.

   Você pode desmarcar **Ativar criptografia de nó** sem risco de perda de dados até selecionar **Salvar** e o nó do dispositivo acessar as chaves de criptografia KMS em seu sistema StorageGRID e iniciar a criptografia de disco. Não é possível desativar a criptografia de nó após a instalação do dispositivo.

   > Depois de adicionar um dispositivo que tenha a criptografia de nó ativada a um site do StorageGRID que tenha um KMS, você não poderá parar de usar a criptografia KMS para o nó.

4. Selecione **Guardar**.
5. Implante o dispositivo como um nó no sistema StorageGRID.

   A encriptação controlada POR KMS começa quando o dispositivo acede às chaves KMS configuradas para o seu site StorageGRID. O instalador exibe mensagens de progresso durante o processo de criptografia KMS, o que pode levar alguns minutos, dependendo do número de volumes de disco no dispositivo.

   > Os dispositivos são configurados inicialmente com uma chave de criptografia aleatória não KMS atribuída a cada volume de disco. Os discos são criptografados usando essa chave de criptografia temporária, que não é segura, até que o dispositivo que tem criptografia de nó habilitada acesse as chaves KMS configuradas para o site do StorageGRID.

Depois de terminar

Você pode exibir o status da criptografia do nó, os detalhes do KMS e os certificados em uso quando o nó do dispositivo está no modo de manutenção.

Informações relacionadas

"Administrar o StorageGRID"

"Monitorização da encriptação do nó no modo de manutenção"

Opcional: Alterar o modo RAID (apenas SG6000)

Você pode mudar para um modo RAID diferente no dispositivo para acomodar seus requisitos de armazenamento e recuperação. Você só pode alterar o modo antes de

implantar o nó de storage do dispositivo.

O que você vai precisar

- Você está usando qualquer cliente que possa se conetar ao StorageGRID.
- O cliente tem um navegador da Web suportado.

Sobre esta tarefa

Antes de implantar o dispositivo como nó de storage, você pode escolher uma das seguintes opções de configuração de volume:

- **DDP**: Esse modo usa duas unidades de paridade para cada oito unidades de dados. Este é o modo padrão e recomendado para todos os aparelhos. Em comparação com o RAID6, o DDP oferece melhor performance do sistema, tempos de reconstrução reduzidos após falhas de unidade e facilidade de gerenciamento. O DDP também fornece proteção contra perda de gaveta em dispositivos de 60 unidades.
- **DDP16**: Esse modo usa duas unidades de paridade para cada unidade de dados de 16 TB, o que resulta em maior eficiência de storage em comparação com o DDP. Em comparação com o RAID6, o DDP16 oferece melhor desempenho do sistema, tempos de reconstrução reduzidos após falhas de unidade, facilidade de gerenciamento e eficiência de storage comparável. Para usar o modo DDP16, sua configuração deve conter pelo menos 20 unidades. DDP16 não fornece proteção contra perda de gaveta.
- **RAID6**: Este modo usa duas unidades de paridade para cada 16 ou mais unidades de dados. Para usar o modo RAID 6, sua configuração deve conter pelo menos 20 unidades. Embora o RAID6 possa aumentar a eficiência de storage do dispositivo em comparação com o DDP, ele não é recomendado para a maioria dos ambientes StorageGRID.

> Se algum volume já tiver sido configurado ou se o StorageGRID tiver sido instalado anteriormente, a alteração do modo RAID fará com que os volumes sejam removidos e substituídos. Quaisquer dados sobre esses volumes serão perdidos.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo.

   `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Avançado modo RAID**.
3. Na página **Configurar modo RAID**, selecione o modo RAID desejado na lista suspensa modo.
4. Clique em **Salvar**.

Informações relacionadas

"Site de Documentação de sistemas NetApp e-Series"

Opcional: Remapeamento de portas de rede para o dispositivo

Talvez seja necessário remapear as portas internas no nó de armazenamento do dispositivo para diferentes portas externas. Por exemplo, talvez seja necessário remapear as portas devido a um problema de firewall.

O que você vai precisar

- Você acessou anteriormente o Instalador de dispositivos StorageGRID.
- Você não configurou e não planeja configurar pontos de extremidade do balanceador de carga.

> Se você remapear quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Se você quiser configurar pontos de extremidade do balanceador de carga e já tiver portas remapeadas, siga as etapas nas instruções de recuperação e manutenção para remover os remapes de portas.

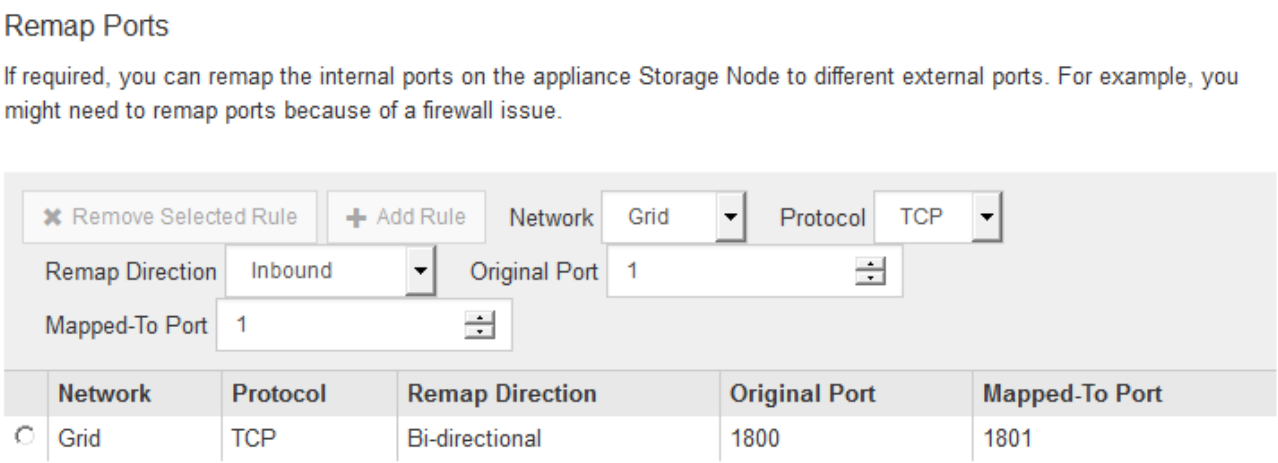
Passos

1. No Instalador de dispositivos StorageGRID, clique em **Configurar rede Remapear portas**.

   É apresentada a página Remapear porta.

2. Na caixa suspensa **rede**, selecione a rede para a porta que deseja remapear: Grade, Admin ou Cliente.
3. Na caixa suspensa **Protocol** (Protocolo), selecione o protocolo IP: TCP ou UDP.
4. Na caixa suspensa **Remap Direction**, selecione qual direção de tráfego você deseja remapear para esta porta: Inbound, Outbound ou Bi-direcional.
5. Para **original Port**, insira o número da porta que deseja remapear.
6. Para **Mapped-to Port**, insira o número da porta que deseja usar.
7. Clique em **Adicionar regra**.

   O novo mapeamento de portas é adicionado à tabela e o remapeamento entra em vigor imediatamente.



8. Para remover um mapeamento de portas, selecione o botão de opção da regra que deseja remover e clique em **Remover regra selecionada**.

Implantando um nó de storage de dispositivos

Depois de instalar e configurar o dispositivo de storage, você pode implantá-lo como um nó de storage em um sistema StorageGRID. Ao implantar um dispositivo como nó de storage, você usa o Instalador de dispositivos StorageGRID incluído no dispositivo.

O que você vai precisar

- Se você estiver clonando um nó de dispositivo, continue seguindo o processo de recuperação e manutenção.

  "Manter recuperar"

- O dispositivo foi instalado em um rack ou gabinete, conetado às redes e ligado.
- Links de rede, endereços IP e remapeamento de portas (se necessário) foram configurados para o dispositivo usando o Instalador de dispositivos StorageGRID.
- Você conhece um dos endereços IP atribuídos ao controlador de computação do dispositivo. Você pode usar o endereço IP de qualquer rede StorageGRID conetada.
- O nó de administração principal do sistema StorageGRID foi implantado.
- 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.
- Você tem um laptop de serviço com um navegador da Web suportado.

Sobre esta tarefa

Cada dispositivo de storage funciona como um nó de storage único. Qualquer dispositivo pode se conetar à rede de Grade, à rede Admin e à rede Cliente

Para implantar um nó de armazenamento de dispositivos em um sistema StorageGRID, você acessa o Instalador de dispositivos StorageGRID e executa as seguintes etapas:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do nó de armazenamento.
- Você inicia a implantação e espera à medida que os volumes são configurados e o software é instalado.
- Quando a instalação é interrompida parcialmente nas tarefas de instalação do dispositivo, você retoma a instalação iniciando sessão no Gerenciador de Grade, aprovando todos os nós de grade e concluindo os processos de instalação e implantação do StorageGRID.

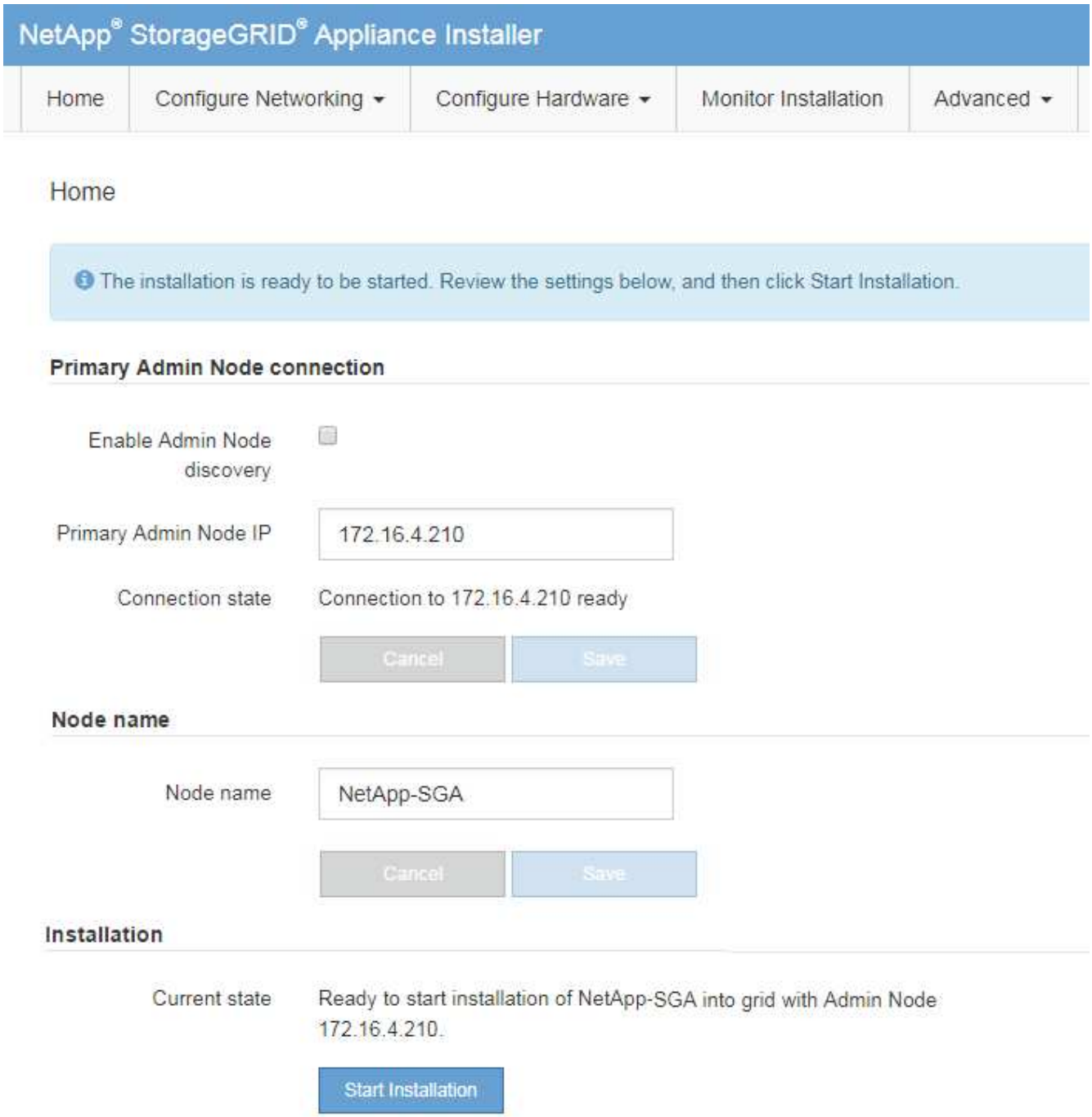
> Se você precisar implantar vários nós de dispositivo de uma só vez, você pode automatizar o processo de instalação usando o `configure-sga.py` script de instalação do dispositivo.

- Se você estiver executando uma operação de expansão ou recuperação, siga as instruções apropriadas:
  - Para adicionar um nó de storage do dispositivo a um sistema StorageGRID existente, consulte as instruções para expandir um sistema StorageGRID.
  - Para implantar um nó de armazenamento de dispositivos como parte de uma operação de recuperação, consulte as instruções para recuperação e manutenção.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `https://Controller_IP:8443`

   A página inicial do instalador do dispositivo StorageGRID é exibida.



2. Na seção **conexão do 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 clique em **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 `node name` na grade com nó Admin principal `*admin_ip*`" e se o botão **Iniciar instalação** está ativado.

   Se o botão **Start Installation** (Iniciar instalação) não estiver ativado, poderá ser necessário alterar a configuração da rede ou as definições da porta. Para obter instruções, consulte as instruções de instalação e manutenção do seu aparelho.

   > Se você estiver implantando o dispositivo Storage Node como um destino de clonagem de nós, interrompa o processo de implantação aqui e continue o procedimento de clonagem de nós na recuperação e na manutenção. E "Manter recuperar"

6. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.

   O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

   > Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor**.

7. Se a grade incluir vários nós de storage do dispositivo, repita estas etapas 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 `configure-sga.py` script de instalação do dispositivo. Este script se aplica somente aos nós de storage.

Informações relacionadas

"Expanda sua grade"

"Manter recuperar"

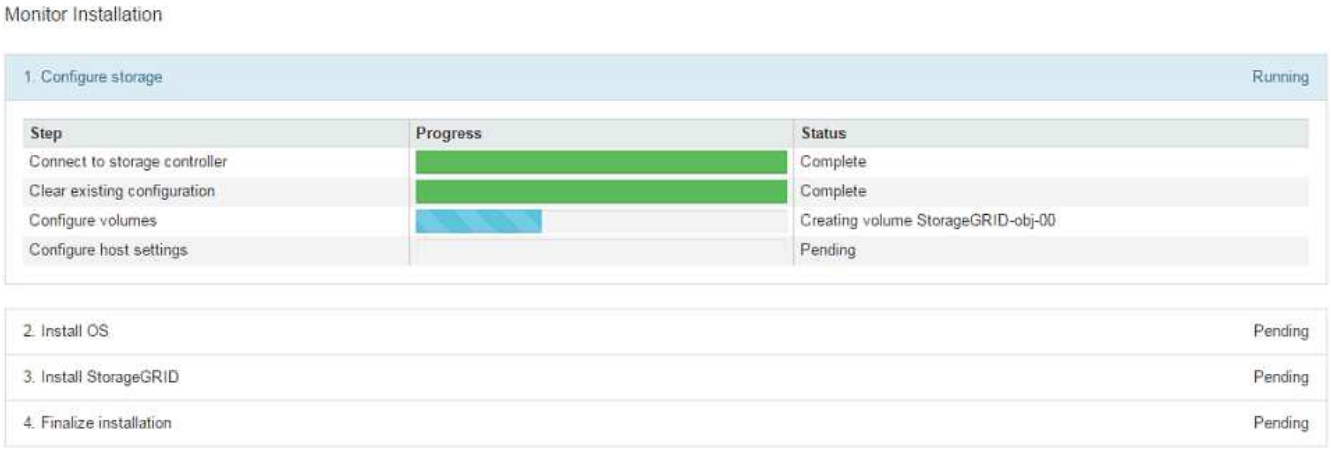
Monitorização da instalação do dispositivo de armazenamento

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**.

   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 serão mostradas com uma barra de status verde e um status de ""pulado"".

2. Reveja o progresso das duas primeiras fases de instalação.

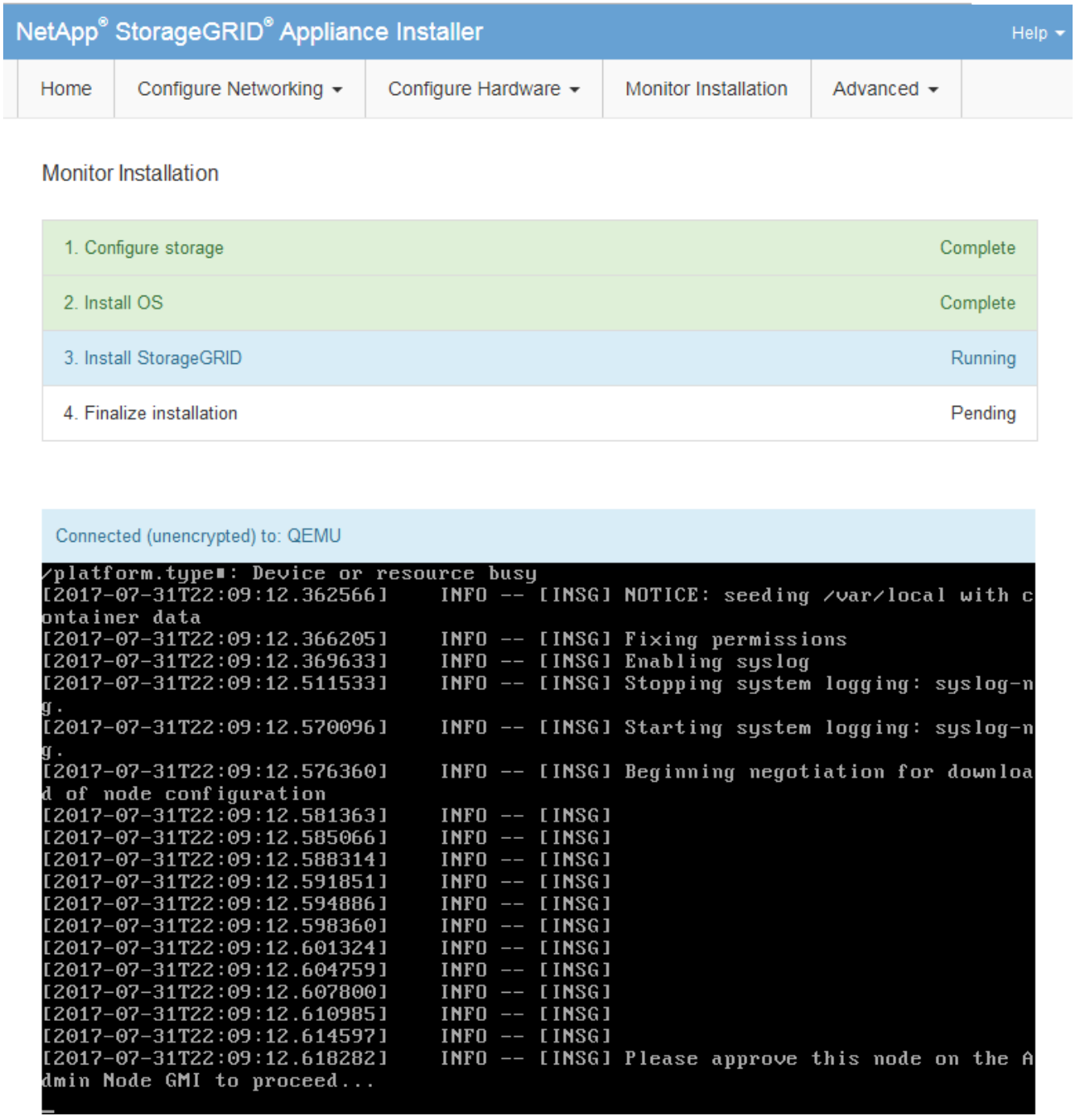
   1. Configurar armazenamento

   Durante essa etapa, o instalador se coneta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o software SANtricity para configurar volumes e configura as configurações do host.

   2. Instale o os

Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID para o dispositivo.

3. Continue monitorando o progresso da instalação até que o estágio **Install StorageGRID** pare e uma mensagem seja exibida no console incorporado, solicitando que você aprove esse nó no nó Admin usando o Gerenciador de Grade. Vá para a próxima etapa.



4. Vá para o Gerenciador de Grade, aprove o nó de armazenamento pendente e conclua o processo de instalação do StorageGRID.

   Quando você clica em **Install** no Gerenciador de Grade, o estágio 3 é concluído e o estágio 4, **Finalize a instalação**, começa. Quando a fase 4 é concluída, o controlador é reinicializado.

Automatizando a instalação e a configuração do dispositivo

Você pode automatizar a instalação e configuração de seus dispositivos e a configuração de todo o sistema StorageGRID.

Sobre esta tarefa

A automação da instalação e configuração pode ser útil para implantar várias instâncias do StorageGRID ou uma instância grande e complexa do StorageGRID.

Para automatizar a instalação e a configuração, use uma ou mais das seguintes opções:

- Crie um arquivo JSON que especifique as configurações para seus dispositivos. Carregue o arquivo JSON usando o instalador do dispositivo StorageGRID.

  Você pode usar o mesmo arquivo para configurar mais de um dispositivo.

- Use o script Python do StorageGRID`configure-sga.py` para automatizar a configuração de seus dispositivos.
- Use scripts Python adicionais para configurar outros componentes de todo o sistema StorageGRID (a "grade").

Você pode usar os scripts Python de automação do StorageGRID diretamente ou usá-los como exemplos de como usar a API REST de instalação do StorageGRID nas ferramentas de implantação e configuração de grade que você mesmo desenvolve. Consulte as informações sobre como baixar e extrair os arquivos de instalação do StorageGRID nas instruções de recuperação e manutenção.

Automatizando a configuração do dispositivo usando o Instalador de dispositivos StorageGRID

Você pode automatizar a configuração de um appliance usando um arquivo JSON que contém as informações de configuração. Você carrega o arquivo usando o Instalador do StorageGRID Appliance.

O que você vai precisar

- O seu dispositivo tem de estar no firmware mais recente compatível com o StorageGRID 11,5 ou superior.
- Você deve estar conetado ao Instalador do StorageGRID Appliance no dispositivo que você está configurando usando um navegador compatível.

Sobre esta tarefa

É possível automatizar as tarefas de configuração do dispositivo, como configurar o seguinte:

- Rede de grade, rede de administração e endereços IP da rede de cliente
- Interface BMC
- Ligações de rede
  - Modo de ligação da porta
  - Modo de ligação de rede
  - Velocidade da ligação

Configurar o dispositivo usando um arquivo JSON carregado geralmente é mais eficiente do que executar a

configuração manualmente usando várias páginas no Instalador de dispositivos StorageGRID, especialmente se você tiver que configurar muitos nós. Você deve aplicar o arquivo de configuração para cada nó um de cada vez.

> Usuários experientes que desejam automatizar tanto a instalação quanto a configuração de seus dispositivos podem usar o `configure-sga.py` script. E "Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py"

Passos

1. Gere o arquivo JSON usando um dos seguintes métodos:
   - O aplicativo ConfigBuilder

     "ConfigBuilder.NetApp.com"

   - O `configure-sga.py` script de configuração do dispositivo. Você pode baixar o script do Instalador do StorageGRID Appliance (**Ajuda Script de configuração do appliance**). Consulte as instruções sobre como automatizar a configuração usando o script configure-sga.py.

     "Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py"

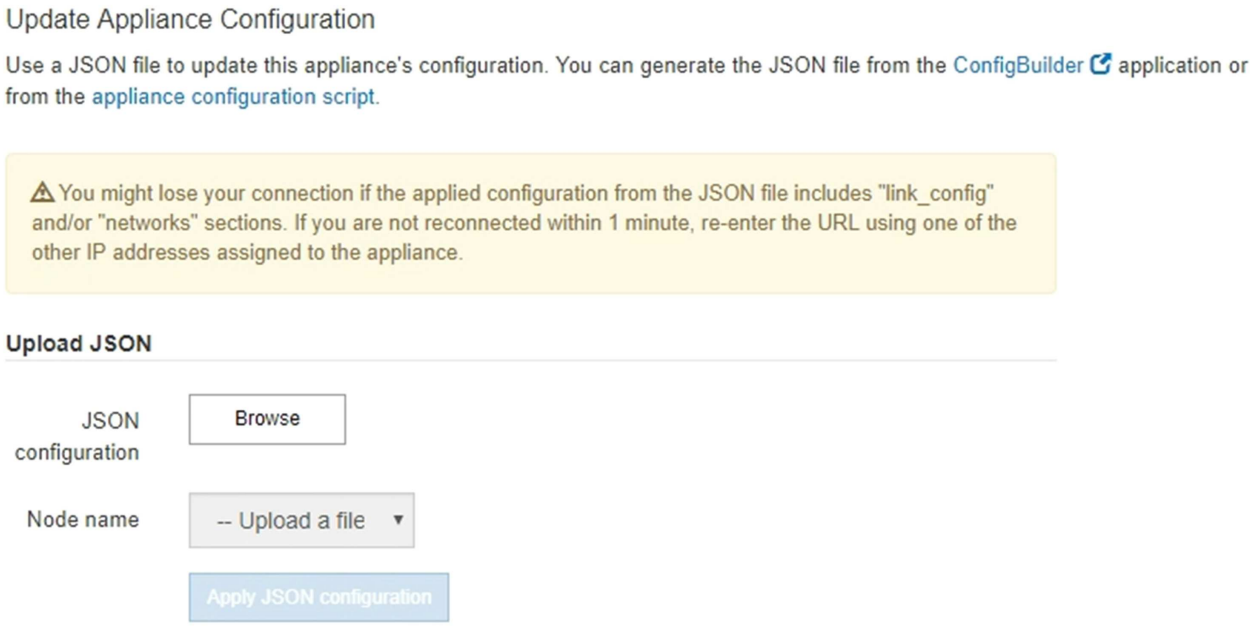
     Os nomes de nós no arquivo JSON devem seguir estes requisitos:

   - Deve ser um nome de host válido contendo pelo menos 1 e não mais de 32 carateres
   - Pode usar letras, números e hífens são permitidos
   - Não é possível iniciar ou terminar com um hífen ou conter apenas números

     > Certifique-se de que os nomes dos nós (os nomes de nível superior) no arquivo JSON sejam únicos, ou você não poderá configurar mais de um nó usando o arquivo JSON.

2. Selecione **Avançado Atualizar Configuração do dispositivo**.

   É apresentada a página Update Appliance Configuration (Atualizar configuração do dispositivo).



3. Selecione o arquivo JSON com a configuração que você deseja carregar.

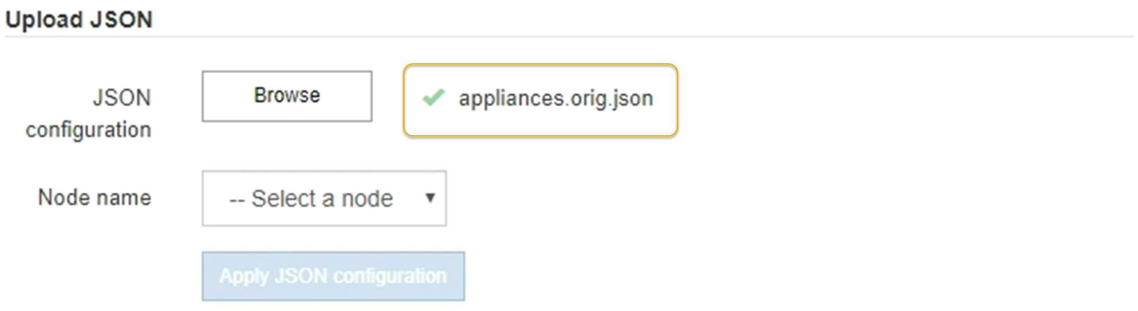
   a. Selecione **Procurar**.

   b. Localize e selecione o ficheiro.

   c. Selecione **Open**.

   O arquivo é carregado e validado. Quando o processo de validação estiver concluído, o nome do ficheiro é apresentado junto a uma marca de verificação verde.

   > Você pode perder a conexão com o dispositivo se a configuração do arquivo JSON incluir seções para "link_config", "redes" ou ambos. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do dispositivo usando um dos outros endereços IP atribuídos ao dispositivo.

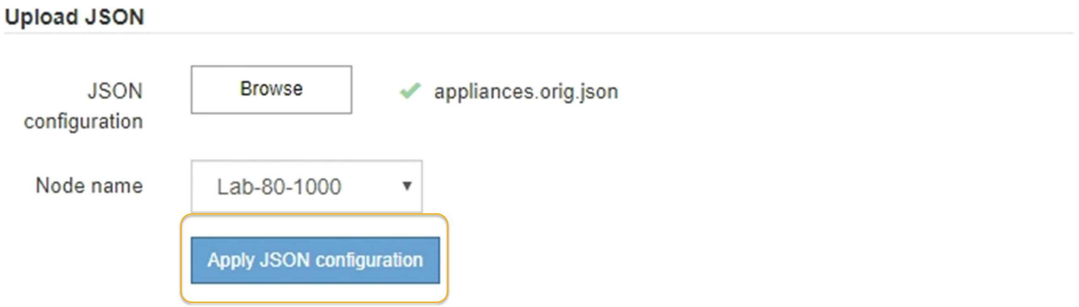


   A lista suspensa **Nome do nó** é preenchida com os nomes de nós de nível superior definidos no arquivo JSON.

Se o arquivo não for válido, o nome do arquivo será exibido em vermelho e uma mensagem de erro será exibida em um banner amarelo. O ficheiro inválido não é aplicado ao dispositivo. Você pode usar o ConfigBuilder para garantir que você tenha um arquivo JSON válido.

4. Selecione um nó na lista suspensa **Nome do nó**.

   O botão **Apply JSON Configuration** está ativado.



5. Selecione **Apply JSON Configuration**.

   A configuração é aplicada ao nó selecionado.

Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py

Você pode usar `configure-sga.py` o script para automatizar muitas das tarefas de instalação e configuração para os nós de dispositivos StorageGRID, incluindo a instalação e configuração de um nó de administrador principal. Este script pode ser útil se você tiver um grande número de dispositivos para configurar. Você também pode usar o script para gerar um arquivo JSON que contém informações de configuração do dispositivo.

O que você vai precisar

- O dispositivo foi instalado em um rack, conetado às redes e ligado.
- Links de rede e endereços IP foram configurados para o nó de administração principal usando o instalador do dispositivo StorageGRID.
- Se você estiver instalando o nó Admin principal, você saberá seu endereço IP.
- Se você estiver instalando e configurando outros nós, o nó Admin principal foi implantado e você sabe seu endereço IP.
- Para todos os nós que não o nó de administração principal, 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.
- Você baixou o `configure-sga.py` arquivo. O arquivo está incluído no arquivo de instalação, ou você pode acessá-lo clicando em **Ajuda Script de Instalação do dispositivo** no Instalador do StorageGRID Appliance.

Este procedimento é para usuários avançados com alguma experiência usando interfaces de linha de comando. Como alternativa, você também pode usar o Instalador de dispositivos StorageGRID para automatizar a configuração. E "Automatizando a configuração do dispositivo usando o Instalador de dispositivos StorageGRID"

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Para obter ajuda geral com a sintaxe do script e para ver uma lista dos parâmetros disponíveis, digite o seguinte:

```
configure-sga.py --help
```

O `configure-sga.py` script usa cinco subcomandos:

- `advanced` Para interações avançadas do StorageGRID Appliance, incluindo a configuração do BMC e a criação de um arquivo JSON contendo a configuração atual do dispositivo
- `configure` Para configurar o modo RAID, o nome do nó e os parâmetros de rede
- `install` Para iniciar uma instalação do StorageGRID
- `monitor` Para monitorar uma instalação do StorageGRID
- `reboot` para reiniciar o aparelho

Se você inserir um argumento de subcomando (avançado, configurar, instalar, monitorar ou reiniciar) seguido da `--help` opção, você receberá um texto de ajuda diferente fornecendo mais detalhes sobre as opções disponíveis dentro desse subcomando
`configure-sga.py` *`subcommand`* `--help`

3. Para confirmar a configuração atual do nó do dispositivo, digite o seguinte local *`SGA-install-ip`* onde está qualquer um dos endereços IP do nó do dispositivo
`configure-sga.py configure` *`SGA-INSTALL-IP`*

Os resultados mostram informações de IP atuais para o dispositivo, incluindo o endereço IP do nó de administração principal e informações sobre as redes de administração, grade e cliente.

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200
```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
             192.168.0.0/21
```

```
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. Se você precisar alterar qualquer um dos valores na configuração atual, use o `configure` subcomando para atualizá-los. Por exemplo, se você quiser alterar o endereço IP que o dispositivo usa para conexão com o nó Admin principal para `172.16.2.99`, digite o seguinte
`configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP`
5. Se você quiser fazer backup da configuração do appliance em um arquivo JSON, use os `advanced` subcomandos e `backup-file` . Por exemplo, se você quiser fazer backup da configuração de um dispositivo com endereço IP *SGA-INSTALL-IP* para um arquivo chamado `appliance-SG1000.json`, digite o seguinte
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

   O arquivo JSON contendo as informações de configuração é gravado no mesmo diretório do qual você executou o script.

   > Verifique se o nome do nó de nível superior no arquivo JSON gerado corresponde ao nome do dispositivo. Não faça alterações neste arquivo, a menos que você seja um usuário experiente e tenha uma compreensão completa das APIs do StorageGRID.

6. Quando estiver satisfeito com a configuração do aparelho, utilize os `install` subcomandos e `monitor` para instalar o aparelho
`configure-sga.py install --monitor SGA-INSTALL-IP`
7. Se pretender reiniciar o aparelho, introduza o seguinte
`configure-sga.py reboot SGA-INSTALL-IP`

Automatizando a configuração do StorageGRID

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

O que você vai precisar

- 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 amostra (`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
   ```

Depois de terminar

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, você precisa extrair o `Passwords.txt` arquivo e procurar 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.
```

Visão geral das APIs REST de instalação

O StorageGRID fornece duas APIs REST para executar tarefas de instalação: A API de instalação do StorageGRID e a API do instalador do dispositivo StorageGRID.

Ambas as APIs usam 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 (JavaScript Object Notation).

> Todas as operações de API que você executa usando a página da Web do API Docs 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 seu sistema StorageGRID e, caso precise 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.

API do instalador do dispositivo StorageGRID

A API do instalador do dispositivo StorageGRID pode ser acessada por HTTPS a partir `*Controller_IP*:8443`do .

Para acessar a documentação da API, vá para o Instalador do StorageGRID Appliance no appliance e selecione **Ajuda Documentação da API** na barra de menus.

A API do instalador do StorageGRID Appliance inclui as seguintes seções:

- **Clone** — operações para configurar e controlar a clonagem de nós.
- **Encryption** — operações para gerenciar a criptografia e visualizar o status da criptografia.
- **Configuração de hardware** — operações para configurar as configurações do sistema no hardware conetado.
- **Installation** — operações para iniciar a instalação do aparelho e para monitorar o status da instalação.
- **Networking** — operações relacionadas à configuração de rede, administrador e rede cliente para um dispositivo StorageGRID e configurações de porta de dispositivo.
- **Setup** — operações para ajudar na configuração inicial da instalação do dispositivo, incluindo solicitações para obter informações sobre o sistema e atualizar o IP do nó de administração principal.
- **Support** — operações para reiniciar o controlador e obter logs.
- **Upgrade** — operações relacionadas à atualização do firmware do appliance.
- * Uploadsg* — operações para upload de arquivos de instalação do StorageGRID.

Solução de problemas da instalação do hardware

Se você encontrar problemas durante a instalação, talvez seja útil revisar informações de solução de problemas relacionadas a problemas de configuração de hardware e

conetividade.

Informações relacionadas

"A configuração do hardware parece travar"

"Solução de problemas de conexão"

Visualizar códigos de inicialização para o controlador SG6000-CN

Quando você aplica energia ao aparelho, o BMC Registra uma série de códigos de inicialização para o controlador SG6000-CN. Você pode visualizar esses códigos de várias maneiras.

O que você vai precisar

- Você sabe como acessar o painel do BMC.
- Se você quiser usar uma máquina virtual baseada em kernel (KVM), você tem experiência em implantar e usar aplicativos KVM.
- Se você quiser usar serial-over-laN (sol), você tem experiência usando aplicativos de console IPMI sol.

Passos

1. Selecione um dos seguintes métodos para visualizar os códigos de arranque do controlador do aparelho e recolha o equipamento necessário.

Método	Equipamento necessário
Consola VGA	• Monitor compatível com VGA • Cabo VGA
KVM	• Aplicação KVM • Cabo RJ-45
Porta serial	• Cabo serial DB-9 • Terminal serial virtual
SOL	• Terminal serial virtual

2. Se você estiver usando um console VGA, execute estas etapas:
   a. Ligue um monitor compatível com VGA à porta VGA na parte posterior do aparelho.
   b. Veja os códigos exibidos no monitor.
3. Se você estiver usando o BMC KVM, execute estas etapas:
   a. Conete-se à porta de gerenciamento do BMC e faça login na interface da Web do BMC.
   b. Selecione **Controle remoto**.
   c. Inicie o KVM.
   d. Veja os códigos no monitor virtual.
4. Se você estiver usando uma porta serial e um terminal, execute estas etapas:

a. Conete-se à porta serial DB-9 na parte traseira do aparelho.
b. Utilize as definições `115200 8-N-1`.
c. Veja os códigos impressos no terminal serial.

5. Se você estiver usando sol, execute estas etapas:
   a. Conete-se ao sol IPMI usando o endereço IP BMC e as credenciais de login.

      ```
      ipmitool -I lanplus -H 10.224.3.91 -U root -P calvin sol activate
      ```

   b. Veja os códigos no terminal serial virtual.
6. Utilize a tabela para procurar os códigos do seu aparelho.

Código	Indica
OLÁ	O script de inicialização mestre foi iniciado.
HP	O sistema está verificando se o firmware da placa de interface de rede (NIC) precisa ser atualizado.
RB	O sistema está reiniciando após a aplicação de atualizações de firmware.
FP	As verificações de atualização do firmware do subsistema de hardware foram concluídas. Os serviços de comunicação entre controladores estão a iniciar.
ELE	Somente para um nó de storage de dispositivo: O sistema está aguardando conetividade com os controladores de armazenamento e sincronização com o sistema operacional SANtricity. **Nota:** se o procedimento de inicialização não avançar além desta etapa, execute estas etapas: a. Confirme se os quatro cabos de interconexão entre o controlador SG6000-CN e os dois controladores de armazenamento estão bem conetados. b. Se necessário, substitua um ou mais cabos e tente novamente. c. Se isso não resolver o problema, entre em Contato com o suporte técnico.
HC	O sistema está a verificar se existem dados de instalação do StorageGRID.

Código	Indica
HO	O Instalador de dispositivos StorageGRID está em execução.
HA	O StorageGRID está em execução.

Visualizar códigos de erro para o controlador SG6000-CN

Se ocorrer um erro de hardware quando o controlador SG6000-CN está a arrancar, o BMC regista um código de erro. Conforme necessário, você pode visualizar esses códigos de erro usando a interface do BMC e trabalhar com suporte técnico para resolver o problema.

O que você vai precisar

- Você sabe como acessar o painel do BMC.

Passos

1. No painel do BMC, selecione **Código POST do BIOS**.
2. Reveja as informações apresentadas para o Código atual e o Código anterior.

   Se algum dos códigos de erro a seguir for exibido, trabalhe com suporte técnico para resolver o problema.

Código	Indica
0x0E	Microcódigo não encontrado
0x0F	Microcódigo não carregado
0x50	Erro de inicialização da memória. Tipo de memória inválido ou velocidade de memória incompatível.
0x51	Erro de inicialização da memória. A leitura SPD falhou.
0x52	Erro de inicialização da memória. O tamanho de memória inválido ou os módulos de memória não correspondem.
0x53	Erro de inicialização da memória. Nenhuma memória utilizável detetada.
0x54	Erro de inicialização de memória não especificado
0x55	Memória não instalada
0x56	Tipo ou velocidade de CPU inválida

Código	Indica
0x57	Incompatibilidade de CPU
0x58	Falha no autoteste da CPU ou possível erro de cache da CPU
0x59	O micro-código da CPU não foi encontrado ou a atualização do micro-código falhou
0x5A	Erro interno da CPU
0x5B	Repor PPI não está disponível
0x5C	Falha do autoteste do PEI fase BMC
0xD0	Erro de inicialização da CPU
0xD1	Erro de inicialização da ponte Norte
0xD2	Erro de inicialização da ponte sul
0xD3	Alguns protocolos arquitetônicos não estão disponíveis
0xD4	Erro de alocação de recursos PCI. Sem recursos.
0xD5	Sem espaço para a ROM de opção herdada
0xD6	Não foram encontrados dispositivos de saída da consola
0xD7	Não foram encontrados dispositivos de entrada da consola
0xD8	Palavra-passe inválida
0xD9	Erro ao carregar a opção de inicialização (erro loadImage retornado)
0xDA	Falha na opção de inicialização (erro retornado pela StartImage)
0xDB	Falha na atualização do flash
0xDC	O protocolo de reposição não está disponível

Código	Indica
0xDD	Avaria no autoteste do BMC de fase DXE
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY
0xEF	RMC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERNAL
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

A configuração do hardware parece travar

O Instalador de dispositivos StorageGRID pode não estar disponível se falhas de hardware ou erros de cabeamento impedirem que os controladores de armazenamento ou o controlador SG6000-CN concluam seu processamento de inicialização.

Passos

1. Para os controladores de storage, observe os códigos nos monitores de sete segmentos.

   Enquanto o hardware está sendo inicializado durante a inicialização, os dois visores de sete segmentos mostram uma sequência de códigos. Quando o hardware é inicializado com êxito, as duas telas de sete segmentos mostram `99`.

2. Revise os LEDs no controlador SG6000-CN e os códigos de inicialização e erro exibidos no BMC.
3. Se você precisar de ajuda para resolver um problema, entre em Contato com o suporte técnico.

Informações relacionadas

"Exibindo códigos de status de inicialização para os controladores de storage SG6000"

"Guia de monitorização do sistema E5700 e E2800"

"Visualizar indicadores de estado e botões no controlador SG6000-CN"

"Visualizar códigos de inicialização para o controlador SG6000-CN"

"Visualizar códigos de erro para o controlador SG6000-CN"

Solução de problemas de conexão

Se você encontrar problemas de conexão durante a instalação do StorageGRID Appliance, execute as etapas de ação corretiva listadas.

Não foi possível ligar ao aparelho

Se não conseguir ligar ao dispositivo, poderá haver um problema de rede ou a instalação do hardware poderá não ter sido concluída com êxito.

Passos

1. Se você não conseguir se conetar ao Gerenciador do sistema do SANtricity:
   a. Tente fazer ping no dispositivo usando o endereço IP para qualquer controlador de armazenamento na rede de gerenciamento para o Gerenciador de sistema SANtricity
      `ping Storage_Controller_IP`
   b. Se não receber resposta do ping, confirme que está a utilizar o endereço IP correto.

      Use o endereço IP para a porta de gerenciamento 1 em qualquer controlador de armazenamento.

   c. Se o endereço IP estiver correto, verifique o cabeamento do dispositivo e a configuração da rede.

      Se isso não resolver o problema, entre em Contato com o suporte técnico.

   d. Se o ping foi bem-sucedido, abra um navegador da Web.

e. Digite o URL para o Gerenciador de sistema do SANtricity
https://*Storage_Controller_IP*

É apresentada a página de início de sessão do Gestor do sistema SANtricity.

2. Se não conseguir ligar ao controlador SG6000-CN:
   a. Tente fazer ping no aparelho usando o endereço IP do controlador SG6000-CN
   ping *SG6000-CN_Controller_IP*
   b. Se não receber resposta do ping, confirme que está a utilizar o endereço IP correto.

      Pode utilizar o endereço IP do dispositivo na rede de grelha, na rede de administração ou na rede de cliente.

   c. Se o endereço IP estiver correto, verifique o cabeamento do dispositivo, os transcetores SFP e a configuração da rede.

      Se isso não resolver o problema, entre em Contato com o suporte técnico.

   d. Se o ping foi bem-sucedido, abra um navegador da Web.
   e. Digite o URL do instalador do StorageGRID Appliance
   https://*SG6000-CN_Controller_IP*:8443

      A página inicial é exibida.

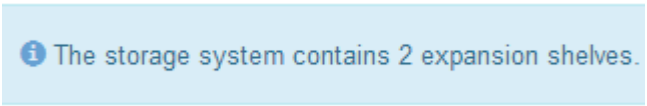
As prateleiras de expansão não aparecem no Instalador de dispositivos

Se você tiver instalado prateleiras de expansão para o SG6060 e elas não aparecerem no Instalador de dispositivos StorageGRID, verifique se as prateleiras foram completamente instaladas e ligadas.

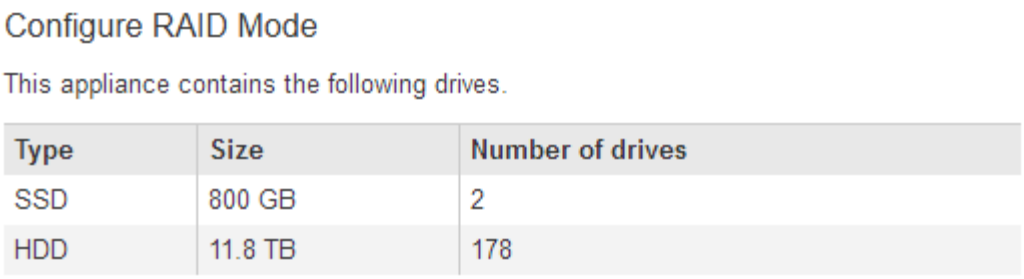
Sobre esta tarefa

Você pode verificar se os compartimentos de expansão estão conetados ao dispositivo visualizando as seguintes informações no Instalador de dispositivos StorageGRID:

- A página **Home** contém uma mensagem sobre prateleiras de expansão.



- A página **Avançado modo RAID** indica pelo número de unidades se o dispositivo inclui ou não compartimentos de expansão. Por exemplo, na captura de tela a seguir, dois SSDs e 178 HDDs são exibidos. Um SG6060 com dois compartimentos de expansão contém um total de 180 unidades.



Se as páginas do Instalador do dispositivo StorageGRID não indicarem que as prateleiras de expansão estão presentes, siga este procedimento.

Passos

1. Verifique se todos os cabos necessários foram firmemente conetados.
2. Verifique se você ativou as gavetas de expansão.
3. Se você precisar de ajuda para resolver um problema, entre em Contato com o suporte técnico.

Informações relacionadas

"SG6060: Cabeamento das gavetas de expansão opcionais"

"Conexão dos cabos de alimentação e alimentação de energia (SG6000)"

Reinicializando o controlador SG6000-CN enquanto o Instalador de dispositivos StorageGRID está em execução

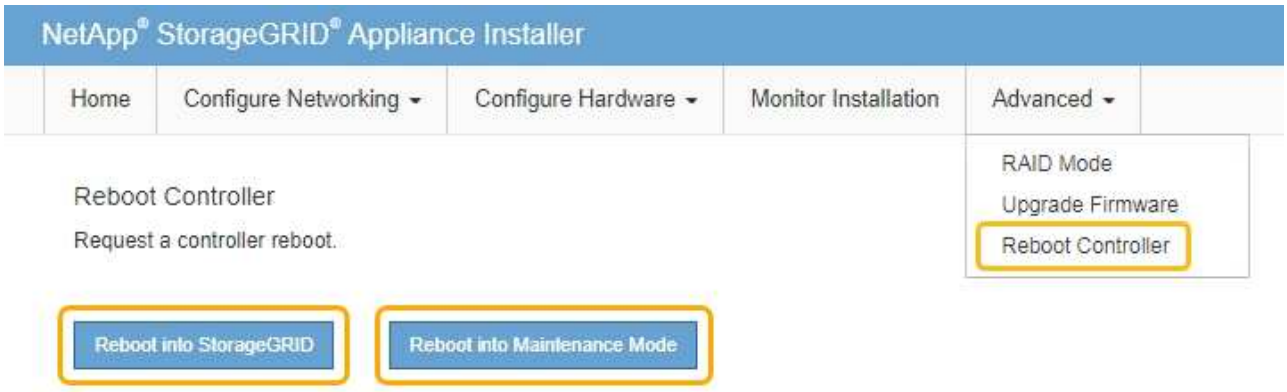
Talvez seja necessário reiniciar o controlador SG6000-CN enquanto o Instalador de dispositivos StorageGRID estiver em execução. Por exemplo, você pode precisar reiniciar o controlador se a instalação falhar.

Sobre esta tarefa

Este procedimento aplica-se apenas quando o controlador SG6000-CN está a executar o Instalador de aplicações StorageGRID. Depois que a instalação estiver concluída, esta etapa não funcionará mais porque o Instalador de dispositivos StorageGRID não está mais disponível.

Passos

1. No Instalador do StorageGRID Appliance, clique em **Avançado controlador de reinicialização** e selecione uma destas opções:
   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



O controlador SG6000-CN é reinicializado.

Manutenção do aparelho SG6000

Poderá ser necessário efetuar procedimentos de manutenção no aparelho SG6000. Os procedimentos nesta seção pressupõem que o dispositivo já foi implantado como nó de storage em um sistema StorageGRID.

Passos

- "Colocar um aparelho no modo de manutenção"
- "Atualizando o SANtricity os nas controladoras de storage"
- "Atualizando o firmware da unidade usando o Gerenciador de sistema do SANtricity"
- "Adição de um compartimento de expansão a um SG6060 implantado"
- "Ligar e desligar o LED de identificação do controlador"
- "Localizar o controlador em um data center"
- "Substituição de um controlador de armazenamento"
- "Substituição de componentes de hardware na gaveta do controlador de storage"
- "Substituição de componentes de hardware no compartimento de expansão de 60 unidades opcional"
- "Encerrar o controlador SG6000-CN"
- "Ligar o controlador SG6000-CN e verificar a operação"
- "Substituição do controlador SG6000-CN"
- "Substituição de uma fonte de alimentação no controlador SG6000-CN"
- "Remover o controlador SG6000-CN de um gabinete ou rack"
- "Reinstalar o controlador SG6000-CN em um gabinete ou rack"
- "Retirar a tampa do controlador SG6000-CN"
- "Voltar a instalar a tampa do controlador SG6000-CN"
- "Substituição do HBA Fibre Channel no controlador SG6000-CN"
- "Alterar a configuração do link do controlador SG6000-CN"

- "Alterar a definição MTU"
- "Verificar a configuração do servidor DNS"
- "Monitorização da encriptação do nó no modo de manutenção"

Colocar um aparelho no modo de manutenção

Deve colocar o aparelho no modo de manutenção antes de efetuar procedimentos de manutenção específicos.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

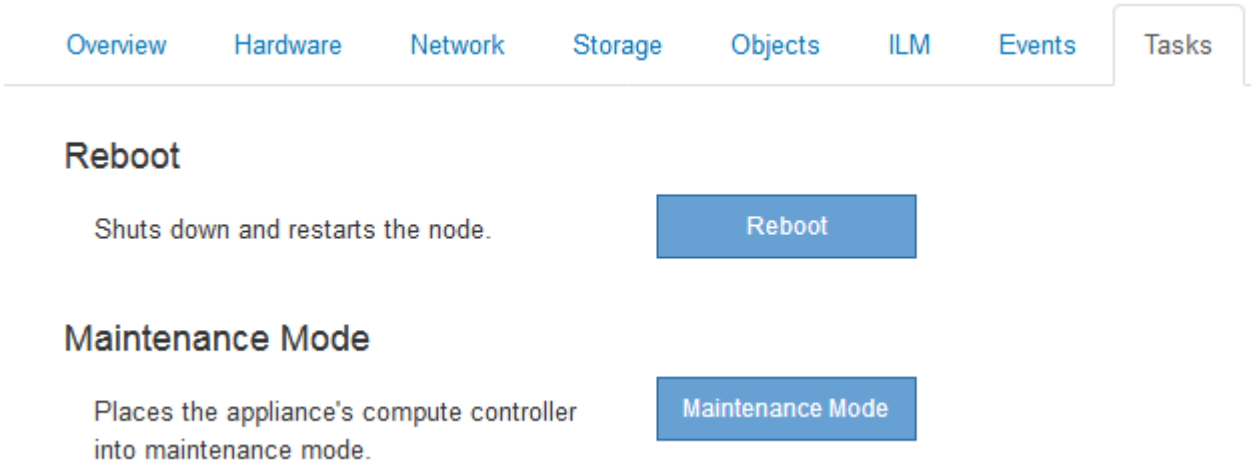
Sobre esta tarefa

Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

> A senha e a chave de host de um dispositivo StorageGRID no modo de manutenção permanecem as mesmas que eram quando o aparelho estava em serviço.

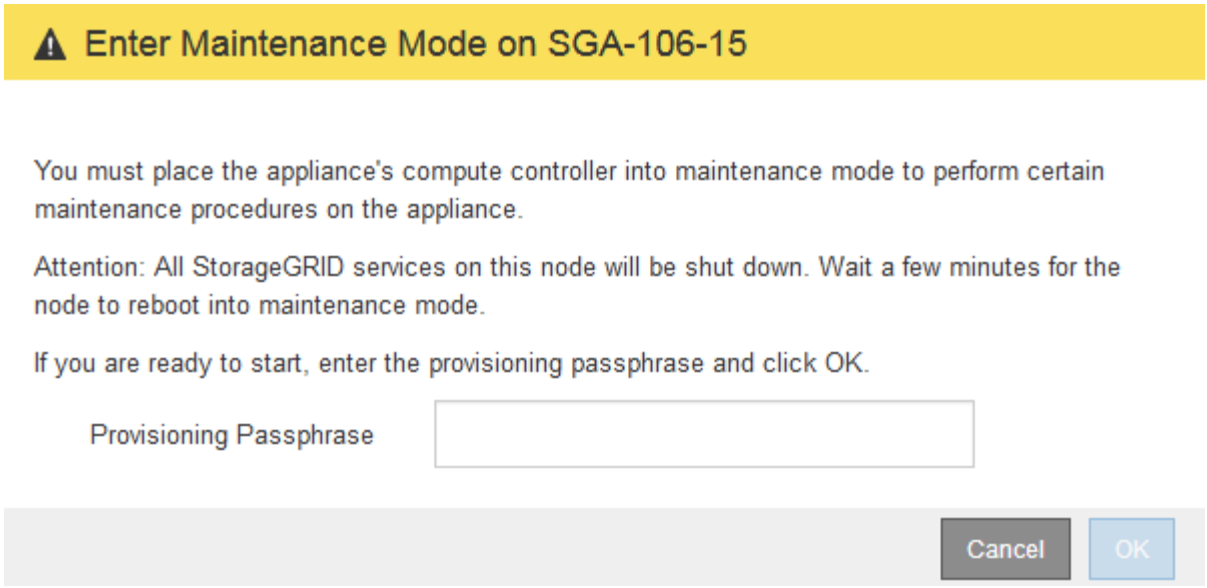
Passos

1. No Gerenciador de Grade, selecione **nós**.
2. Na exibição em árvore da página nós, selecione o nó de storage do dispositivo.
3. Selecione **tarefas**.



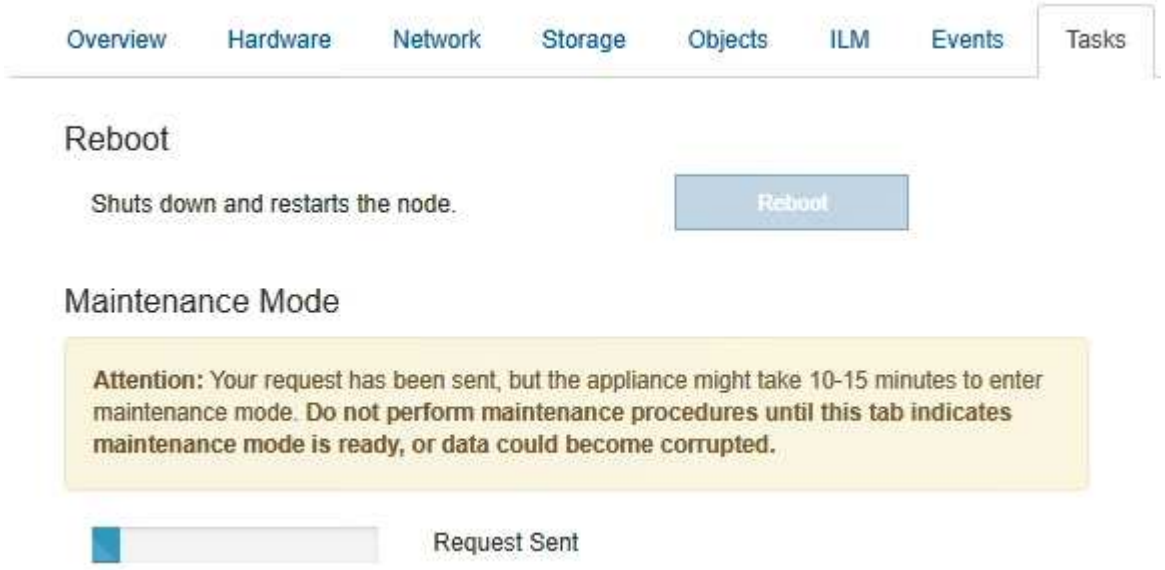
4. Selecione **Maintenance Mode** (modo de manutenção).

   É apresentada uma caixa de diálogo de confirmação.

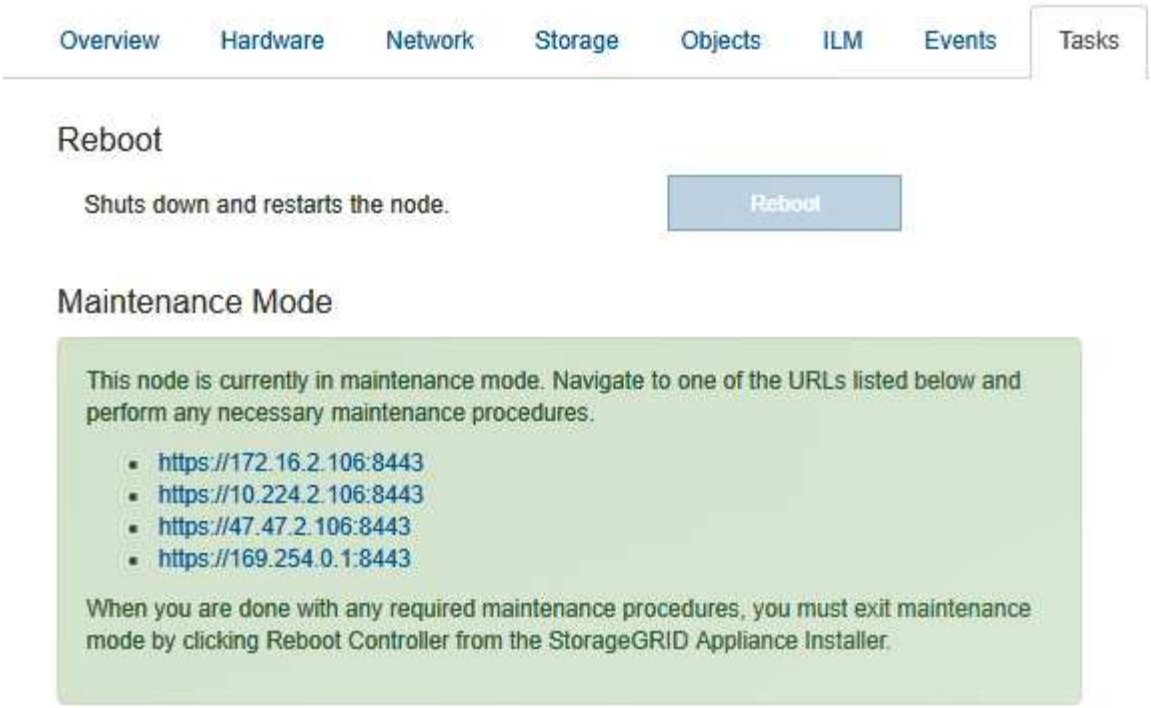


5. Introduza a frase-passe de aprovisionamento e selecione **OK**.

Uma barra de progresso e uma série de mensagens, incluindo "Request Sent" (pedido enviado), "Stop" (Paragem de StorageGRID) e "Reboot" (reinício), indicam que o aparelho está a concluir os passos para entrar no modo de manutenção.



Quando o dispositivo está no modo de manutenção, uma mensagem de confirmação lista os URLs que você pode usar para acessar o Instalador do StorageGRID Appliance.



6. Para acessar o Instalador do StorageGRID Appliance, navegue até qualquer um dos URLs exibidos.

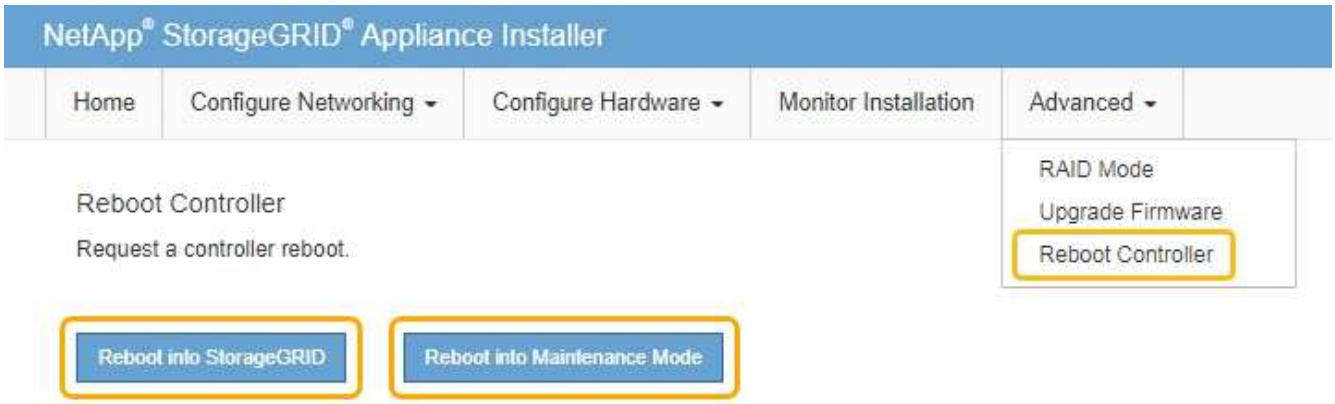
   Se possível, use o URL que contém o endereço IP da porta Admin Network do dispositivo.

   > O acesso `https://169.254.0.1:8443` requer uma conexão direta com a porta de gerenciamento local.

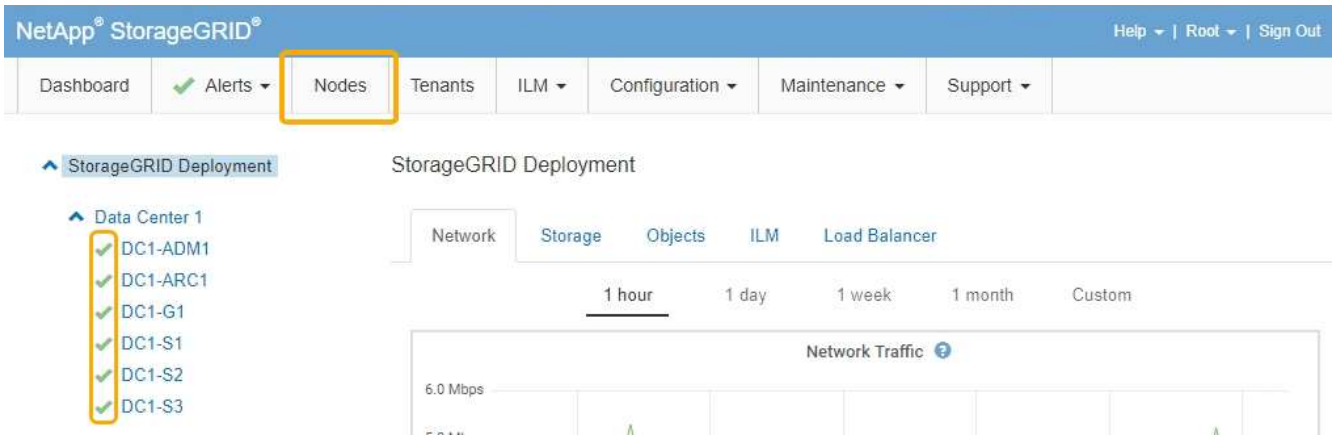
7. A partir do instalador do dispositivo StorageGRID, confirme se o aparelho está no modo de manutenção.

8. Execute todas as tarefas de manutenção necessárias.
9. Depois de concluir as tarefas de manutenção, saia do modo de manutenção e retome a operação normal do nó. No Instalador de dispositivos StorageGRID, selecione **Avançado controlador de reinicialização** e, em seguida, selecione **Reiniciar no StorageGRID**.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Atualizando o SANtricity os nas controladoras de storage

Para garantir o funcionamento ideal do controlador de storage, é necessário atualizar para a versão de manutenção mais recente do SANtricity os qualificado para o seu dispositivo StorageGRID. Consulte a ferramenta de Matriz de interoperabilidade do NetApp (IMT) para determinar qual versão você deve usar. Se você precisar de assistência, entre em Contato com o suporte técnico.

Use um dos seguintes procedimentos com base na versão do SANtricity os atualmente instalado:

- Se o controlador de armazenamento estiver usando o SANtricity os 08.42.20.00 (11,42) ou mais recente, use o Gerenciador de Grade para executar a atualização.

  "Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade"

- Se a controladora de storage estiver usando uma versão do SANtricity os anterior a 08.42.20.00 (11,42), use o modo de manutenção para executar a atualização.

  "Atualizando o SANtricity os nos controladores de storage usando o modo de manutenção"

Ao atualizar o SANtricity os para o seu dispositivo de armazenamento, você deve seguir as instruções na documentação do StorageGRID. Se utilizar quaisquer outras instruções, o aparelho pode ficar inoperável.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Downloads do NetApp: SANtricity os"

"Monitorizar Resolução de problemas"

Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade

Para controladores de storage que atualmente usam o SANtricity os 08.42.20.00 (11,42) ou mais recente, você deve usar o Gerenciador de Grade para aplicar uma atualização.

O que você vai precisar

- Você consultou a ferramenta de Matriz de interoperabilidade (IMT) do NetApp para confirmar que a versão do SANtricity os que você está usando para a atualização é compatível com o seu dispositivo.
- Tem de ter a permissão Manutenção.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a senha de provisionamento.
- Você deve ter acesso à página de downloads do NetApp para o SANtricity os.

Sobre esta tarefa

Não é possível executar outras atualizações de software (atualização de software StorageGRID ou hotfix) até concluir o processo de atualização do SANtricity os. Se você tentar iniciar um hotfix ou uma atualização de software StorageGRID antes do processo de atualização do SANtricity os terminar, você será redirecionado para a página de atualização do SANtricity os.

O procedimento não será concluído até que a atualização do SANtricity os tenha sido aplicada com êxito a todos os nós aplicáveis. Pode levar mais de 30 minutos para carregar o SANtricity os em cada nó e até 90 minutos para reinicializar cada dispositivo de storage StorageGRID.

As etapas a seguir são aplicáveis somente quando você estiver usando o Gerenciador de Grade para executar a atualização. Os controladores de armazenamento nos dispositivos da série SG6000 não podem ser atualizados usando o Gerenciador de Grade quando os controladores estão usando o SANtricity os mais antigo que 08.42.20.00 (11,42).

Este procedimento atualizará automaticamente a NVSRAM para a versão mais recente associada à atualização do sistema operacional SANtricity. Não é necessário aplicar um ficheiro de atualização NVSRAM separado.

Passos

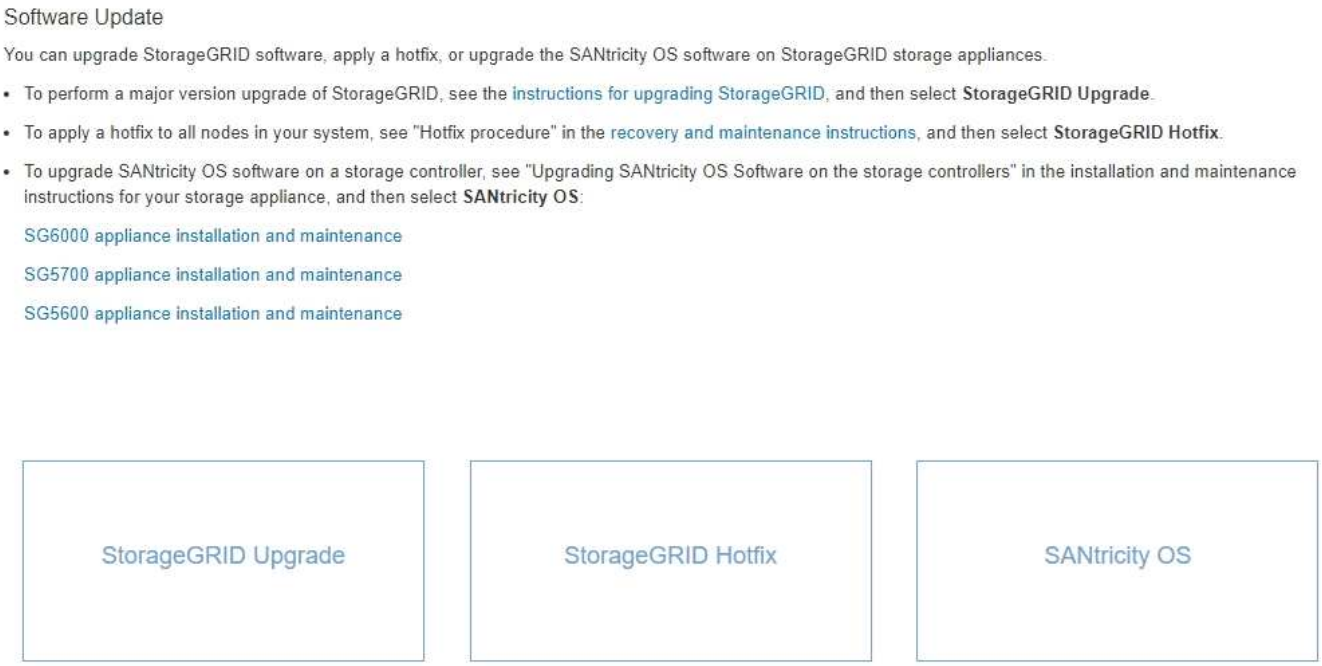
1. A partir de um portátil de serviço, transfira o novo ficheiro de software SANtricity os a partir do site de suporte da NetApp.

   Certifique-se de escolher a versão correta do SANtricity os para os controladores de armazenamento no seu dispositivo. O SG6060 usa o controlador E2800 e o SGF6024 usa o controlador EF570.

"Downloads do NetApp: SANtricity os"

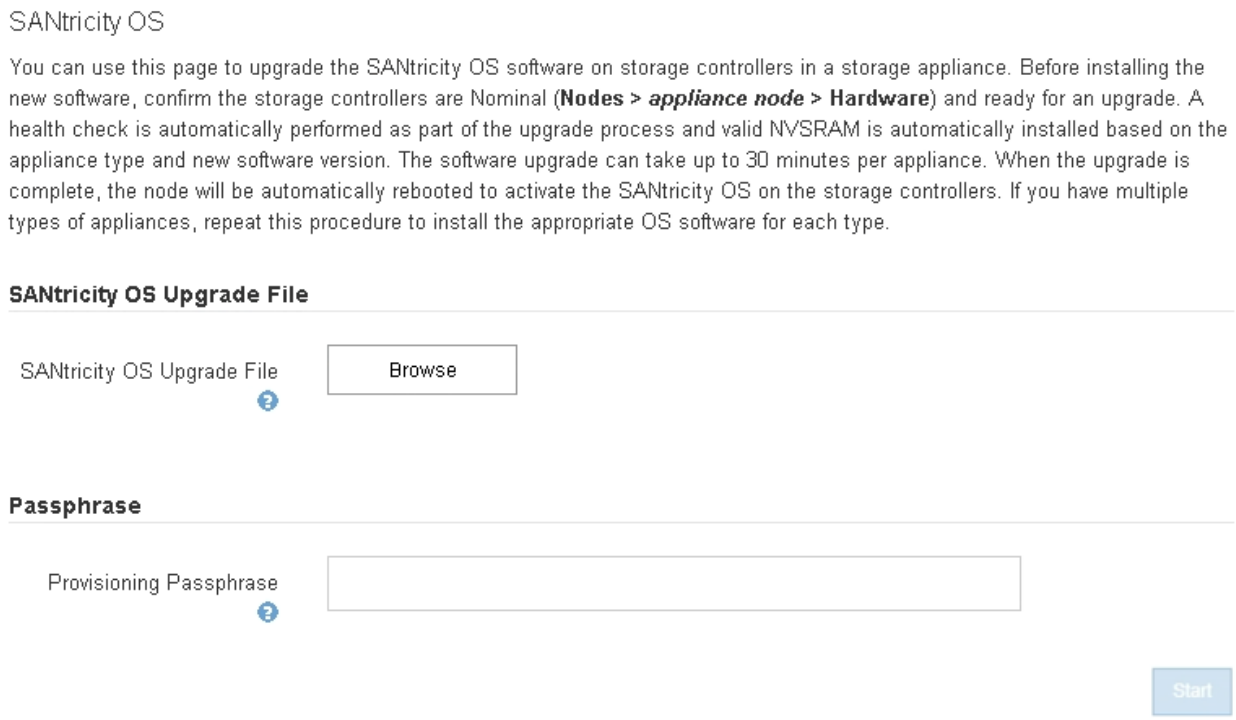
2. Faça login no Gerenciador de Grade usando um navegador compatível.
3. Selecione **Manutenção**. Em seguida, na seção sistema do menu, selecione **Atualização de software**.

   A página Atualização de software é exibida.



4. Clique em **SANtricity os**.

   A página do SANtricity os é exibida.



5. Selecione o arquivo de atualização do SANtricity os que você baixou no site de suporte do NetApp.

   a. Clique em **Procurar**.
   b. Localize e selecione o ficheiro.
   c. Clique em **abrir**.

   O arquivo é carregado e validado. Quando o processo de validação é concluído, o nome do arquivo é mostrado no campo Detalhes.

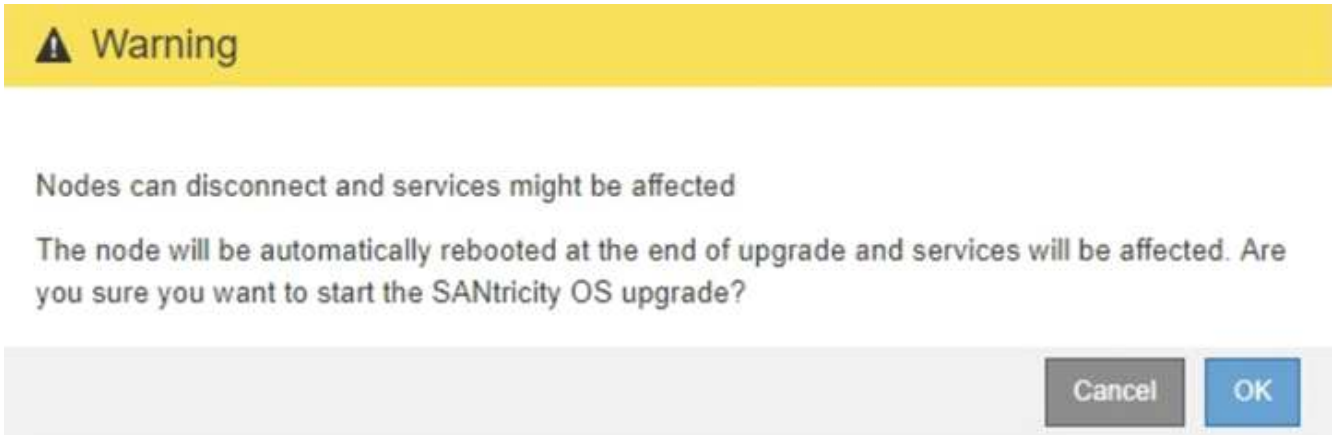
   Não altere o nome do arquivo, pois ele faz parte do processo de verificação.

6. Introduza a frase-passe de aprovisionamento.

   O botão **Start** está ativado.

7. Clique em **Iniciar**.

Uma caixa de aviso aparece informando que a conexão do seu navegador pode ser perdida temporariamente à medida que os serviços nos nós atualizados são reiniciados.



8. Clique em **OK** para colocar o arquivo de atualização do SANtricity os no nó de administração principal.

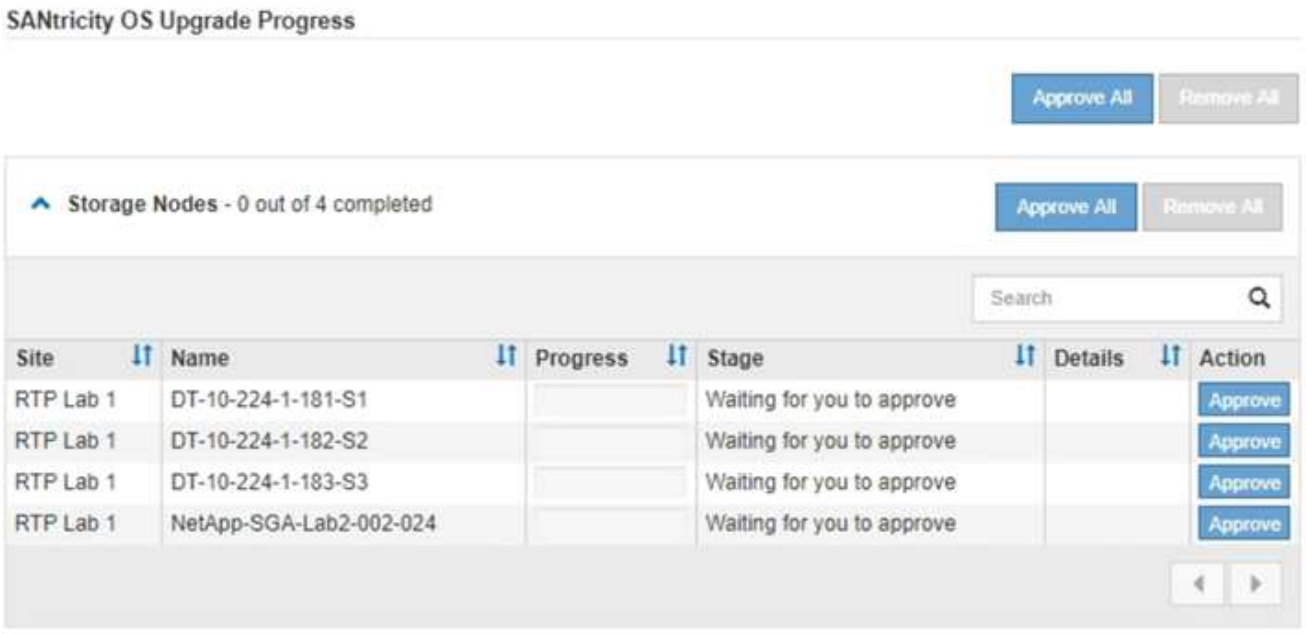
   Quando a atualização do SANtricity os é iniciada:

   a. A verificação de integridade é executada. Esse processo verifica se nenhum nó tem o status de precisa de atenção.

      Se algum erro for relatado, resolva-os e clique em **Start** novamente.

   b. A tabela de progresso da atualização do SANtricity os é exibida. Esta tabela mostra todos os nós de storage na grade e a etapa atual da atualização para cada nó.

      A tabela mostra todos os nós de storage, incluindo nós de storage baseados em software. Você precisa aprovar a atualização para todos os nós de storage, mesmo que uma atualização do SANtricity os não afete os nós de storage baseados em software. A mensagem de atualização retornada para nós de storage baseados em software é "a atualização do SANtricity os não se aplica a este nó."



9. Opcionalmente, classifique a lista de nós em ordem crescente ou decrescente por **Site**, **Nome**, **progresso**, **Estágio** ou **Detalhes**. Ou insira um termo na caixa **pesquisar** para pesquisar nós específicos.

   Você pode rolar pela lista de nós usando as setas esquerda e direita no canto inferior direito da seção.

10. Aprove os nós de grade que você está pronto para adicionar à fila de atualização. Nós aprovados do mesmo tipo são atualizados um de cada vez.

    > Não aprove a atualização do SANtricity os para um nó de armazenamento de dispositivo, a menos que você tenha certeza de que o nó está pronto para ser interrompido e reinicializado.quando a atualização do SANtricity os for aprovada em um nó, os serviços nesse nó são interrompidos. Mais tarde, quando o nó é atualizado, o nó do appliance é reinicializado. Essas operações podem causar interrupções de serviço para clientes que estão se comunicando com o nó.

    - Clique em um dos botões **Approve All** para adicionar todos os nós de armazenamento à fila de atualização do SANtricity os.

      > 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).

    - Clique em um ou mais botões **Approve** para adicionar um ou mais nós à fila de atualização do SANtricity os.

      > Você pode atrasar a aplicação de uma atualização do SANtricity os a um nó, mas o processo de atualização do SANtricity os não será concluído até que você aprove a atualização do SANtricity os em todos os nós de armazenamento listados.

      Depois de clicar em **Approve**, o processo de atualização determina se o nó pode ser atualizado. Se um nó puder ser atualizado, ele será adicionado à fila de atualização. E

      Para alguns nós, o arquivo de atualização selecionado não é aplicado intencionalmente e você pode concluir o processo de atualização sem atualizar esses nós específicos. Para nós intencionalmente não atualizados, o processo mostrará o estágio completo com uma das seguintes mensagens na coluna Detalhes:

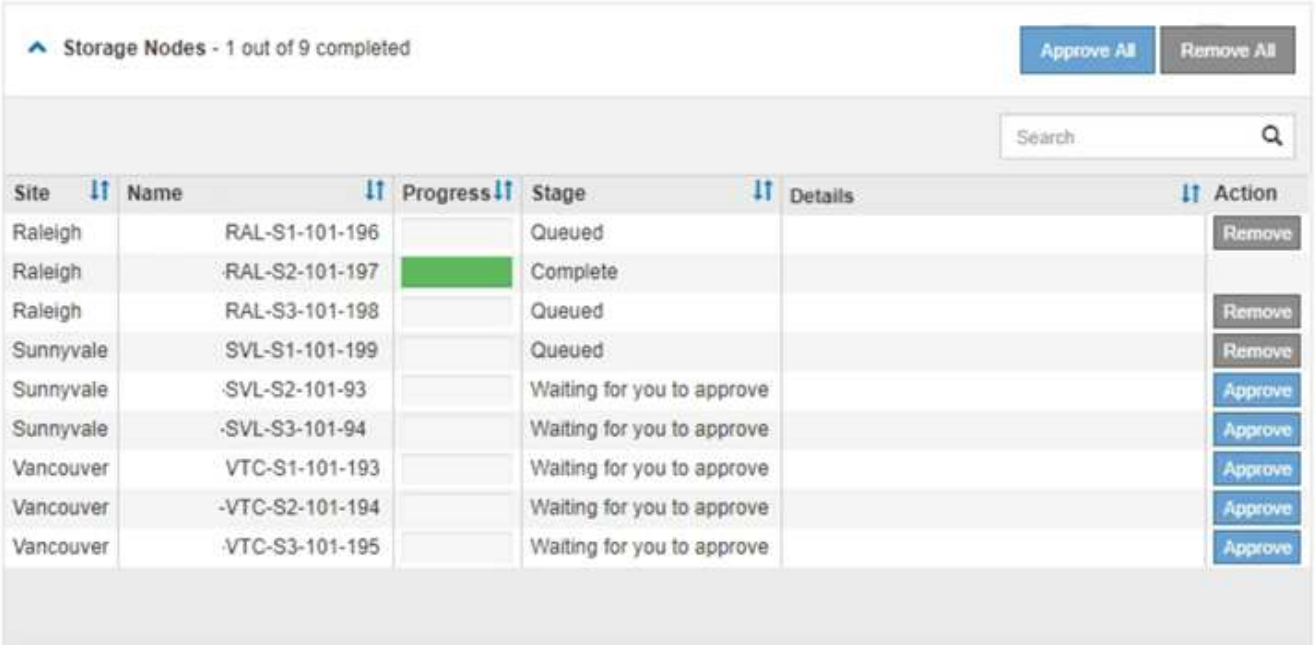
      - O nó de storage já foi atualizado.
      - A atualização do SANtricity os não é aplicável a este nó.
      - O ficheiro SANtricity os não é compatível com este nó.

    A mensagem "'SANtricity os upgrade não é aplicável a este nó'" indica que o nó não tem um controlador de armazenamento que pode ser gerenciado pelo sistema StorageGRID. Essa mensagem será exibida para nós de storage que não sejam do dispositivo. Você pode concluir o processo de atualização do SANtricity os sem atualizar o nó exibindo esta mensagem. A mensagem "'arquivo SANtricity os não é compatível com este nó'" indica que o nó requer um arquivo SANtricity os diferente daquele que o processo está tentando instalar. Depois de concluir a atualização atual do SANtricity os, baixe o SANtricity os apropriado para o nó e repita o processo de atualização.

11. Se você precisar remover um nó ou todos os nós da fila de atualização do SANtricity os, clique em **Remover** ou **Remover tudo**.

    Como mostrado no exemplo, quando o estágio avança além da fila, o botão **Remover** fica oculto e você

não pode mais remover o nó do processo de atualização do SANtricity os.



12. Aguarde enquanto a atualização do SANtricity os é aplicada a cada nó de grade aprovado.

> Se algum nó mostrar um estágio de erro enquanto a atualização do SANtricity os está sendo aplicada, a atualização falhou para esse nó. Pode ser necessário colocar o aparelho no modo de manutenção para recuperar da falha. Contacte o suporte técnico antes de continuar.

Se o firmware no nó é muito antigo para ser atualizado com o Gerenciador de Grade, o nó mostra um estágio de erro com os detalhes: "'você deve usar o modo de manutenção para atualizar o SANtricity os neste nó. Consulte as instruções de instalação e manutenção do seu aparelho. Após a atualização, você pode usar este utilitário para futuras atualizações." para resolver o erro, faça o seguinte:

a. Use o modo de manutenção para atualizar o SANtricity os no nó que mostra um estágio de erro.
b. Use o Gerenciador de Grade para reiniciar e concluir a atualização do SANtricity os.

   Quando a atualização do SANtricity os é concluída em todos os nós aprovados, a tabela de progresso da atualização do SANtricity os fecha e um banner verde mostra a data e a hora em que a atualização do SANtricity os foi concluída.

13. Repita este procedimento de atualização para todos os nós com um estágio de conclusão que exigem um

arquivo de atualização diferente do SANtricity os.

> Para todos os nós com um status de precisa de atenção, use o modo de manutenção para executar a atualização.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Atualizando o SANtricity os nos controladores de storage usando o modo de manutenção"

Atualizando o SANtricity os nos controladores de storage usando o modo de manutenção

Para controladores de storage que atualmente usam o SANtricity os com mais de 08.42.20.00 GB (11,42 GB), você deve usar o procedimento de modo de manutenção para aplicar uma atualização.

O que você vai precisar

- Você consultou a ferramenta de Matriz de interoperabilidade (IMT) do NetApp para confirmar que a versão do SANtricity os que você está usando para a atualização é compatível com o seu dispositivo.
- Se o aparelho StorageGRID estiver em execução em um sistema StorageGRID, o controlador SG6000-CN foi colocado no modo de manutenção.

  > O modo de manutenção interrompe a conexão com o controlador de storage.

  "Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Não atualize o SANtricity os ou a NVSRAM na controladora e-Series em mais de um dispositivo StorageGRID de cada vez.

> A atualização de mais de um dispositivo StorageGRID por vez pode causar indisponibilidade de dados, dependendo do modelo de implantação e das políticas de ILM.

Passos

1. A partir de um portátil de serviço, aceda ao Gestor de sistema SANtricity e inicie sessão.
2. Transfira o novo ficheiro de software SANtricity os e o ficheiro NVSRAM para o cliente de gestão.

   > A NVSRAM é específica do dispositivo StorageGRID. Não utilize a transferência NVSRAM padrão.

3. Siga as instruções no guia *Atualizando o SANtricity os* ou na ajuda on-line do Gerenciador de sistema do SANtricity para atualizar o firmware e a NVSRAM.

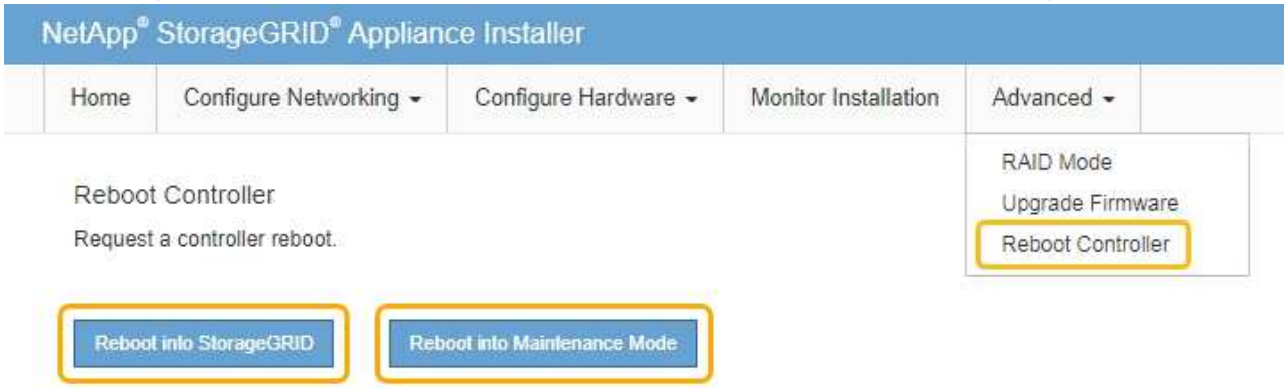
   > Ative os arquivos de atualização imediatamente. Não adiar a ativação.

4. Uma vez concluída a operação de atualização, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

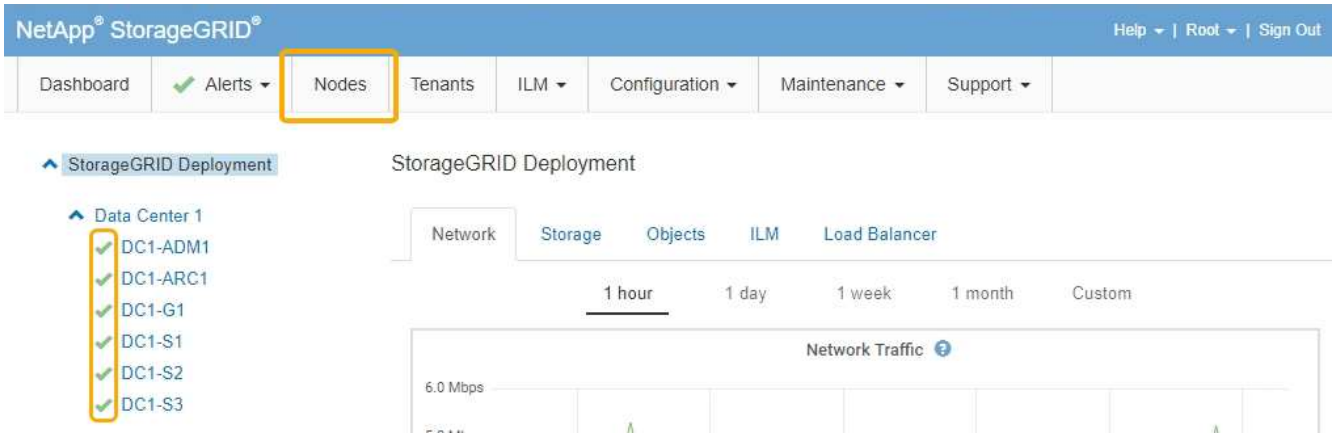
   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade.

Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.

- Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔ para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade"

Atualizando o firmware da unidade usando o Gerenciador de sistema do SANtricity

Você atualiza o firmware da sua unidade para garantir que você tenha todos os recursos mais recentes e correções de bugs.

O que você vai precisar

- O dispositivo de armazenamento tem um status ideal.
- Todas as unidades têm um status ideal.

- Você tem a versão mais recente do Gerenciador de sistema do SANtricity instalada que é compatível com sua versão do StorageGRID.
- Colocou o aparelho StorageGRID no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

> O modo de manutenção interrompe a conexão com o controlador de storage, interrompendo todas as atividades de e/S e colocando todas as unidades offline.

> Não atualize o firmware da unidade em mais de um dispositivo StorageGRID de cada vez. Isso pode causar indisponibilidade de dados, dependendo do modelo de implantação e das políticas de ILM.

Passos

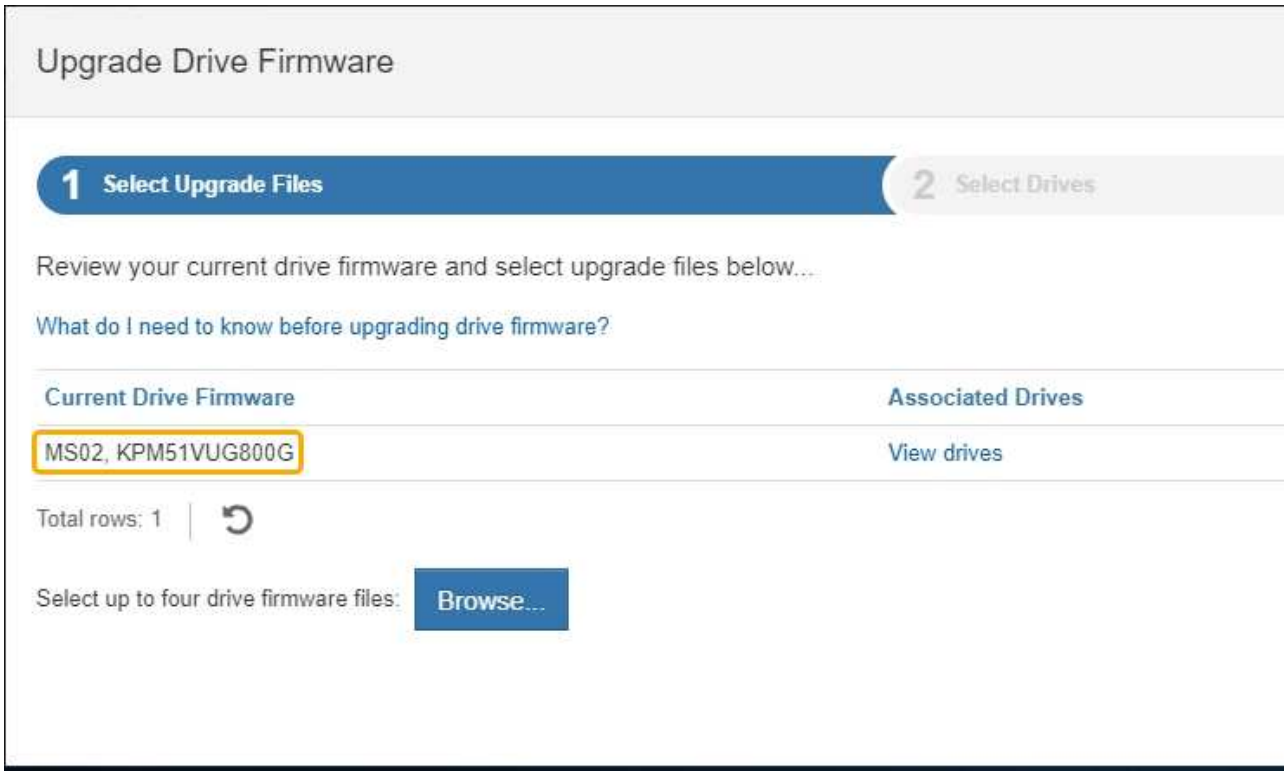
1. Acesse o Gerenciador de sistemas do SANtricity usando um destes métodos:
   - Use o Instalador do StorageGRID Appliance e selecione **Avançado Gerenciador do sistema SANtricity**
   - Use o Gerenciador de Grade e selecione **nós** * `***appliance Storage Node***`Gerenciador de sistema SANtricity*

> Se estas opções não estiverem disponíveis ou a página de início de sessão do Gestor do sistema SANtricity não for apresentada, aceda ao Gestor do sistema SANtricity navegando para o IP do controlador de armazenamento
> `https://Storage_Controller_IP`

2. Introduza o nome de utilizador e a palavra-passe do administrador do Gestor do sistema SANtricity, se necessário.
3. Verifique a versão do firmware da unidade atualmente instalada no dispositivo de armazenamento:
   a. No Gerenciador do sistema SANtricity, selecione **suporte Centro de Atualização**.
   b. Em Drive firmware upgrade, selecione **Begin Upgrade** (Iniciar atualização).

      O firmware da unidade de atualização exibe os arquivos de firmware da unidade atualmente instalados.

   c. Observe as revisões atuais do firmware da unidade e os identificadores da unidade na coluna firmware da unidade atual.



Neste exemplo:

- A revisão do firmware da unidade é **MS02**.
- O identificador da unidade é **KPM51VUG800G**.

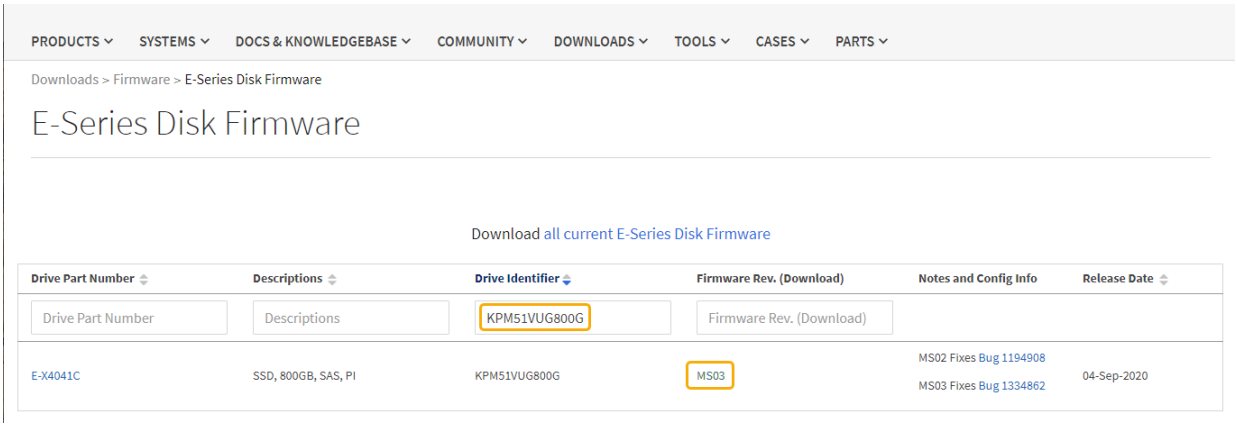
Selecione **Exibir unidades** na coluna unidades associadas para exibir onde essas unidades estão instaladas no seu dispositivo de armazenamento.

a. Feche a janela Upgrade Drive firmware (Atualizar firmware da unidade).

4. Transfira e prepare a atualização de firmware da unidade disponível:
   a. Em Atualização do firmware da unidade, selecione **suporte NetApp**.
   b. No site de suporte da NetApp, selecione a guia **Downloads** e, em seguida, selecione **firmware da unidade de disco da série e**.

      É apresentada a página firmware do disco e-Series.

   c. Procure cada **Drive Identifier** instalado no seu dispositivo de armazenamento e verifique se cada identificador de unidade tem a revisão de firmware mais recente.
      - Se a revisão do firmware não for um link, esse identificador de unidade terá a revisão de firmware mais recente.
      - Se um ou mais números de peça de unidade forem listados para um identificador de unidade, uma atualização de firmware estará disponível para essas unidades. Pode selecionar qualquer ligação para transferir o ficheiro de firmware.



d. Se estiver listada uma revisão de firmware posterior, selecione o link na coluna firmware Rev. (Download) para baixar um `.zip` arquivo contendo o arquivo de firmware.

e. Extraia (descompacte) os arquivos de arquivo de firmware da unidade que você baixou do site de suporte.

5. Instale a atualização do firmware da unidade:

a. No Gerenciador de sistema do SANtricity, em Atualização do firmware da unidade, selecione **Begin Upgrade**.

b. Selecione **Procurar** e selecione os novos arquivos de firmware da unidade que você baixou no site de suporte.

Os arquivos de firmware da unidade têm um nome de arquivo semelhante ao `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`.

Você pode selecionar até quatro arquivos de firmware da unidade, um de cada vez. Se mais de um arquivo de firmware de unidade for compatível com a mesma unidade, você receberá um erro de conflito de arquivo. Decida qual arquivo de firmware da unidade você deseja usar para a atualização e remova o outro.

c. Selecione **seguinte**.

Selecionar unidades lista as unidades que você pode atualizar com os arquivos de firmware selecionados.

Apenas as unidades compatíveis aparecem.

O firmware selecionado para a unidade aparece em **firmware proposto**. Se tiver de alterar este firmware, selecione **voltar**.

d. Selecione **Offline (paralelo)** upgrade.

Você pode usar o método de atualização off-line porque o dispositivo está no modo de manutenção, onde a atividade de e/S é interrompida para todas as unidades e todos os volumes.

e. Na primeira coluna da tabela, selecione a unidade ou unidades que deseja atualizar.

A prática recomendada é atualizar todas as unidades do mesmo modelo para a mesma revisão de firmware.

f. Selecione **Iniciar** e confirme que deseja executar a atualização.

Se você precisar parar a atualização, selecione **Stop**. Todas as transferências de firmware atualmente em curso são concluídas. Quaisquer downloads de firmware que não tenham sido iniciados são cancelados.

> Parar a atualização do firmware da unidade pode resultar em perda de dados ou unidades indisponíveis.

g. (Opcional) para ver uma lista do que foi atualizado, selecione **Save Log**.

O arquivo de log é salvo na pasta de downloads do navegador com o `latest-upgrade-log-timestamp.txt` nome .

Se ocorrer algum dos seguintes erros durante o procedimento de atualização, tome a ação recomendada apropriada.

- **Unidades atribuídas com falha**

  Um motivo para a falha pode ser que a unidade não tenha a assinatura apropriada. Certifique-se de que a unidade afetada é uma unidade autorizada. Entre em Contato com o suporte técnico para obter mais informações.

Ao substituir uma unidade, certifique-se de que a unidade de substituição tem uma capacidade igual ou superior à unidade com falha que está a substituir.

Você pode substituir a unidade com falha enquanto a matriz de armazenamento está recebendo e/S

- **Verifique a matriz de armazenamento**
  - Certifique-se de que foi atribuído um endereço IP a cada controlador.
  - Certifique-se de que todos os cabos ligados ao controlador não estão danificados.
  - Certifique-se de que todos os cabos estão bem ligados.
- **Unidades hot spare integradas**

  Esta condição de erro tem de ser corrigida antes de poder atualizar o firmware.

- **Grupos de volumes incompletos**

  Se um ou mais grupos de volumes ou pools de discos estiverem incompletos, você deverá corrigir essa condição de erro antes de atualizar o firmware.

- * Operações exclusivas (exceto Mídia em segundo plano/varredura de paridade) atualmente em execução em qualquer grupo de volume*

  Se uma ou mais operações exclusivas estiverem em andamento, as operações devem ser concluídas antes que o firmware possa ser atualizado. Use o System Manager para monitorar o andamento das operações.

- **Volumes em falta**

  Você deve corrigir a condição de volume ausente antes que o firmware possa ser atualizado.

- * Qualquer controlador em um estado diferente do ideal*

  Um dos controladores de storage array precisa de atenção. Esta condição deve ser corrigida antes

que o firmware possa ser atualizado.

- **Informações de partição de armazenamento incompatíveis entre gráficos de objetos do controlador**

  Ocorreu um erro ao validar os dados nos controladores. Contacte o suporte técnico para resolver este problema.

- **SPM verificar falha na verificação do controlador de banco de dados**

  Ocorreu um erro de banco de dados de mapeamento de partições de armazenamento em um controlador. Contacte o suporte técnico para resolver este problema.

- **Validação da base de dados de configuração (se suportada pela versão do controlador da matriz de armazenamento)**

  Ocorreu um erro de banco de dados de configuração em um controlador. Contacte o suporte técnico para resolver este problema.

- **Verificações relacionadas ao mel**

  Contacte o suporte técnico para resolver este problema.

- **Mais de 10 eventos informativos ou críticos de mel foram relatados nos últimos 7 dias**

  Contacte o suporte técnico para resolver este problema.

- **Mais de 2 Página 2C Eventos críticos de mel foram relatados nos últimos 7 dias**

  Contacte o suporte técnico para resolver este problema.

- **Mais de 2 eventos de mel críticos de canal de unidade degradada foram relatados nos últimos 7 dias**

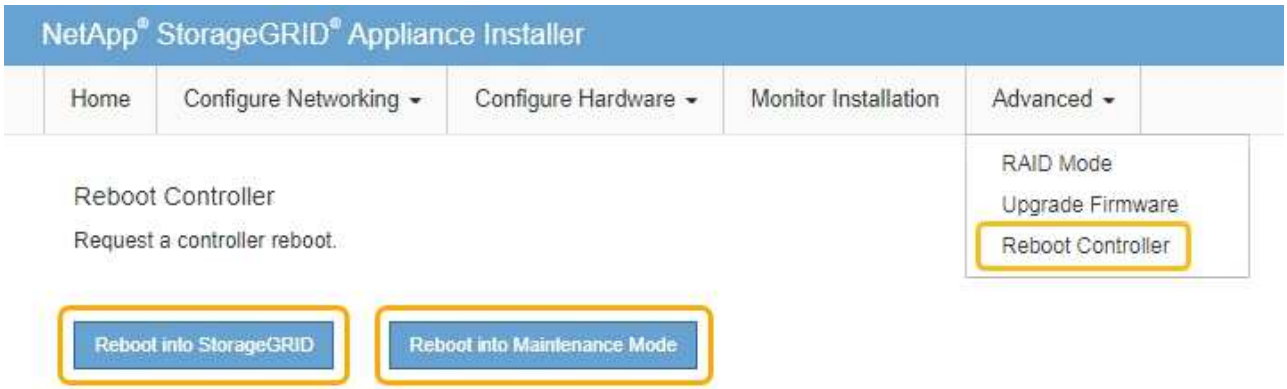
  Contacte o suporte técnico para resolver este problema.

- **Mais de 4 entradas críticas de mel nos últimos 7 dias**

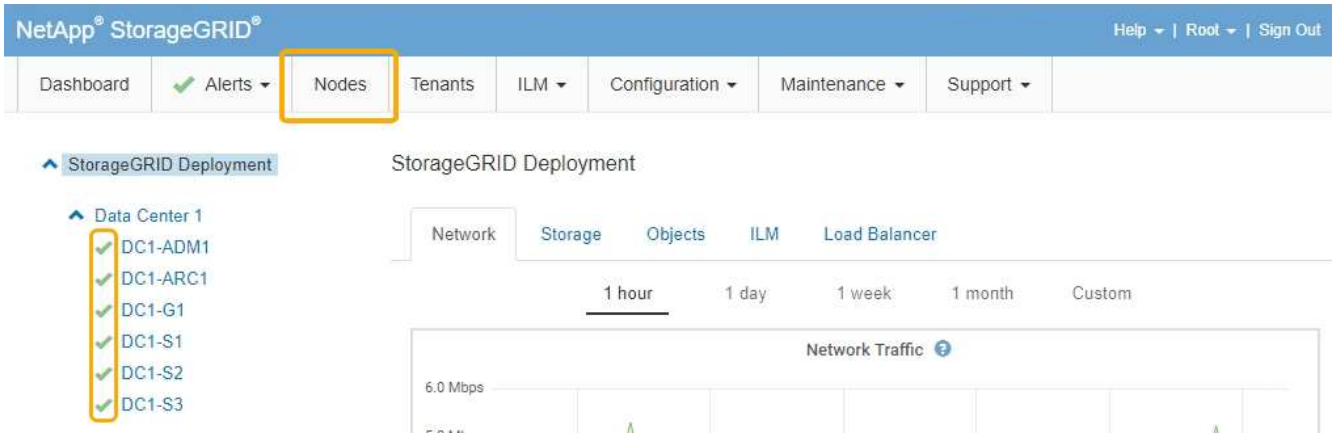
  Contacte o suporte técnico para resolver este problema.

6. Quando a operação de atualização estiver concluída, reinicie o aparelho. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Atualizando o SANtricity os nas controladoras de storage"

Adição de um compartimento de expansão a um SG6060 implantado

Para aumentar a capacidade de storage, é possível adicionar uma ou duas gavetas de expansão a um SG6060 implantado em sistema StorageGRID.

O que você vai precisar

- Você deve ter a senha de provisionamento.
- Você deve estar executando o StorageGRID 11,4 ou posterior.
- Você tem o compartimento de expansão e dois cabos SAS para cada compartimento de expansão.
- Você localizou fisicamente o dispositivo de armazenamento onde está adicionando o compartimento de expansão no data center.

  "Localizar o controlador em um data center"

Sobre esta tarefa

Para adicionar um compartimento de expansão, execute estas etapas de alto nível:

- Instale o hardware no gabinete ou rack.
- Coloque o SG6060 no modo de manutenção.
- Conete o compartimento de expansão ao compartimento de controladora E2860 ou a outro compartimento de expansão.
- Inicie a expansão usando o Instalador de dispositivos StorageGRID
- Aguarde até que os novos volumes estejam configurados.

A conclusão do procedimento para um ou dois compartimentos de expansão deve levar uma hora ou menos por nó do dispositivo. Para minimizar o tempo de inatividade, as etapas a seguir instruem você a instalar os novos compartimentos de expansão e unidades antes de colocar o SG6060 no modo de manutenção. As etapas restantes devem levar aproximadamente 20 a 30 minutos por nó do dispositivo.

Passos

1. Siga as instruções para instalar gavetas de 60 unidades em um gabinete ou rack.

   "SG6060: Instalação de compartimentos de 60 unidades em um gabinete ou rack"

2. Siga as instruções para instalar as unidades.

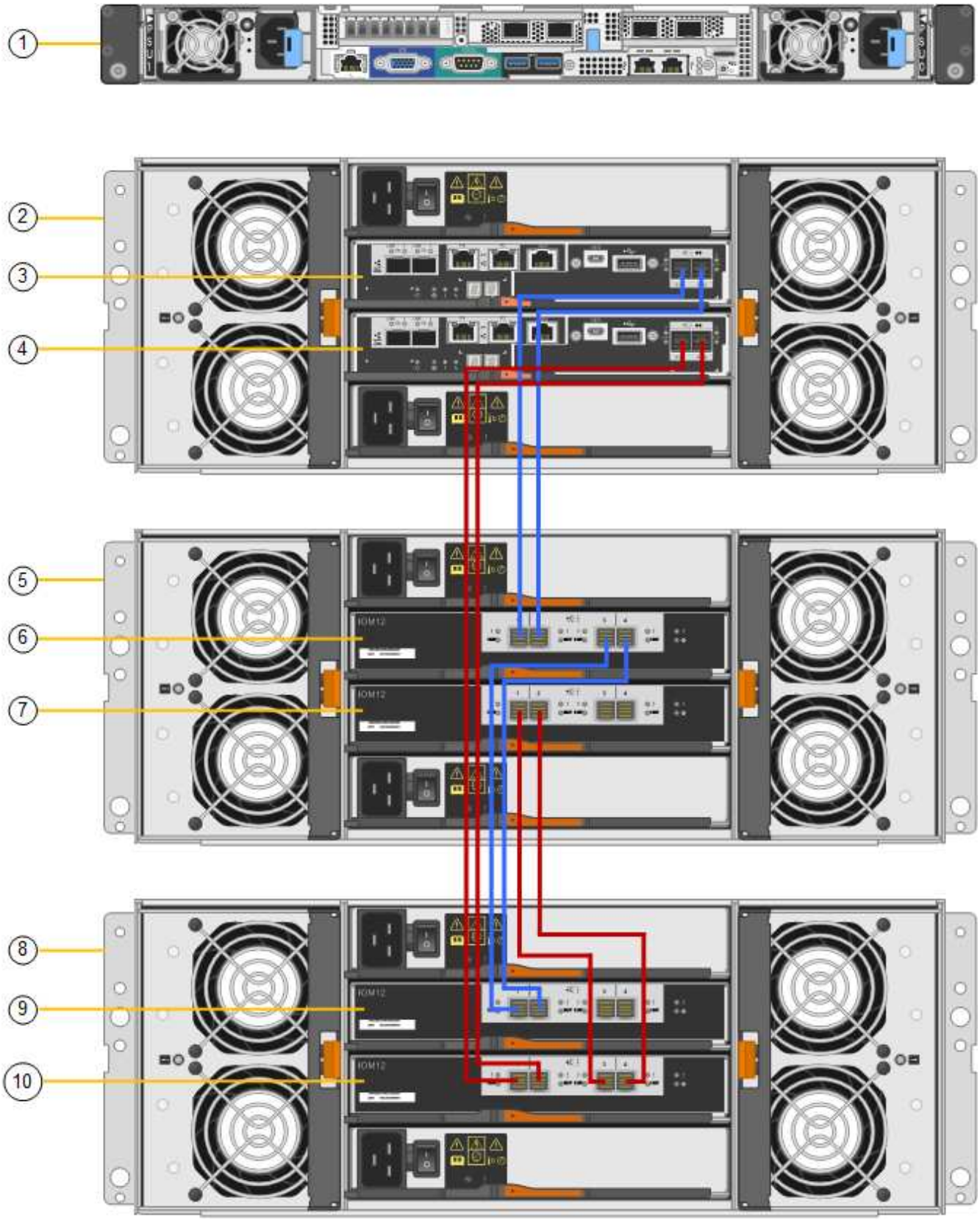
   "SG6060: Instalar as unidades"

3. No Grid Manager, coloque o controlador SG6000-CN no modo de manutenção.

   "Colocar um aparelho no modo de manutenção"

4. Conete cada compartimento de expansão ao compartimento de controladora E2860, conforme mostrado no diagrama.

   Este desenho mostra duas prateleiras de expansão. Se tiver apenas uma, ligue a IOM A ao controlador A e ligue a IOM B ao controlador B.



	Descrição
1	SG6000-CN

	Descrição
2	Compartimento do controlador de E2860 TB
3	Controlador A
4	Controlador B
5	Compartimento de expansão 1
6	IOM A para compartimento de expansão 1
7	IOM B para compartimento de expansão 1
8	Compartimento de expansão 2
9	IOM A para compartimento de expansão 2
10	IOM B para compartimento de expansão 2

5. Conecte os cabos de energia e aplique energia às gavetas de expansão.
   a. Conete um cabo de alimentação a cada uma das duas unidades de fonte de alimentação em cada compartimento de expansão.
   b. Conete os dois cabos de alimentação em cada compartimento de expansão a duas PDUs diferentes no gabinete ou no rack.
   c. Ligue os dois interruptores de energia para cada compartimento de expansão.
      - Não desligue os interrutores de alimentação durante o processo de ativação.
      - Os ventiladores nas prateleiras de expansão podem ser muito altos quando eles começam a funcionar. O ruído alto durante o arranque é normal.
6. Monitore a página inicial do instalador do dispositivo StorageGRID.

   Em aproximadamente cinco minutos, as prateleiras de expansão terminam de ligar e são detetadas pelo sistema. A página inicial mostra o número de novas prateleiras de expansão detetadas e o botão Iniciar expansão está ativado.

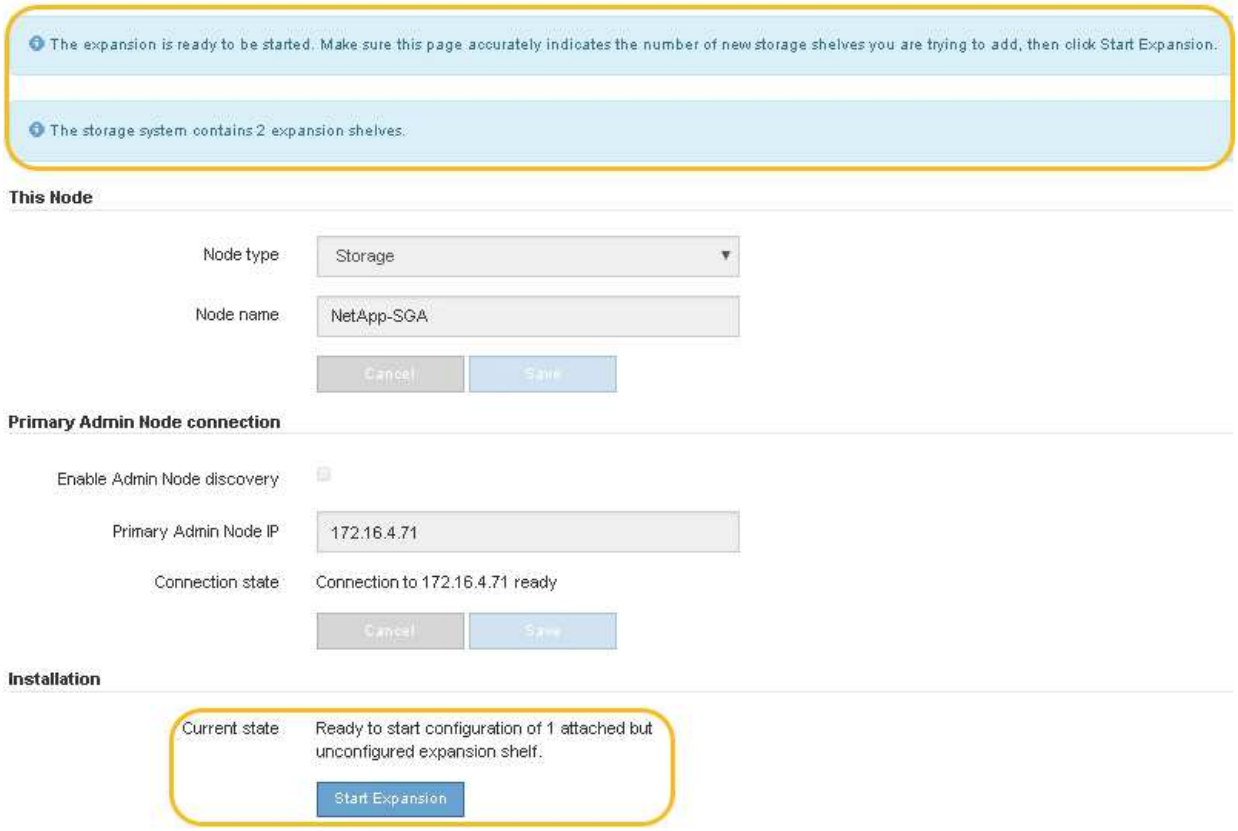
   A captura de tela mostra exemplos das mensagens que podem aparecer na página inicial, dependendo do número de prateleiras de expansão existentes ou novas, como segue:

   - O banner circulado na parte superior da página indica o número total de prateleiras de expansão detetadas.
     - O banner indica o número total de compartimentos de expansão, quer as prateleiras estejam configuradas e implantadas ou novas e não configuradas.
     - Se não forem detetadas prateleiras de expansão, o banner não aparecerá.
   - A mensagem circulada na parte inferior da página indica que uma expansão está pronta para ser iniciada.
     - A mensagem indica o número de novos compartimentos de expansão detetados pelo

StorageGRID. "Anexo" indica que a prateleira foi detetada. "'unconfigured'" indica que o shelf é novo e ainda não está configurado usando o Instalador de dispositivos StorageGRID.

> Os compartimentos de expansão que já estão implantados não estão incluídos nesta mensagem. Eles estão incluídos na contagem no banner no topo da página.

- A mensagem não aparecerá se novos compartimentos de expansão não forem detetados.



7. Conforme necessário, resolva quaisquer problemas descritos nas mensagens da página inicial.

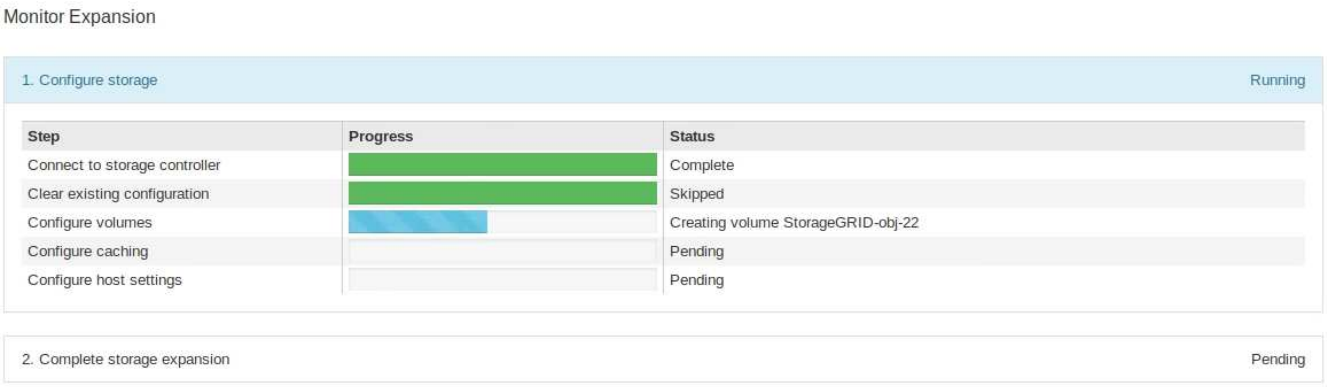
   Por exemplo, use o Gerenciador de sistema do SANtricity para resolver quaisquer problemas de hardware de armazenamento.

8. Verifique se o número de prateleiras de expansão exibidas na página inicial corresponde ao número de prateleiras de expansão que você está adicionando.

   > Se os novos compartimentos de expansão não tiverem sido detetados, verifique se eles estão cabeados e ligados corretamente.

9. Clique em **Start Expansion** (Iniciar expansão) para configurar as prateleiras de expansão e disponibilizá-las para armazenamento de objetos.
10. Monitorar o andamento da configuração do compartimento de expansão.

    As barras de progresso aparecem na página da Web, tal como fazem durante a instalação inicial.



Quando a configuração estiver concluída, o aparelho reinicializa automaticamente para sair do modo de manutenção e voltar a ligar a grelha. Este processo pode demorar até 20 minutos.

> Se o aparelho não se juntar novamente à grade, vá para a página inicial do Instalador de dispositivos StorageGRID, selecione **Avançado Reiniciar controlador** e, em seguida, selecione **Reiniciar no modo de manutenção**.

Quando a reinicialização estiver concluída, a guia **Tasks** parece com a seguinte captura de tela:

11. Verifique o status do nó de storage do dispositivo e dos novos compartimentos de expansão.
    a. No Gerenciador de Grade, selecione **nós** e verifique se o nó de armazenamento do dispositivo tem um ícone de marca de seleção verde.

       O ícone verde da marca de seleção significa que não há alertas ativos e o nó está conetado à grade. Para obter uma descrição dos ícones de nós, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

    b. Selecione a guia **armazenamento** e confirme se 16 novos armazenamentos de objetos são exibidos na tabela armazenamento de objetos para cada compartimento de expansão adicionado.
    c. Verifique se cada novo compartimento de expansão tem um status de compartimento nominal e um status de configuração de configurado.

Storage Shelves

Shelf Chassis Serial Number	Shelf ID	Shelf Status	IOM Status	Power Supply Status	Drawer Status	Fan Status	Drive Slots	Data Drives	Data Drive Size	Cache Drives	Cache Drive Size	Configuration Status
721924500063	99	Nominal	N/A	Nominal	Nominal	Nominal	60	58	9.80 TB	2	800.17 GB	Configured (in use)
721929500038	0	Nominal	Nominal	Nominal	Nominal	Nominal	60	60	9.80 TB	0	0 bytes	Configured (in use)
721929500039	1	Nominal	Nominal	Nominal	Nominal	Nominal	60	60	9.80 TB	0	0 bytes	Configured (in use)

Informações relacionadas

"Desembalar as caixas (SG6000)"

"SG6060: Instalação de compartimentos de 60 unidades em um gabinete ou rack"

"SG6060: Instalar as unidades"

"Monitorizar Resolução de problemas"

Ligar e desligar o LED de identificação do controlador

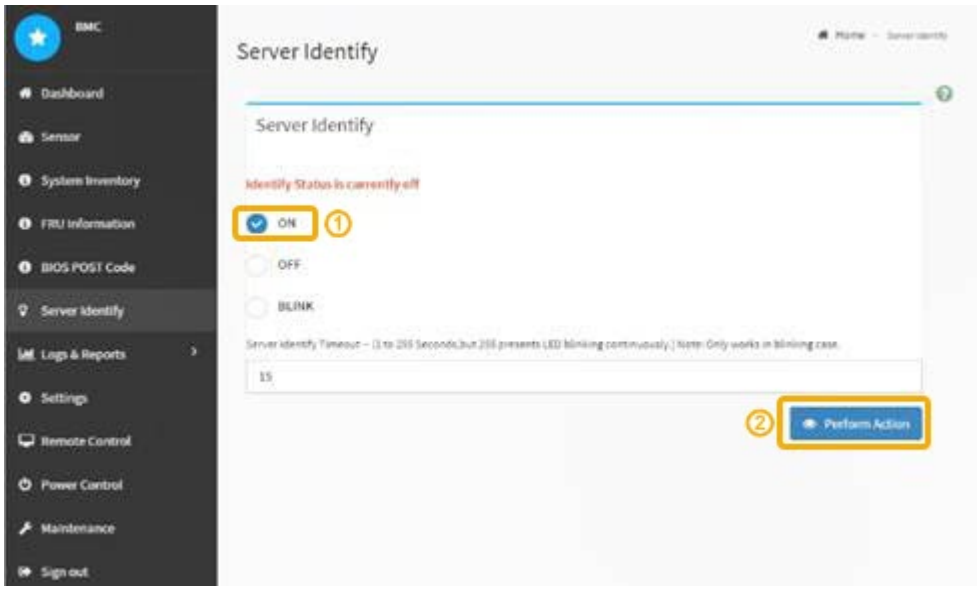
O LED de identificação azul na parte frontal e traseira do controlador pode ser ligado para ajudar a localizar o aparelho em um data center.

O que você vai precisar

Tem de ter o endereço IP BMC do controlador que pretende identificar.

Passos

1. Acesse a interface BMC do controlador.
2. Selecione **identificação do servidor**.
3. Selecione **ON** e, em seguida, selecione **Perform Action**.



Resultado

Os LEDs de identificação azul acendem-se na parte frontal (mostrada) e traseira do controlador.

Se um painel frontal estiver instalado no controlador, pode ser difícil ver o LED de identificação frontal.

Depois de terminar

Para desligar o LED de identificação do controlador:

- Pressione o interrutor Identify LED no painel frontal do controlador.
- Na interface BMC do controlador, selecione **identificação do servidor**, selecione **OFF** e, em seguida, selecione **Perform Action**.

Os LEDs de identificação azul na parte frontal e traseira do controlador apagam-se.

Informações relacionadas

"Verificar a substituição do HBA Fibre Channel"

"Localizar o controlador em um data center"

"Acessando a interface BMC"

Localizar o controlador em um data center

Localize o controlador para que você possa executar a manutenção ou atualizações de hardware.

O que você vai precisar

- Você determinou qual controlador requer manutenção.

(Opcional) para ajudar a localizar o controlador no seu data center, ligue o LED de identificação azul.

"Ligar e desligar o LED de identificação do controlador"

Passos

1. Encontre o controlador que precisa de manutenção no data center.
   - Procure um LED de identificação azul aceso na parte frontal ou traseira do controlador.

     O LED de identificação frontal está atrás do painel frontal do controlador e pode ser difícil ver se o painel frontal está instalado.

   - Verifique se há um número de peça correspondente nas etiquetas anexadas à frente de cada controlador.
2. Remova o painel frontal do controlador, se estiver instalado, para acessar os controles e indicadores do painel frontal.
3. Opcional: Desligue o LED de identificação azul se o tiver utilizado para localizar o controlador.
   - Pressione o interrutor Identify LED no painel frontal do controlador.
   - Use a interface BMC do controlador.

     "Ligar e desligar o LED de identificação do controlador"

Informações relacionadas

"Remover o HBA Fibre Channel"

"Remover o controlador SG6000-CN de um gabinete ou rack"

"Encerrar o controlador SG6000-CN"

Substituição de um controlador de armazenamento

Pode ser necessário substituir um controlador E2800 ou um controlador EF570 se não estiver a funcionar de forma ideal ou se tiver falhado.

O que você vai precisar

- Você tem um controlador de substituição com o mesmo número de peça do controlador que está substituindo.

- Você tem etiquetas para identificar cada cabo conetado ao controlador.
- Você tem uma pulseira antiestática ou tomou outras precauções antiestáticas.
- Você tem uma chave de fenda Phillips nº 1.
- Você tem as instruções e-Series para substituir um controlador na configuração duplex.

> Consulte as instruções da Série e apenas quando for direcionado ou se precisar de mais detalhes para executar uma etapa específica. Não confie nas instruções do e-Series para substituir um controlador no dispositivo StorageGRID, porque os procedimentos não são os mesmos.

- Você localizou fisicamente o dispositivo de armazenamento onde está substituindo o controlador no data center.

  "Localizar o controlador em um data center"

Sobre esta tarefa

Você pode determinar se você tem um controlador com falha de duas maneiras:

- O Guru de recuperação no Gerenciador de sistema do SANtricity direciona você para substituir o controlador.
- O LED âmbar de atenção no controlador está aceso, indicando que o controlador tem uma avaria.

> Se ambos os controladores na gaveta tiverem seus LEDs de atenção ligados, entre em Contato com o suporte técnico para obter assistência.

Como o compartimento da controladora de storage contém duas controladoras de storage, você pode substituir uma delas enquanto o dispositivo está ligado e executa operações de leitura/gravação, contanto que as condições a seguir sejam verdadeiras:

- O segundo controlador na gaveta tem o status ideal.
- O campo "OK para remover" na área Detalhes do Guru de recuperação no Gerenciador de sistemas do SANtricity exibe Sim, indicando que é seguro remover esse componente.

> Se o segundo recipiente do controlador na gaveta não tiver o status ideal ou se o Recovery Guru indicar que não é bom remover o recipiente do controlador, entre em Contato com o suporte técnico.

Quando substituir um controlador, tem de remover a bateria do controlador original e instalá-la no controlador de substituição.

> Os controladores de storage no dispositivo não incluem placas de interface de host (HIC).

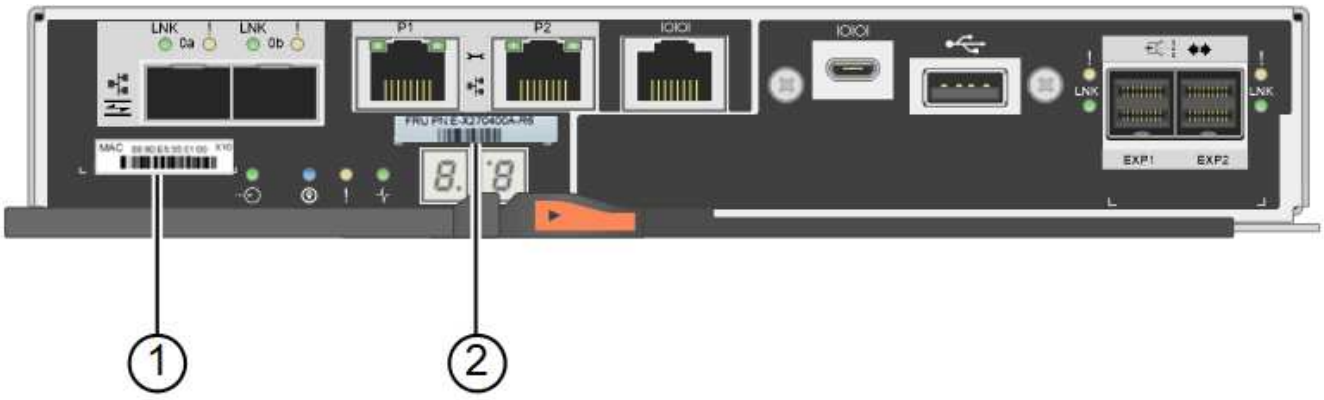
Passos

1. Desembale o novo controlador e coloque-o numa superfície plana e livre de estática.

   Guarde os materiais de embalagem a utilizar ao enviar o controlador avariado.

2. Localize o endereço MAC e as etiquetas de número de peça FRU na parte traseira do controlador de substituição.

Esta figura mostra o controlador E2800. O procedimento de substituição do controlador EF570 é idêntico.



Etiqueta	Etiqueta	Descrição
1	Endereço MAC	O endereço MAC da porta de gerenciamento 1 ("'P1"). Se você usou DHCP para obter o endereço IP do controlador original, precisará desse endereço para se conetar ao novo controlador.
2	Número de peça FRU	O número de peça da FRU. Este número deve corresponder ao número de peça de substituição para o controlador atualmente instalado.

3. Prepare-se para remover o controlador.

Use o Gerenciador de sistema do SANtricity para executar estas etapas. Conforme necessário para obter detalhes adicionais, consulte as instruções do e-Series para substituir o controlador de storage.

a. Confirme se o número de peça de substituição para o controlador com falha é o mesmo que o número de peça FRU para o controlador de substituição.

   Quando um controlador tem uma falha e precisa ser substituído, o número de peça de substituição é exibido na área Detalhes do Recovery Guru. Se você precisar encontrar esse número manualmente, você pode procurar o controlador na guia **base**.

> **Possível perda de acesso aos dados --** se os dois números de peça não forem os mesmos, não tente este procedimento.

a. Faça uma cópia de segurança da base de dados de configuração.

   Se ocorrer um problema ao remover um controlador, pode utilizar o ficheiro guardado para restaurar a configuração.

b. Colete dados de suporte para o dispositivo.

A coleta de dados de suporte antes e depois da substituição de um componente garante que você possa enviar um conjunto completo de logs para o suporte técnico caso a substituição não resolva o problema.

c. Leve o controlador que pretende substituir offline.

4. Retire o controlador do aparelho:
   a. Coloque uma pulseira antiestática ou tome outras precauções antiestáticas.
   b. Identifique os cabos e, em seguida, desligue os cabos e SFPs.

      Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos.

   c. Solte o controlador do aparelho apertando o trinco na pega do came até soltar e, em seguida, abra a pega do came para a direita.
   d. Utilizando as duas mãos e a pega do came, deslize o controlador para fora do aparelho.

      Utilize sempre duas mãos para suportar o peso do controlador.

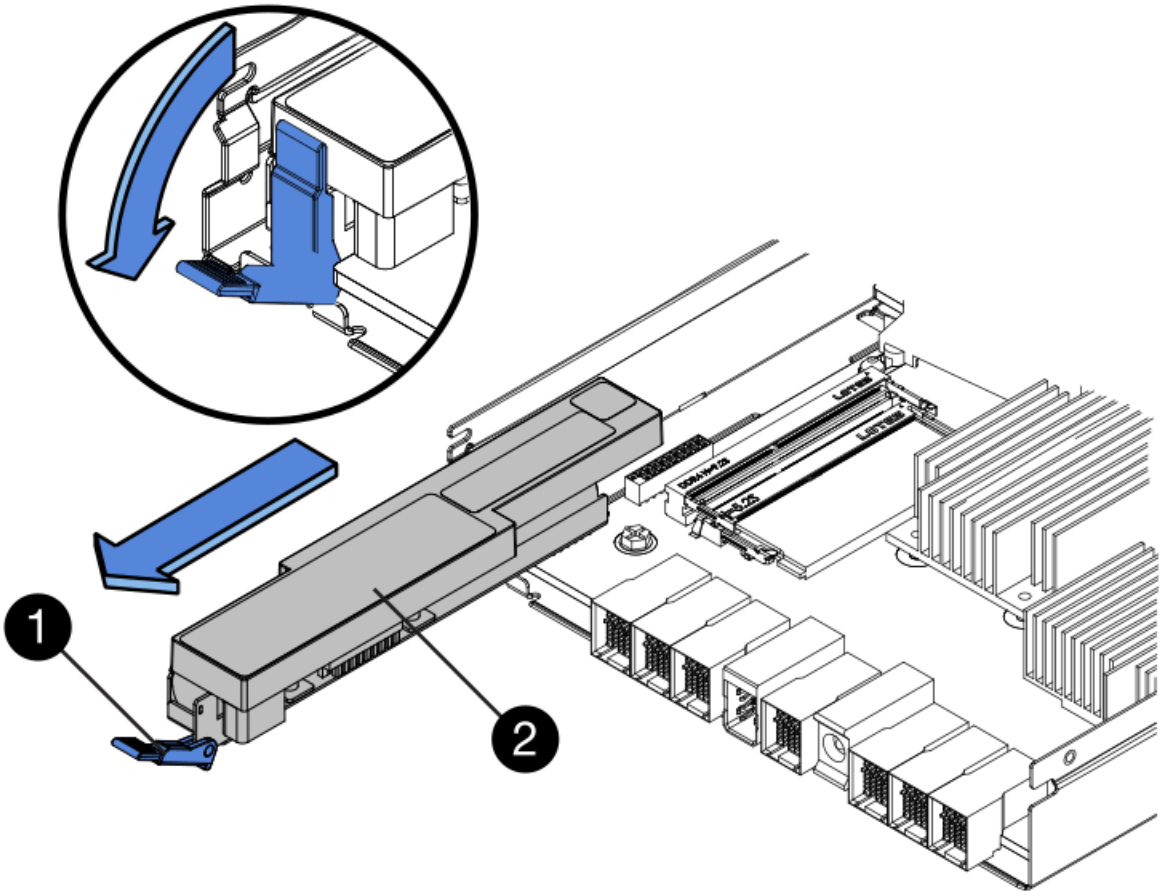
   e. Coloque o controlador numa superfície plana e sem estática com a tampa amovível virada para cima.
   f. Remova a tampa pressionando o botão e deslizando a tampa para fora.
5. Remova a bateria do controlador com falha e instale-a no controlador de substituição:
   a. Confirme se o LED verde dentro do controlador (entre a bateria e os DIMMs) está desligado.

      Se este LED verde estiver ligado, o controlador ainda está a utilizar a bateria. Deve aguardar que este LED se apague antes de remover quaisquer componentes.

Item	Descrição
	LED Ativo Cache Interno
	Bateria

b. Localize a trava de liberação azul da bateria.

c. Desengate a bateria empurrando a trava de liberação para baixo e afastando-a do controlador.



Item	Descrição
	Trinco de desbloqueio da bateria
	Bateria

d. Levante a bateria e deslize-a para fora do controlador.

e. Retire a tampa do controlador de substituição.

f. Oriente o controlador de substituição para que a ranhura da bateria fique voltada para si.

g. Introduza a bateria no controlador a um ligeiro ângulo descendente.

   Deve inserir a flange metálica na parte frontal da bateria na ranhura na parte inferior do controlador e deslizar a parte superior da bateria por baixo do pequeno pino de alinhamento no lado esquerdo do controlador.

h. Desloque o trinco da bateria para cima para fixar a bateria.

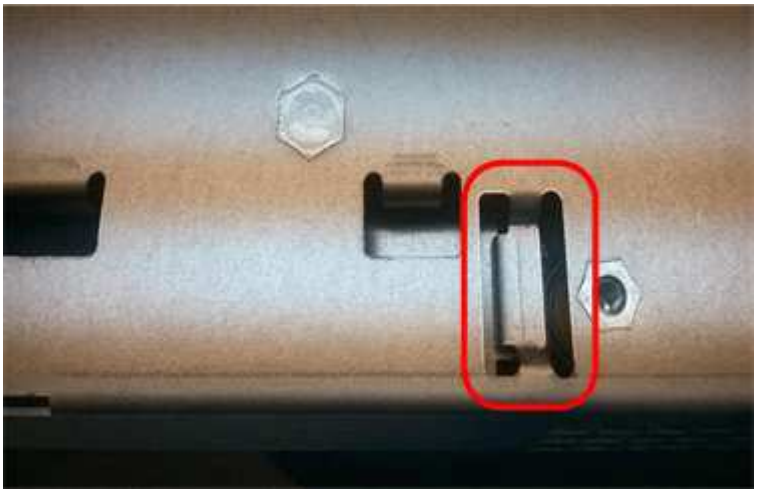
   Quando a trava se encaixa no lugar, a parte inferior da trava se encaixa em uma ranhura metálica no chassi.

i. Vire o controlador para confirmar que a bateria está instalada corretamente.

> **Possíveis danos ao hardware** — a flange metálica na parte frontal da bateria deve ser completamente inserida na ranhura do controlador (como mostrado na primeira figura). Se a bateria não estiver instalada corretamente (como mostrado na segunda figura), a flange metálica pode entrar em Contato com a placa controladora, causando danos.

- **Correto — a flange de metal da bateria está completamente inserida na ranhura do controlador:**

- **Incorreto — a flange metálica da bateria não está inserida na ranhura do controlador:**



j. Volte a colocar a tampa do controlador.

6. Instale o controlador de substituição no aparelho.
   a. Vire o controlador ao contrário, de modo a que a tampa amovível fique virada para baixo.
   b. Com a pega do came na posição aberta, deslize o controlador até ao aparelho.
   c. Mova a alavanca do came para a esquerda para bloquear o controlador no lugar.
   d. Substitua os cabos e SFPs.
   e. Se o controlador original usou DHCP para o endereço IP, localize o endereço MAC na etiqueta na parte de trás do controlador de substituição. Peça ao administrador da rede para associar o DNS/rede e o endereço IP do controlador removido com o endereço MAC do controlador de substituição.

      Se o controlador original não tiver utilizado DHCP para o endereço IP, o novo controlador adotará o endereço IP do controlador removido.

7. Coloque o controlador on-line usando o Gerenciador de sistemas da SANtricity:
   a. Selecione **hardware**.
   b. Se o gráfico mostrar as unidades, selecione **Mostrar parte traseira da prateleira**.
   c. Selecione o controlador que pretende colocar online.
   d. Selecione **Place Online** no menu de contexto e confirme que deseja executar a operação.
   e. Verifique se o visor de sete segmentos mostra um estado `99` de .
8. Confirme se o novo controlador é ideal e recolha dados de suporte.

Informações relacionadas

"Site de Documentação de sistemas NetApp e-Series"

Substituição de componentes de hardware na gaveta do controlador de storage

Se ocorrer um problema de hardware, talvez seja necessário substituir um componente no compartimento do controlador de storage.

O que você vai precisar

- Você tem o procedimento de substituição de hardware do e-Series.
- Você localizou fisicamente o dispositivo de armazenamento onde está substituindo os componentes de hardware do compartimento de armazenamento no data center.

  "Localizar o controlador em um data center"

Sobre esta tarefa

Para substituir a bateria no controlador de armazenamento, consulte as instruções nestas instruções para substituir um controlador de armazenamento. Essas instruções descrevem como remover um controlador do aparelho, remover a bateria do controlador, instalar a bateria e substituir o controlador.

Para obter instruções para as outras unidades substituíveis em campo (FRUs) nas gavetas de controladores, acesse os procedimentos e-Series para manutenção do sistema.

FRU	Consulte as instruções
Bateria	StorageGRID (estas instruções): Substituição de um controlador de armazenamento
Condução	E-Series: • Substitua a unidade (60 unidades) • Substitua a unidade (12 ou 24 unidades)
Depósito de alimentação	E-Series • Substitua o recipiente de alimentação (60 unidades) • Substitua a fonte de alimentação (12 unidades ou 24 unidades)
Recipiente do ventilador (somente compartimentos de 60 unidades)	E-Series: Substitua o recipiente do ventilador (60 unidades)
Gaveta de unidades (somente compartimentos de 60 unidades)	E-Series: Substitua a gaveta da unidade (60 unidades)

Informações relacionadas

"Site de Documentação de sistemas NetApp e-Series"

"Substituição de um controlador de armazenamento"

Substituição de componentes de hardware no compartimento de expansão de 60 unidades opcional

Talvez seja necessário substituir um módulo de entrada/saída, uma fonte de alimentação ou um ventilador no compartimento de expansão.

O que você vai precisar

- Você tem o procedimento de substituição de hardware do e-Series.
- Você localizou fisicamente o dispositivo de armazenamento onde está substituindo os componentes de hardware do compartimento de expansão no data center.

  "Localizar o controlador em um data center"

Sobre esta tarefa

Para substituir um módulo de entrada/saída (IOM) em um compartimento de expansão de 60 unidades, consulte as instruções nestas instruções para substituir um controlador de storage.

Para substituir uma fonte de alimentação ou um ventilador em um compartimento de expansão de 60 unidades, acesse os procedimentos do e-Series para manter o hardware de 60 unidades.

FRU	Consulte as instruções do e-Series para
Módulo de entrada/saída (IOM)	Substituindo uma OIM
Depósito de alimentação	Substitua o recipiente de alimentação (60 unidades)
Recipiente da ventoinha	Substitua o recipiente da ventoinha (60 unidades)

Encerrar o controlador SG6000-CN

Desligue o controlador SG6000-CN para efetuar a manutenção do hardware.

O que você vai precisar

- Você localizou fisicamente o controlador SG6000-CN que exige manutenção no data center.

  "Localizar o controlador em um data center"

- O aparelho foi colocado no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Para evitar interrupções de serviço, confirme se todos os outros nós de armazenamento estão conetados à grade antes de desligar o controlador ou desligue o controlador durante uma janela de manutenção programada quando os períodos de interrupção de serviço são normalmente esperados. Consulte as informações sobre como determinar estados de conexão de nós nas instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

> Se você já usou uma regra ILM que cria apenas uma cópia de um objeto, você deve encerrar o controlador durante uma janela de manutenção agendada. Caso contrário, você pode perder temporariamente o acesso a esses objetos durante este procedimento. Veja informações sobre o gerenciamento de objetos com o gerenciamento do ciclo de vida das informações.

Passos

1. Quando o aparelho tiver sido colocado no modo de manutenção, desligue o controlador SG6000-CN:

   > Você deve executar um desligamento controlado do controlador inserindo os comandos especificados abaixo. Desligar o controlador usando o interrutor de alimentação resultará em perda de dados.

   a. Faça login no nó de grade usando PuTTY ou outro cliente ssh:

      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 `#`.

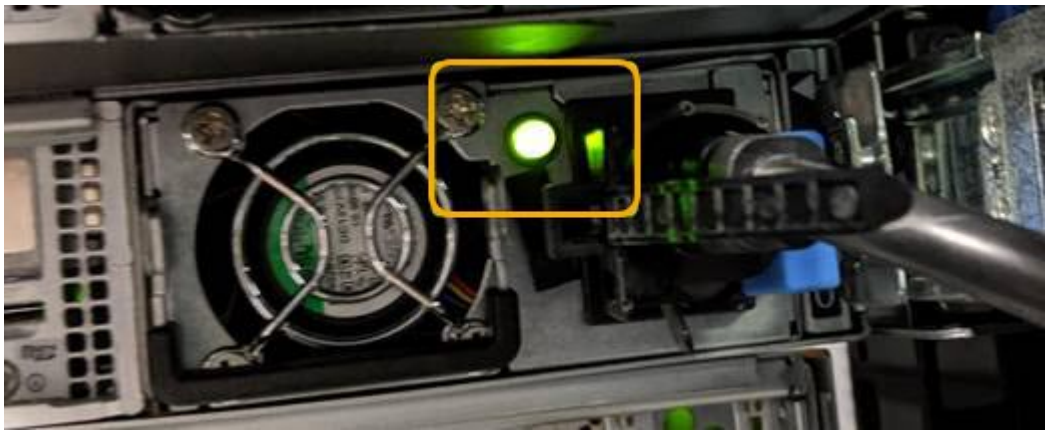
b. Desligar o controlador SG6000-CN

```
shutdown -h now
```

Esse comando pode levar até 10 minutos para ser concluído.

2. Use um dos seguintes métodos para verificar se o controlador SG6000-CN está desligado:
   - Olhe para o LED azul de alimentação na parte frontal do controlador e confirme que está desligado.

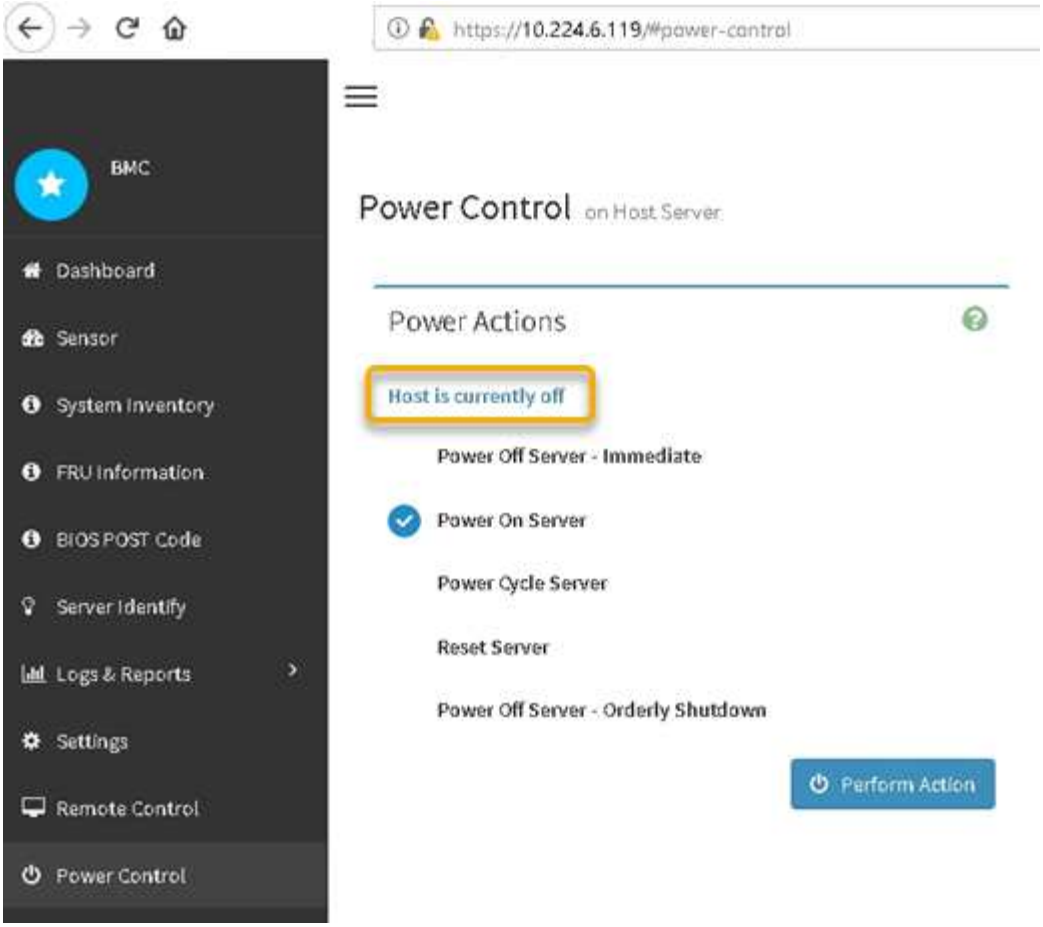
   - Observe os LEDs verdes em ambas as fontes de alimentação na parte traseira do controlador e confirme que piscam a uma taxa regular (aproximadamente um piscar por segundo).



   - Use a interface BMC do controlador:
     i. Acesse a interface BMC do controlador.

     "Acessando a interface BMC"

     ii. Selecione **Power Control**.
     iii. Verifique se as ações de energia indicam que o host está desligado no momento.



Informações relacionadas

"Remover o controlador SG6000-CN de um gabinete ou rack"

Ligar o controlador SG6000-CN e verificar a operação

Ligue o controlador após concluir a manutenção.

O que você vai precisar

- Você instalou o controlador em um gabinete ou rack e conetou os cabos de dados e alimentação.

  "Reinstalar o controlador SG6000-CN em um gabinete ou rack"

- Você localizou fisicamente o controlador no data center.

  "Localizar o controlador em um data center"

Passos

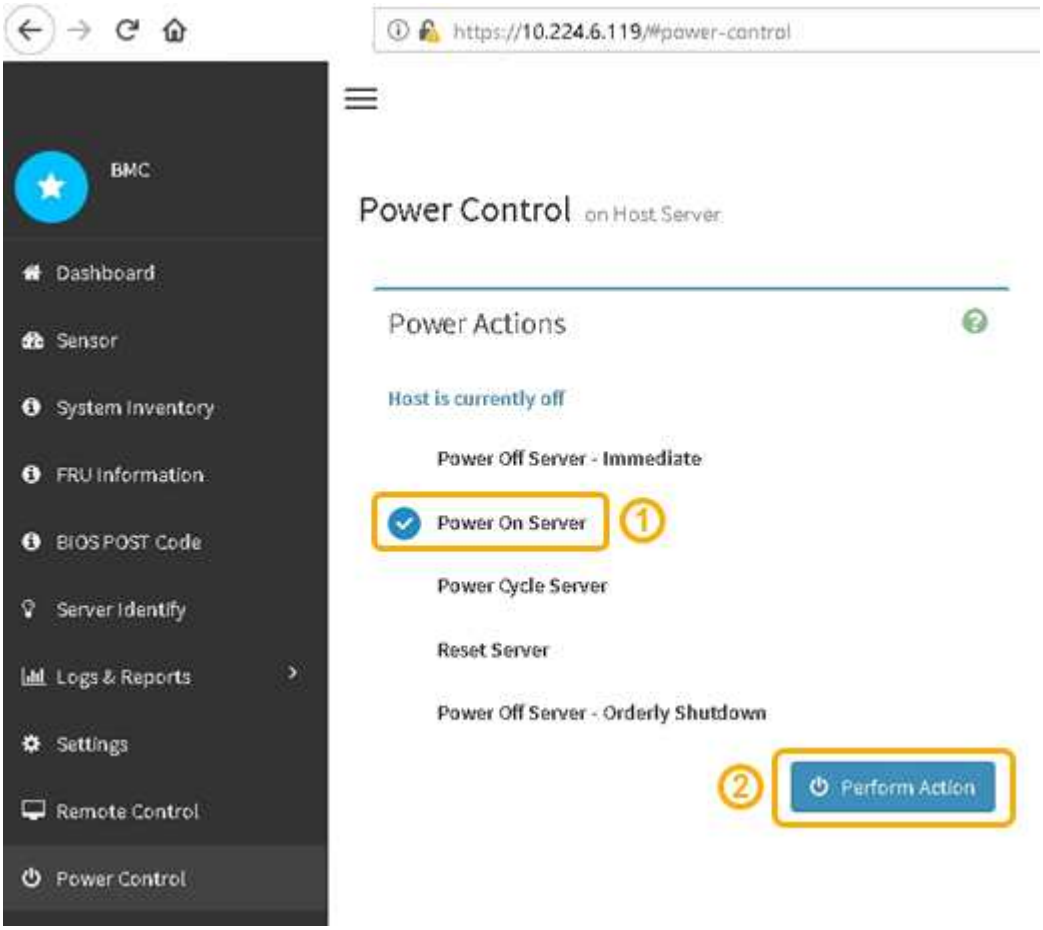
1. Ligue o controlador SG6000-CN e monitorize os LEDs do controlador e os códigos de arranque utilizando um dos seguintes métodos:

   - Prima o interrutor de alimentação na parte frontal do controlador.

- Use a interface BMC do controlador:
  i. Acesse a interface BMC do controlador.

     "Acessando a interface BMC"

  ii. Selecione **Power Control**.
  iii. Selecione **Power on Server** e, em seguida, selecione **Perform Action**.



Use a interface BMC para monitorar o status de inicialização.

2. Confirme se o controlador do dispositivo é apresentado no Gestor de grelha e sem alertas.

   Pode levar até 20 minutos para o controlador ser exibido no Gerenciador de Grade.

3. Confirme se o novo controlador SG6000-CN está totalmente operacional:

   a. Faça login no nó de grade usando PuTTY ou outro cliente ssh:

      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. Digite o seguinte comando e verifique se ele retorna a saída esperada
   `cat /sys/class/fc_host/*/port_state`

   Saída esperada:

   ```
   Online
   Online
   Online
   ```

   Se a saída esperada não for devolvida, entre em Contato com o suporte técnico.

   c. Digite o seguinte comando e verifique se ele retorna a saída esperada
   `cat /sys/class/fc_host/*/speed`

   Saída esperada:

```
16 Gbit
16 Gbit
16 Gbit16 Gbit
16 Gbit
```

+
Se a saída esperada não for devolvida, entre em Contato com o suporte técnico.

   a. Na página nós no Gerenciador de Grade, verifique se o nó do dispositivo está conetado à grade e não tem alertas.

   > Não coloque outro nó de dispositivo offline a menos que este aparelho tenha um ícone verde.

4. Opcional: Instale o painel frontal, se um tiver sido removido.

Informações relacionadas

"Visualizar indicadores de estado e botões no controlador SG6000-CN"

"Exibindo códigos de status de inicialização para os controladores de storage SG6000"

Substituição do controlador SG6000-CN

Talvez seja necessário substituir o controlador SG6000-CN se ele não estiver funcionando de forma ideal ou se ele tiver falhado.

O que você vai precisar

- Você tem um controlador de substituição com o mesmo número de peça do controlador que está substituindo.
- Você tem etiquetas para identificar cada cabo conetado ao controlador.
- Você localizou fisicamente o controlador para substituir no data center.

  "Localizar o controlador em um data center"

Sobre esta tarefa

O nó de armazenamento do aparelho não estará acessível quando substituir o controlador SG6000-CN. Se o controlador SG6000-CN estiver a funcionar o suficiente, pode efetuar um encerramento controlado no início deste procedimento.

> Se você estiver substituindo o controlador antes de instalar o software StorageGRID, talvez você não consiga acessar o instalador do StorageGRID Appliance imediatamente após concluir este procedimento. Embora você possa acessar o Instalador de dispositivos StorageGRID de outros hosts na mesma sub-rede que o appliance, você não pode acessá-lo de hosts em outras sub-redes. Esta condição deve resolver-se dentro de 15 minutos (quando qualquer entrada de cache ARP para o tempo limite do controlador original), ou você pode limpar a condição imediatamente, limpando quaisquer entradas de cache ARP antigas manualmente do roteador ou gateway local.

Passos

1. Se o controlador SG6000-CN estiver a funcionar o suficiente para permitir um encerramento controlado, desligue o controlador SG6000-CN.

   "Encerrar o controlador SG6000-CN"

   O LED verde Cache ative na parte de trás do controlador E2800 fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue.

2. Utilize um dos dois métodos para verificar se a alimentação do controlador SG6000-CN está desligada:
   - O LED indicador de alimentação na parte frontal do controlador está apagado.
   - A página Controle de Energia da interface BMC indica que o controlador está desligado.
3. Se as redes StorageGRID conetadas ao controlador usarem servidores DHCP, atualize as configurações de DNS/rede e endereço IP.

   a. Localize a etiqueta de endereço MAC na parte frontal do controlador SG6000-CN e determine o endereço MAC da porta Admin Network.

O rótulo de endereço MAC lista o endereço MAC da porta de gerenciamento BMC. Para determinar o endereço MAC da porta Admin Network, você deve adicionar **2** ao número hexadecimal na etiqueta. Por exemplo, se o endereço MAC na etiqueta terminar em **09**, o endereço MAC da porta Admin terminaria em **0B**. Se o endereço MAC na etiqueta terminar em **(*y*)FF**, o endereço MAC da porta Admin terminaria em **(*y*(1)01**. Você pode facilmente fazer esse cálculo abrindo o Calculator no Windows, definindo-o para o modo Programador, selecionando Hex, digitando o endereço MAC e, em seguida, digitando * 2 *.

b. Peça ao administrador da rede para associar o DNS/rede e o endereço IP do controlador removido com o endereço MAC do controlador de substituição.

Você deve garantir que todos os endereços IP do controlador original foram atualizados antes de aplicar energia ao controlador de substituição. Caso contrário, o controlador obterá novos endereços IP DHCP quando iniciar e poderá não conseguir reconetar-se ao StorageGRID. Esta etapa se aplica a todas as redes StorageGRID conetadas ao controlador.

Se o controlador original usou o endereço IP estático, o novo controlador adotará automaticamente os endereços IP do controlador que você removeu.

4. Retirar e substituir o controlador SG6000-CN:
   a. Identifique os cabos e, em seguida, desconete os cabos e quaisquer transcetores SFP ou SFP28.

      Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos.

   b. Remova o controlador com falha do gabinete ou rack.
   c. Instale o controlador de substituição no gabinete ou rack.
   d. Substitua os cabos e quaisquer transcetores SFP ou SFP28.
   e. Ligue o controlador e monitorize os LEDs do controlador e os códigos de arranque.
5. Confirme se o nó de armazenamento do dispositivo é exibido no Gerenciador de Grade e se nenhum alarme é exibido.
6. No Gerenciador de Grade, selecione **nós** e verifique se o endereço IP do BMC para o controlador de nó está correto.

   Se o endereço IP do controlador do nó não for válido ou não estiver no intervalo esperado, reconfigure o endereço IP conforme descrito nas instruções de recuperação e manutenção.

   "Manter recuperar"

Informações relacionadas

"SG6000-CN: Instalação em um gabinete ou rack"

"Visualizar indicadores de estado e botões no controlador SG6000-CN"

"Visualizar códigos de inicialização para o controlador SG6000-CN"

Substituição de uma fonte de alimentação no controlador SG6000-CN

O controlador SG6000-CN tem duas fontes de alimentação para redundância. Se uma das fontes de alimentação falhar, você deve substituí-la o mais rápido possível para garantir que o controlador de computação tenha energia redundante.

O que você vai precisar

- Desembalou a fonte de alimentação de substituição.
- Você localizou fisicamente o controlador onde está substituindo a fonte de alimentação no data center.

  "Localizar o controlador em um data center"

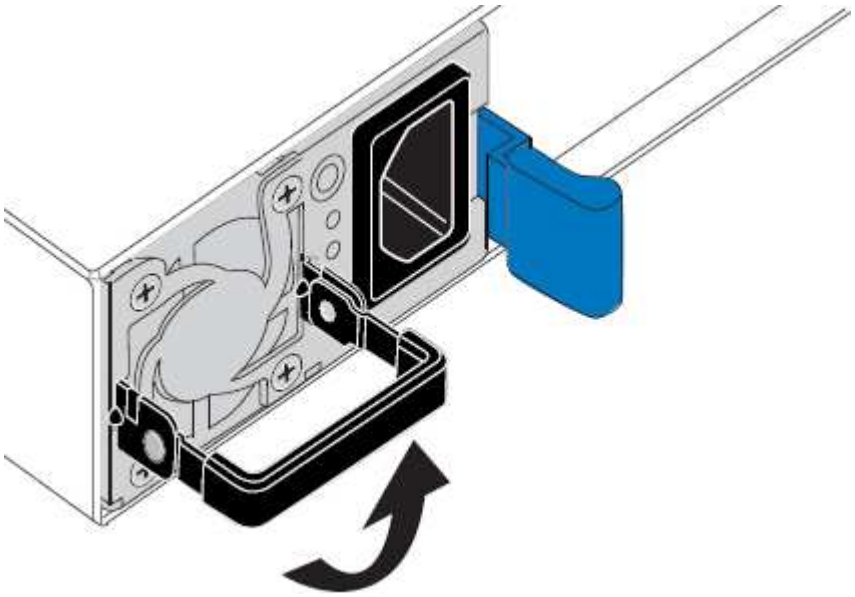
- Confirmou que a outra fonte de alimentação está instalada e em funcionamento.

Sobre esta tarefa

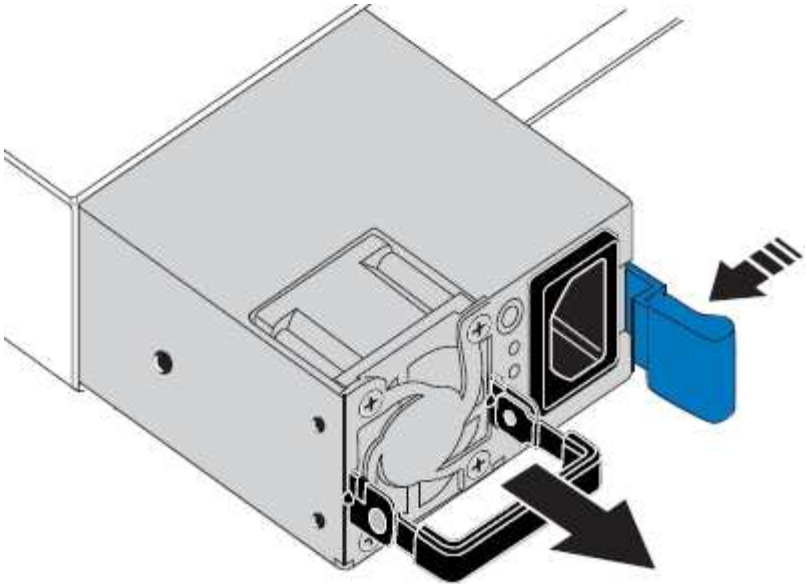
A figura mostra as duas unidades de fonte de alimentação para o controlador SG6000-CN, que são acessíveis a partir da parte de trás do controlador.

Passos

1. Desconete o cabo de alimentação da fonte de alimentação.
2. Levante o manípulo do excêntrico.

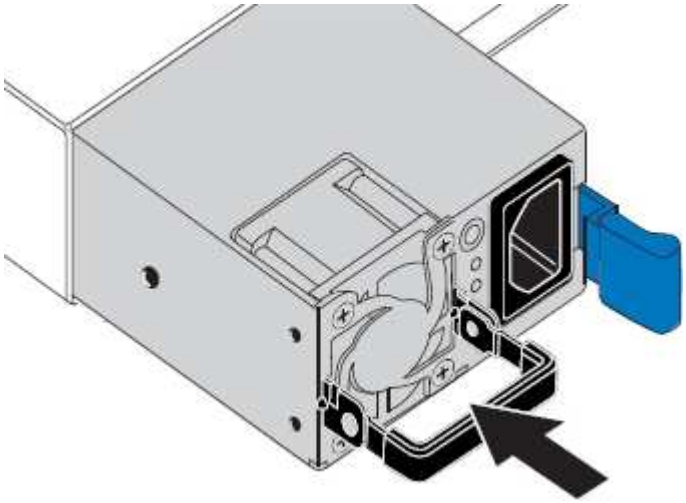


3. Pressione o trinco azul e puxe a fonte de alimentação para fora.



4. Faça deslizar a fonte de alimentação de substituição para o chassis.

   Certifique-se de que o trinco azul se encontra no lado direito ao deslizar a unidade para dentro.



5. Empurre o manípulo do came para baixo para fixar a fonte de alimentação.
6. Ligue o cabo de alimentação à fonte de alimentação e certifique-se de que o LED verde se acende.

Remover o controlador SG6000-CN de um gabinete ou rack

Remova o controlador SG6000-CN de um gabinete ou rack para acessar a tampa superior ou mover o controlador para um local diferente.

O que você vai precisar

- Você tem etiquetas para identificar cada cabo conetado ao controlador SG6000-CN.
- Você localizou fisicamente o controlador SG6000-CN onde está realizando manutenção no data center.

  "Localizar o controlador em um data center"

- Desligou o controlador SG6000-CN.

"Encerrar o controlador SG6000-CN"

Não desligue o controlador utilizando o interrutor de alimentação.

Passos

1. Identifique e, em seguida, desligue os cabos de alimentação do controlador.
2. Enrole a extremidade da correia da pulseira ESD à volta do pulso e fixe a extremidade do clipe a um solo metálico para evitar descargas estáticas.
3. Identifique e desconete os cabos de dados do controlador e quaisquer transcetores SFP ou SFP28.

   Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos.

4. Desaperte os dois parafusos integrados no painel frontal do controlador.

5. Deslize o controlador SG6000-CN para a frente para fora do rack até que os trilhos de montagem estejam totalmente estendidos e você ouvir os trincos em ambos os lados clicarem.

   A tampa superior do controlador está acessível.

6. Opcional: Se você estiver removendo totalmente o controlador do gabinete ou rack, siga as instruções para o kit de trilho para remover o controlador dos trilhos.

Informações relacionadas

"Retirar a tampa do controlador SG6000-CN"

Reinstalar o controlador SG6000-CN em um gabinete ou rack

Reinstale o controlador em um gabinete ou rack quando a manutenção do hardware estiver concluída.

O que você vai precisar

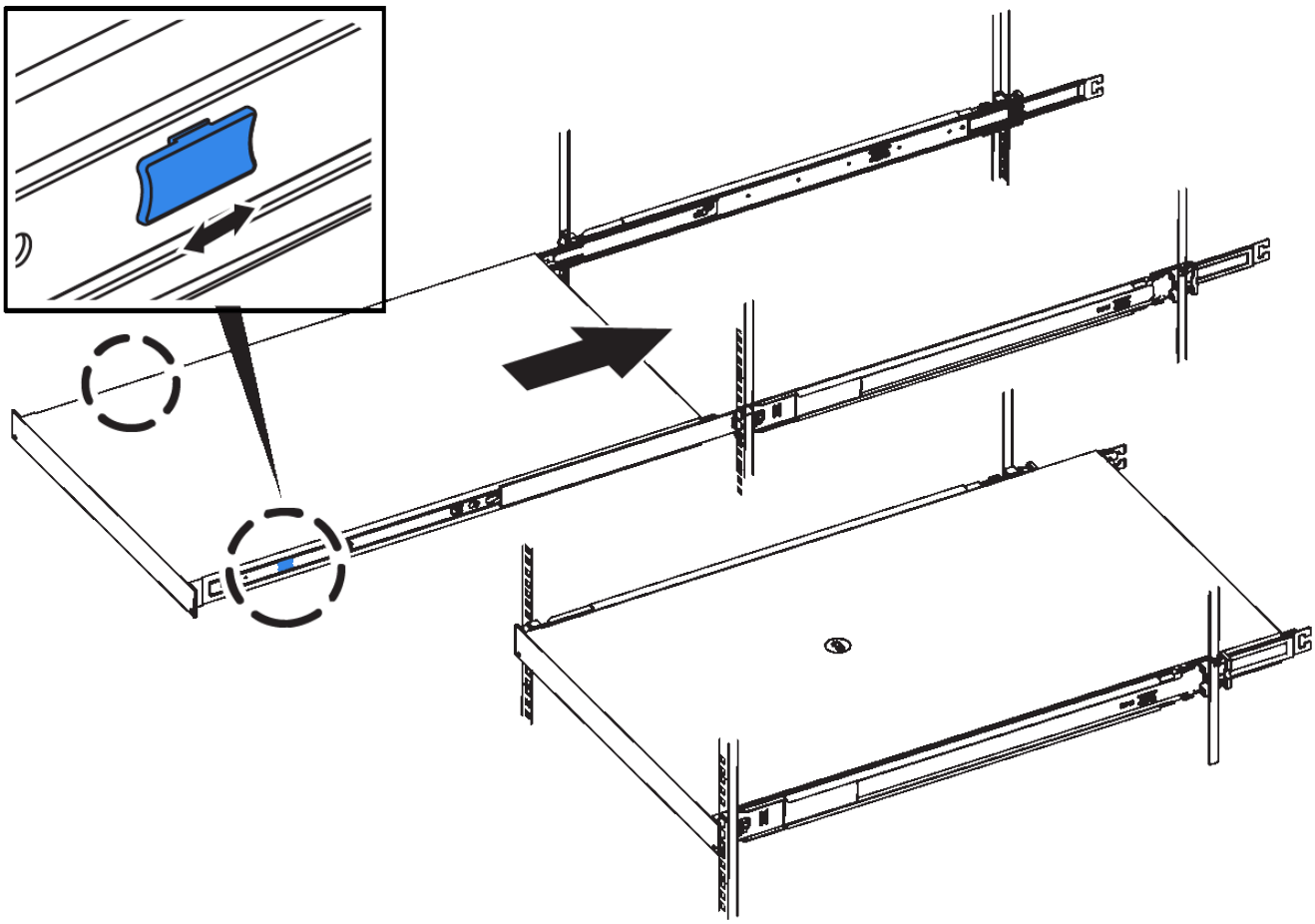
Reinstalou a tampa do controlador.

"Voltar a instalar a tampa do controlador SG6000-CN"

Passos

1. Pressione o trilho azul libera ambos os trilhos do rack ao mesmo tempo e deslize o controlador SG6000-CN para dentro do rack até que ele esteja totalmente assentado.

   Quando não conseguir mover o controlador mais, puxe os trincos azuis em ambos os lados do chassis para deslizar o controlador até ao fim.



Não conete a moldura frontal até que você ligue o controlador.

2. Aperte os parafusos integrados no painel frontal do controlador para fixar o controlador no rack.

3. Enrole a extremidade da correia da pulseira ESD à volta do pulso e fixe a extremidade do clipe a um solo metálico para evitar descargas estáticas.
4. Reconecte os cabos de dados do controlador e quaisquer transcetores SFP ou SFP28.

Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos.

"Cabeamento do aparelho (SG6000)"

5. Reconecte os cabos de alimentação do controlador.

"Conexão dos cabos de alimentação e alimentação de energia (SG6000)"

Depois de terminar

O controlador pode ser reiniciado.

"Ligar o controlador SG6000-CN e verificar a operação"

Retirar a tampa do controlador SG6000-CN

Retire a tampa do controlador para aceder aos componentes internos para manutenção.

O que você vai precisar

Remova o controlador do gabinete ou rack para acessar a tampa superior.

"Remover o controlador SG6000-CN de um gabinete ou rack"

Passos

1. Certifique-se de que o trinco da tampa do controlador SG6000-CN não está bloqueado. Se necessário, rode o bloqueio do trinco de plástico azul um quarto de volta na direção de desbloqueio, conforme ilustrado no bloqueio do trinco.
2. Rode o trinco para cima e para trás em direção à parte traseira do chassis do controlador SG6000-CN até parar; em seguida, levante cuidadosamente a tampa do chassis e coloque-a de lado.

Enrole a extremidade da correia de uma pulseira antiestática em torno do pulso e fixe a extremidade do clipe a uma terra metálica para evitar descarga estática ao trabalhar dentro do controlador SG6000-CN.

Informações relacionadas

"Remover o HBA Fibre Channel"

Voltar a instalar a tampa do controlador SG6000-CN

Reinstale a tampa do controlador quando a manutenção interna do hardware estiver concluída.

O que você vai precisar

Concluiu todos os procedimentos de manutenção no interior do controlador.

Passos

1. Com a trava da tampa aberta, segure a tampa acima do chassi e alinhe o orifício no trinco da tampa superior com o pino no chassi. Quando a tampa estiver alinhada, baixe-a sobre o chassis.

2. Rode o trinco da tampa para a frente e para baixo até parar e a tampa assentar totalmente no chassis. Verifique se não existem folgas ao longo da extremidade dianteira da tampa.

   Se a tampa não estiver totalmente encaixada, talvez você não consiga deslizar o controlador SG6000-CN para dentro do rack.

3. Opcional: Rode o fecho de plástico azul um quarto de volta na direção do bloqueio, conforme ilustrado no bloqueio do trinco, para o bloquear.

Depois de terminar

Reinstale o controlador no gabinete ou rack.

"Reinstalar o controlador SG6000-CN em um gabinete ou rack"

Substituição do HBA Fibre Channel no controlador SG6000-CN

Talvez seja necessário substituir o adaptador de barramento de host (HBA) Fibre Channel no controlador SG6000-CN se ele não estiver funcionando de forma ideal ou se tiver falhado.

Verificar a substituição do HBA Fibre Channel

Se não tiver a certeza de qual adaptador de barramento de host (HBA) Fibre Channel deve ser substituído, execute este procedimento para identificá-lo.

O que você vai precisar

- Tem o número de série do dispositivo de armazenamento ou do controlador SG6000-CN em que o HBA Fibre Channel precisa de ser substituído.

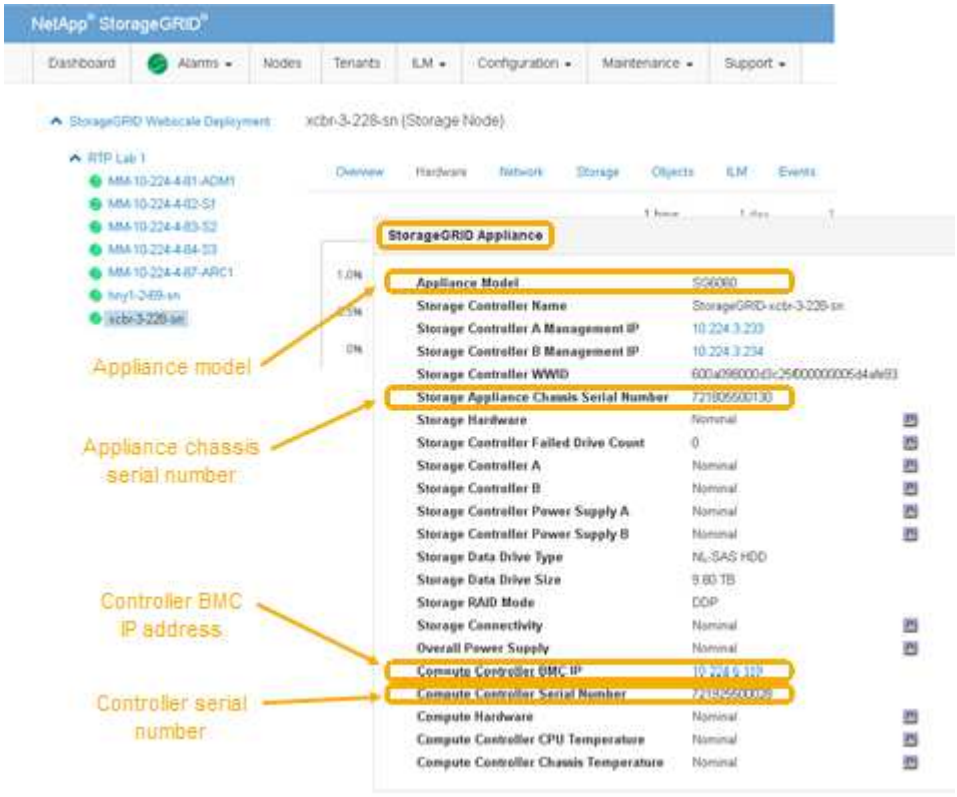
  > Se o número de série do dispositivo de armazenamento que contém o HBA Fibre Channel que você está substituindo começar pela letra Q, ele não será listado no Gerenciador de Grade. Você deve verificar as tags anexadas à frente de cada controlador SG6000-CN no data center até encontrar uma correspondência.

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. No Gerenciador de Grade, selecione **nós**.
2. Na exibição em árvore da página nós, selecione um nó de storage do dispositivo.
3. Selecione a guia **hardware**.

   Verifique o número de série do chassi do dispositivo de armazenamento e o número de série do controlador de computação na seção StorageGRID Appliance para ver se um desses números de série corresponde ao número de série do dispositivo de armazenamento onde você está substituindo o HBA Fibre Channel. Se qualquer um dos números de série corresponder, encontrou o aparelho correto.



   - Se a seção StorageGRID Appliance não for exibida, o nó selecionado não será um dispositivo StorageGRID. Selecione um nó diferente na exibição em árvore.
   - Se o modelo do aparelho não for SG6060, selecione um nó diferente na vista em árvore.
   - Se os números de série não corresponderem, selecione um nó diferente na vista de árvore.
4. Depois de localizar o nó onde o HBA Fibre Channel precisa ser substituído, anote o endereço IP do BMC do controlador de computação listado na seção StorageGRID Appliance.

   Você pode usar esse endereço IP para ativar o LED de identificação do controlador de computação, para ajudá-lo a localizar o dispositivo no data center.

   "Ligar e desligar o LED de identificação do controlador"

Informações relacionadas

"Remover o HBA Fibre Channel"

Remover o HBA Fibre Channel

Talvez seja necessário substituir o adaptador de barramento de host (HBA) Fibre Channel no controlador SG6000-CN se ele não estiver funcionando de forma ideal ou se tiver falhado.

O que você vai precisar

- Tem a HBA Fibre Channel de substituição correta.
- Você determinou qual controlador SG6000-CN contém o HBA Fibre Channel para substituir.

  "Verificar a substituição do HBA Fibre Channel"

- Você localizou fisicamente o controlador SG6000-CN onde está substituindo o HBA Fibre Channel no data center.

  "Localizar o controlador em um data center"

- Removeu a tampa do controlador.

  "Retirar a tampa do controlador SG6000-CN"

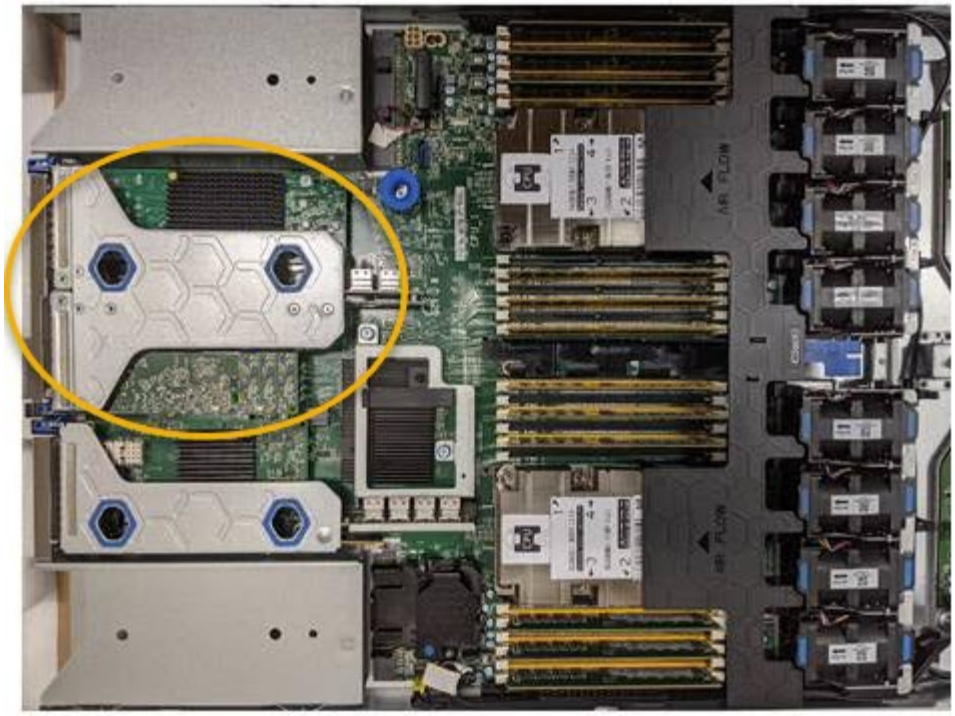
Sobre esta tarefa

Para evitar interrupções de serviço, confirme se todos os outros nós de armazenamento estão conetados à grade antes de iniciar a substituição do HBA Fibre Channel ou substitua o adaptador durante uma janela de manutenção programada quando períodos de interrupção de serviço normalmente forem esperados. Consulte as informações sobre como determinar estados de conexão de nós nas instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

> Se você já usou uma regra ILM que cria apenas uma cópia de um objeto, você deve substituir o HBA Fibre Channel durante uma janela de manutenção agendada. Caso contrário, você pode perder temporariamente o acesso a esses objetos durante este procedimento. Veja informações sobre o gerenciamento de objetos com o gerenciamento do ciclo de vida das informações.

Passos

1. Enrole a extremidade da correia da pulseira ESD à volta do pulso e fixe a extremidade do clipe a um solo metálico para evitar descargas estáticas.
2. Localize o conjunto da riser na parte traseira do controlador que contém o HBA Fibre Channel.



3. Segure o conjunto da riser através dos orifícios marcados a azul e levante-o cuidadosamente para cima. Mova o conjunto da riser em direção à parte frontal do chassi enquanto o levanta para permitir que os conetores externos em seus adaptadores instalados evitem o chassi.
4. Coloque a placa riser em uma superfície plana e antiestática com o lado da estrutura metálica voltado para baixo para acessar os adaptadores.

Há dois adaptadores no conjunto da riser: Um HBA Fibre Channel e um adaptador de rede Ethernet. A HBA Fibre Channel é indicada na ilustração.

5. Abra a trava azul do adaptador (circulada) e remova cuidadosamente o HBA Fibre Channel do conjunto da riser. Agite ligeiramente o adaptador para ajudar a remover o adaptador do respetivo conetor. Não utilize força excessiva.
6. Coloque o adaptador numa superfície plana anti-estática.

Depois de terminar

Instale o HBA Fibre Channel de substituição.

"Reinstalar o HBA Fibre Channel"

Informações relacionadas

"Reinstalar o HBA Fibre Channel"

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

"Gerenciar objetos com ILM"

Reinstalar o HBA Fibre Channel

O HBA Fibre Channel de substituição é instalado no mesmo local que o que foi removido.

O que você vai precisar

- Tem a HBA Fibre Channel de substituição correta.
- Removeu a HBA Fibre Channel existente.

  "Remover o HBA Fibre Channel"

Passos

1. Enrole a extremidade da correia da pulseira ESD à volta do pulso e fixe a extremidade do clipe a um solo metálico para evitar descargas estáticas.
2. Retire a HBA Fibre Channel de substituição da embalagem.
3. Com a trava azul do adaptador na posição aberta, alinhe o HBA Fibre Channel com seu conetor no conjunto da riser; em seguida, pressione cuidadosamente o adaptador no conetor até que ele esteja totalmente assentado.

   Há dois adaptadores no conjunto da riser: Um HBA Fibre Channel e um adaptador de rede Ethernet. A HBA Fibre Channel é indicada na ilustração.

4. Localize o orifício de alinhamento no conjunto da riser (circulado) que se alinha com um pino guia na placa de sistema para garantir o posicionamento correto do conjunto da riser.

5. Posicione o conjunto da riser no chassi, certificando-se de que ele se alinha com o conetor e o pino guia na placa de sistema; em seguida, insira o conjunto da riser.
6. Pressione cuidadosamente o conjunto da riser no lugar ao longo de sua linha central, ao lado dos orifícios marcados com azul, até que esteja totalmente assentado.
7. Retire as tampas de proteçãoão das portas HBA Fibre Channel onde irá reinstalar os cabos.

Depois de terminar

Se não houver outros procedimentos de manutenção a serem executados no controlador, reinstale a tampa do controlador.

"Voltar a instalar a tampa do controlador SG6000-CN"

Alterar a configuração do link do controlador SG6000-CN

Pode alterar a configuração da ligação Ethernet do controlador SG6000-CN. Pode alterar o modo de ligação de porta, o modo de ligação de rede e a velocidade de ligação.

O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

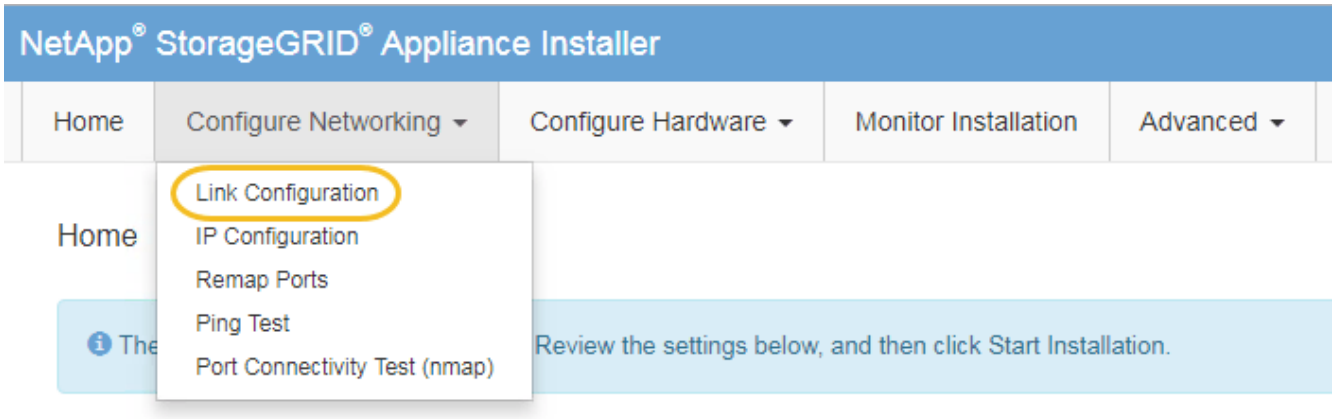
Sobre esta tarefa

As opções para alterar a configuração do link Ethernet do controlador SG6000-CN incluem:

- Alterar o modo **Port bond** de fixo para agregado, ou de agregado para fixo
- Alteração do **modo de ligação de rede** de ative-Backup para LACP ou de LACP para ative-Backup
- Ativar ou desativar a marcação de VLAN ou alterar o valor de uma tag VLAN
- Alterar a velocidade da ligação.

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Configurar rede Configuração de ligação**.



1. Faça as alterações desejadas na configuração do link.

   Para obter mais informações sobre as opções, "Configurando links de rede (SG6000)"consulte .

2. Quando estiver satisfeito com suas seleções, clique em **Salvar**.

   > Poderá perder a ligação se tiver efetuado alterações à rede ou à ligação através da qual está ligado. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do Instalador de appliance StorageGRID usando um dos outros endereços IP atribuídos ao appliance
   > **`https://Appliance_Controller_IP:8443`**

   Se você fez alterações nas configurações de VLAN, a sub-rede do dispositivo pode ter sido alterada. Se você precisar alterar os endereços IP do dispositivo, siga as instruções para configurar endereços IP.

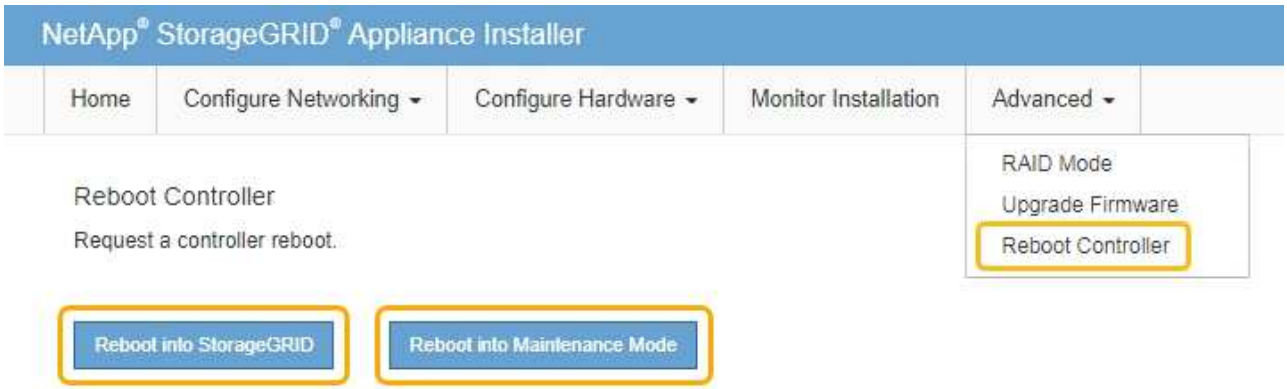
   "Configurando endereços IP do StorageGRID"

3. Selecione **Configurar rede Teste de ping** no menu.
4. Use a ferramenta Teste de ping para verificar a conetividade com endereços IP em qualquer rede que possa ter sido afetada pelas alterações de configuração de link feitas na alterações na configuração do link etapa.

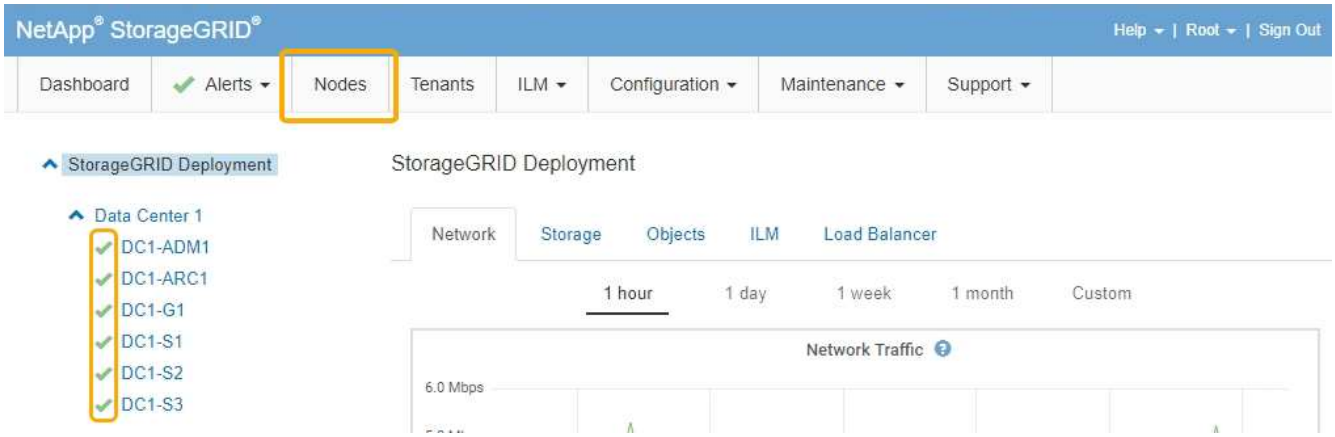
   Além de quaisquer outros testes que você escolher executar, confirme que você pode fazer ping no endereço IP da rede de Grade do nó Admin principal e no endereço IP da rede de Grade de pelo menos um outro nó de armazenamento. Se necessário, retorne à alterações na configuração do link etapa e corrija quaisquer problemas de configuração de link.

5. Quando estiver satisfeito de que as alterações na configuração do link estão funcionando, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Alterar a definição MTU

Você pode alterar a configuração MTU atribuída quando configurou endereços IP para o nó do dispositivo.

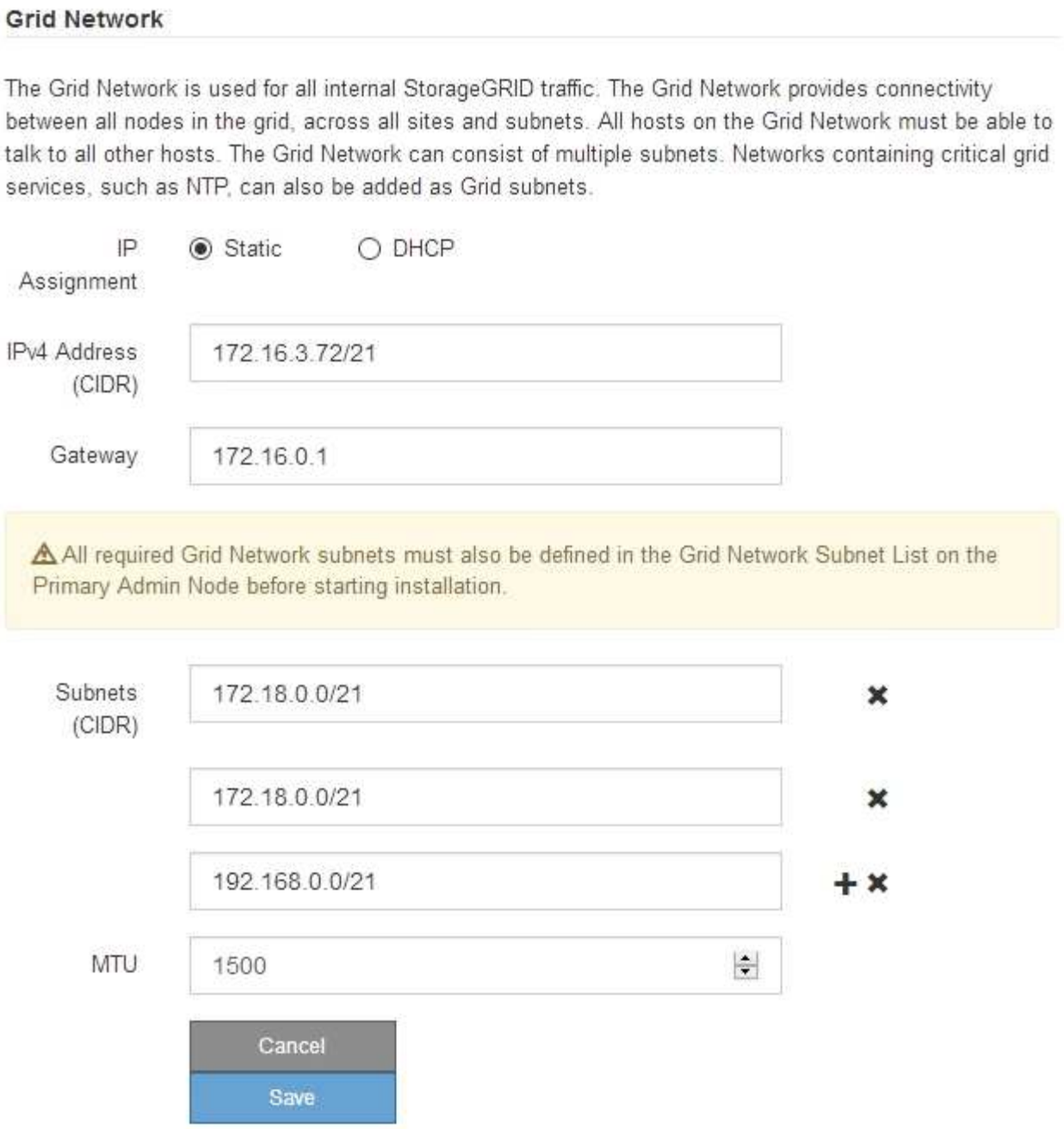
O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração IP**.
2. Faça as alterações desejadas nas configurações de MTU para rede de Grade, rede de Admin e rede de cliente.



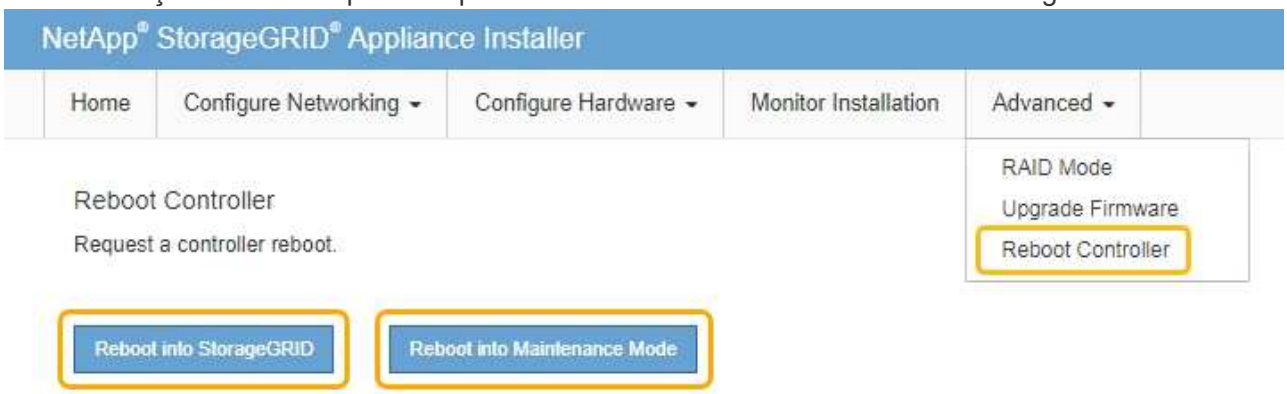
O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

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.

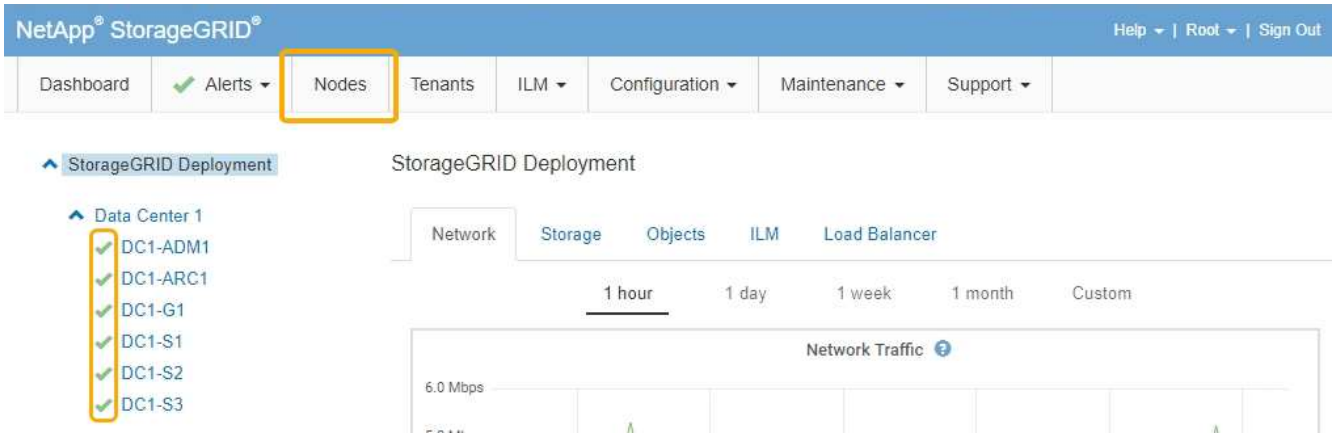
3. Quando estiver satisfeito com as definições, selecione **Guardar**.
4. Reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de**

reinicialização e, em seguida, selecione uma destas opções:

- Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
- Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Administrar o StorageGRID"

Verificar a configuração do servidor DNS

Você pode verificar e alterar temporariamente os servidores DNS (sistema de nomes de domínio) que estão atualmente em uso por este nó de appliance.

O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Talvez seja necessário alterar as configurações do servidor DNS se um dispositivo criptografado não puder se conetar ao servidor de gerenciamento de chaves (KMS) ou ao cluster KMS porque o nome do host para o KMS foi especificado como um nome de domínio em vez de um endereço IP. Quaisquer alterações efetuadas nas definições de DNS do dispositivo são temporárias e perdem-se quando sai do modo de manutenção. Para tornar essas alterações permanentes, especifique os servidores DNS no Gerenciador de Grade (**Manutenção rede servidores DNS**).

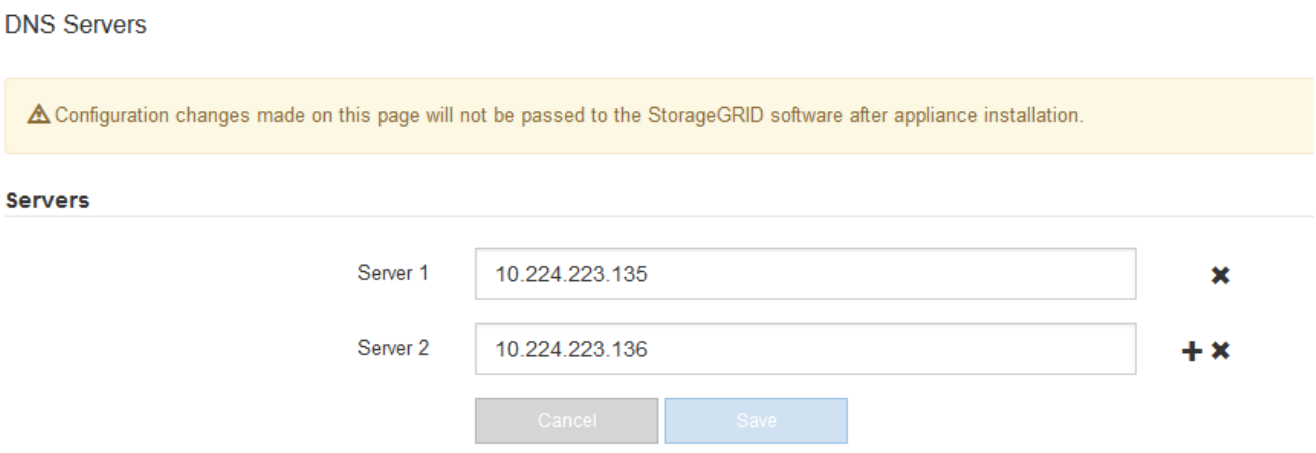
- As alterações temporárias na configuração DNS são necessárias apenas para dispositivos encriptados por nó onde o servidor KMS é definido utilizando um nome de domínio totalmente qualificado, em vez de um endereço IP, para o nome de anfitrião.
- Quando um dispositivo criptografado por nó se coneta a um KMS usando um nome de domínio, ele deve se conetar a um dos servidores DNS definidos para a grade. Um desses servidores DNS converte o nome de domínio em um endereço IP.
- Se o nó não conseguir alcançar um servidor DNS para a grade, ou se você alterou as configurações de DNS em toda a grade quando um nó de dispositivo criptografado por nó estava off-line, o nó não consegue se conetar ao KMS. Os dados criptografados no dispositivo não podem ser descriptografados até que o problema de DNS seja resolvido.

Para resolver um problema de DNS que impede a ligação KMS, especifique o endereço IP de um ou mais servidores DNS no Instalador de aplicações StorageGRID. Essas configurações de DNS temporárias permitem que o dispositivo se conete ao KMS e descriptografar dados no nó.

Por exemplo, se o servidor DNS para a grade mudar enquanto um nó criptografado estava off-line, o nó não será capaz de alcançar o KMS quando ele voltar on-line, uma vez que ainda está usando os valores DNS anteriores. A introdução do novo endereço IP do servidor DNS no Instalador de aplicações StorageGRID permite que uma ligação KMS temporária desencripte os dados do nó.

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração de DNS**.
2. Verifique se os servidores DNS especificados estão corretos.



3. Se necessário, altere os servidores DNS.

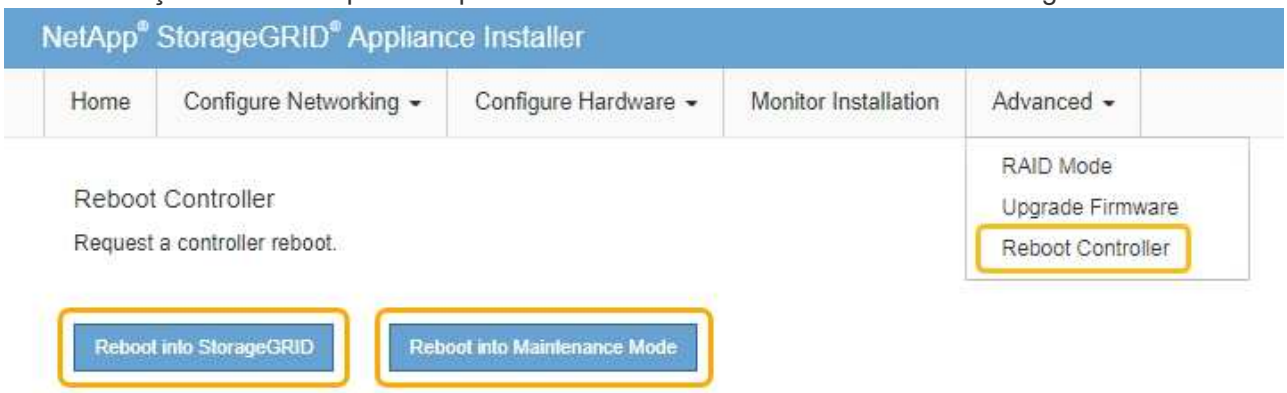
As alterações efetuadas nas definições de DNS são temporárias e perdem-se quando sai do modo de manutenção.

4. Quando estiver satisfeito com as definições de DNS temporárias, selecione **Guardar**.

   O nó usa as configurações do servidor DNS especificadas nesta página para se reconetar ao KMS, permitindo que os dados no nó sejam descriptografados.

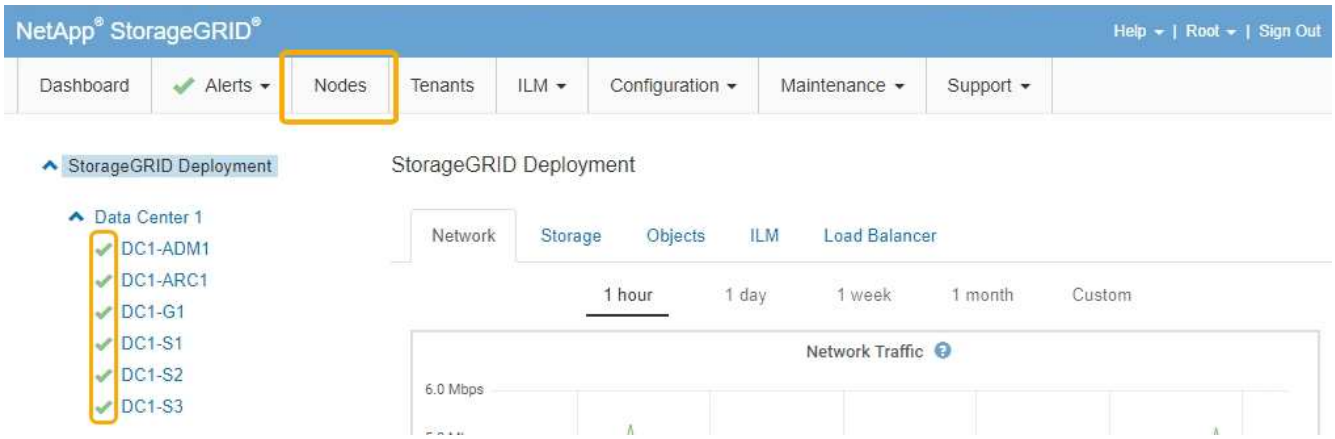
5. Depois que os dados do nó forem descriptografados, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Quando o nó reinicializa e realegra a grade, ele usa os servidores DNS de todo o sistema listados no Gerenciador de Grade. Depois de reingressar na grade, o dispositivo não usará mais os servidores DNS temporários especificados no Instalador de dispositivos StorageGRID enquanto o dispositivo estava no modo de manutenção.

Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Monitorização da encriptação do nó no modo de manutenção

Se você ativou a criptografia de nó para o dispositivo durante a instalação, poderá monitorar o status de criptografia de nó de cada nó do dispositivo, incluindo os detalhes do estado de criptografia de nó e do servidor de gerenciamento de chaves (KMS).

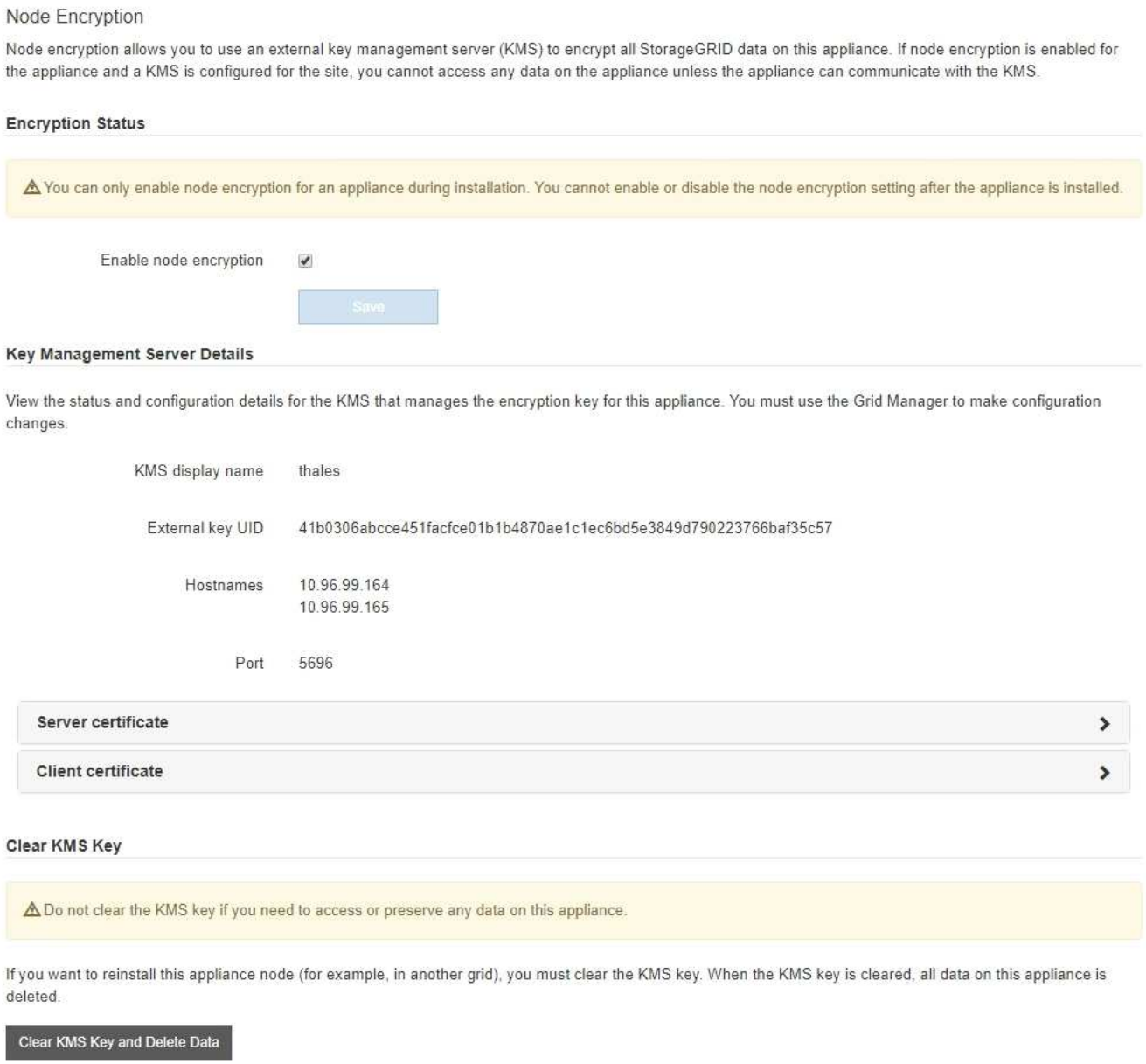
O que você vai precisar

- A criptografia do nó deve ter sido ativada para o dispositivo durante a instalação. Não é possível ativar a criptografia de nó depois que o dispositivo estiver instalado.
- O aparelho foi colocado no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Configurar hardware criptografia de nó**.



A página criptografia do nó inclui estas três seções:

- O estado de encriptação mostra se a encriptação do nó está ativada ou desativada para o dispositivo.
- Detalhes do servidor de gerenciamento de chaves mostra informações sobre o KMS sendo usado para criptografar o dispositivo. Você pode expandir as seções de certificado de servidor e cliente para exibir detalhes e status do certificado.
  - Para resolver problemas com os próprios certificados, como a renovação de certificados expirados, consulte as informações sobre o KMS nas instruções de administração do StorageGRID.
  - Se houver problemas inesperados ao se conetar aos hosts KMS, verifique se os servidores DNS (sistema de nomes de domínio) estão corretos e se a rede do appliance está configurada corretamente.

    "Verificar a configuração do servidor DNS"

  - Se você não conseguir resolver os problemas do certificado, entre em Contato com o suporte técnico.

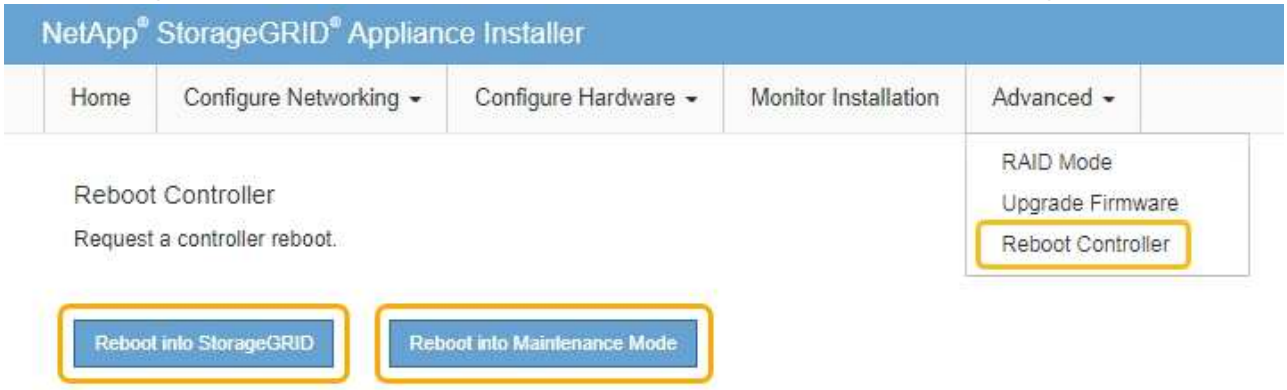
- Limpar chave KMS desativa a criptografia de nó para o dispositivo, remove a associação entre o dispositivo e o servidor de gerenciamento de chaves que foi configurado para o site StorageGRID e exclui todos os dados do dispositivo. Tem de limpar a chave KMS antes de poder instalar o aparelho noutro sistema StorageGRID.

  "Limpando a configuração do servidor de gerenciamento de chaves"

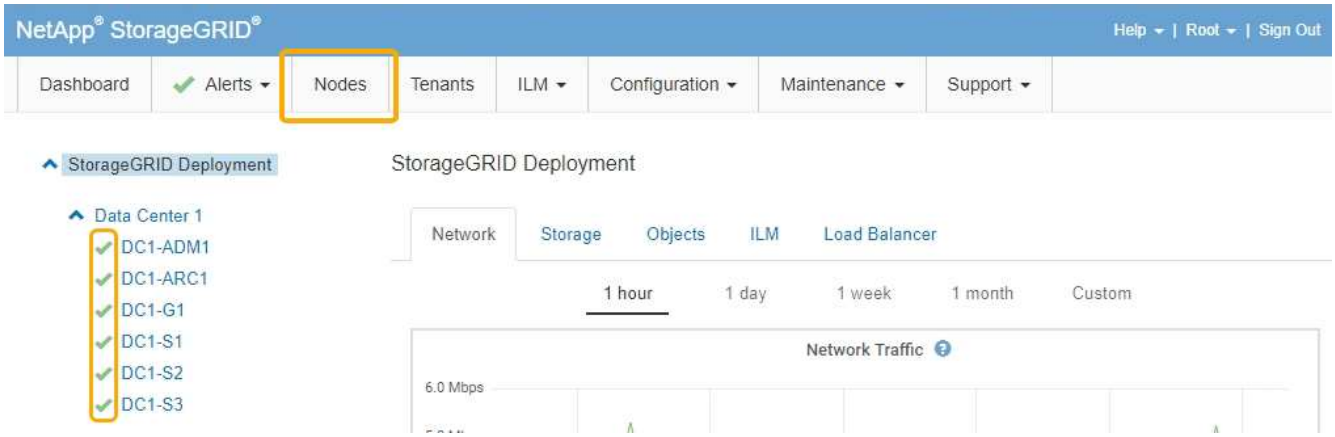
  Limpar a configuração do KMS exclui os dados do dispositivo, tornando-os permanentemente inacessíveis. Estes dados não são recuperáveis.

2. Quando terminar de verificar o estado da encriptação do nó, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Administrar o StorageGRID"

Limpando a configuração do servidor de gerenciamento de chaves

Limpar a configuração do servidor de gerenciamento de chaves (KMS) desativa a criptografia de nó no seu dispositivo. Depois de limpar a configuração do KMS, os dados do seu aparelho são excluídos permanentemente e não são mais acessíveis. Estes dados não são recuperáveis.

O que você vai precisar

Se você precisar preservar dados no dispositivo, você deve executar um procedimento de desativação de nós antes de limpar a configuração do KMS.

> Quando o KMS é eliminado, os dados no aparelho serão eliminados permanentemente e deixarão de estar acessíveis. Estes dados não são recuperáveis.

Desative o nó para mover quaisquer dados que ele contenha para outros nós no StorageGRID. Consulte as instruções de recuperação e manutenção para a desativação do nó da grade.

Sobre esta tarefa

A limpeza da configuração do KMS do appliance desativa a criptografia do nó, removendo a associação entre o nó do appliance e a configuração do KMS para o site do StorageGRID. Os dados no dispositivo são então excluídos e o dispositivo é deixado em um estado de pré-instalação. Este processo não pode ser revertido.

Você deve limpar a configuração do KMS:

- Antes de instalar o aparelho em outro sistema StorageGRID, isso não usa um KMS ou que usa um KMS diferente.

  > Não limpe a configuração do KMS se você planeja reinstalar um nó de dispositivo em um sistema StorageGRID que usa a mesma chave KMS.

- Antes de poder recuperar e reinstalar um nó onde a configuração do KMS foi perdida e a chave KMS não é recuperável.
- Antes de devolver qualquer aparelho que estava anteriormente em uso em seu site.
- Após a desativação de um dispositivo que tinha a criptografia de nó ativada.

> Desative o dispositivo antes de limpar o KMS para mover seus dados para outros nós em seu sistema StorageGRID. Limpar o KMS antes de desativar o aparelho resultará em perda de dados e pode tornar o aparelho inoperável.

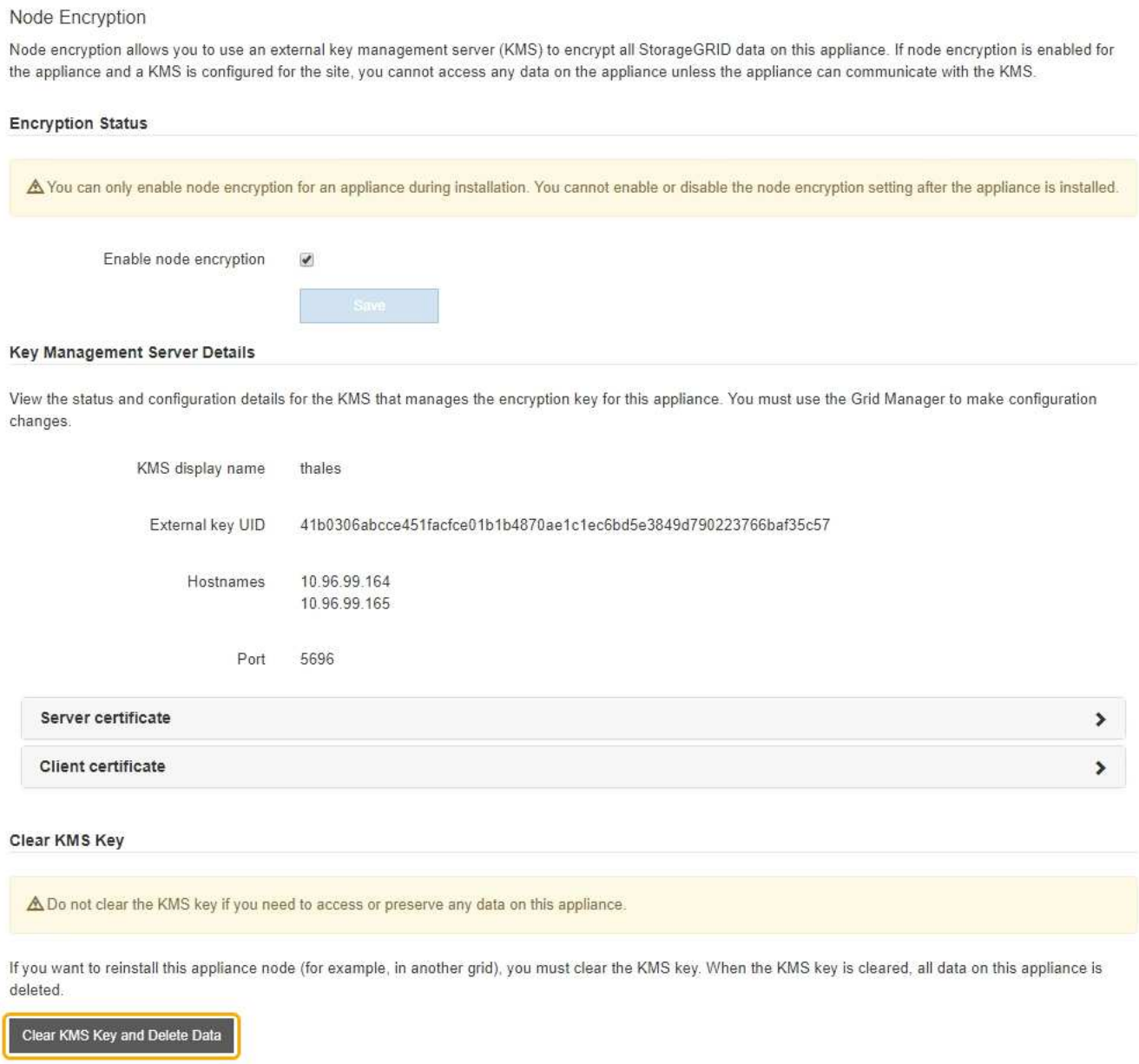
Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

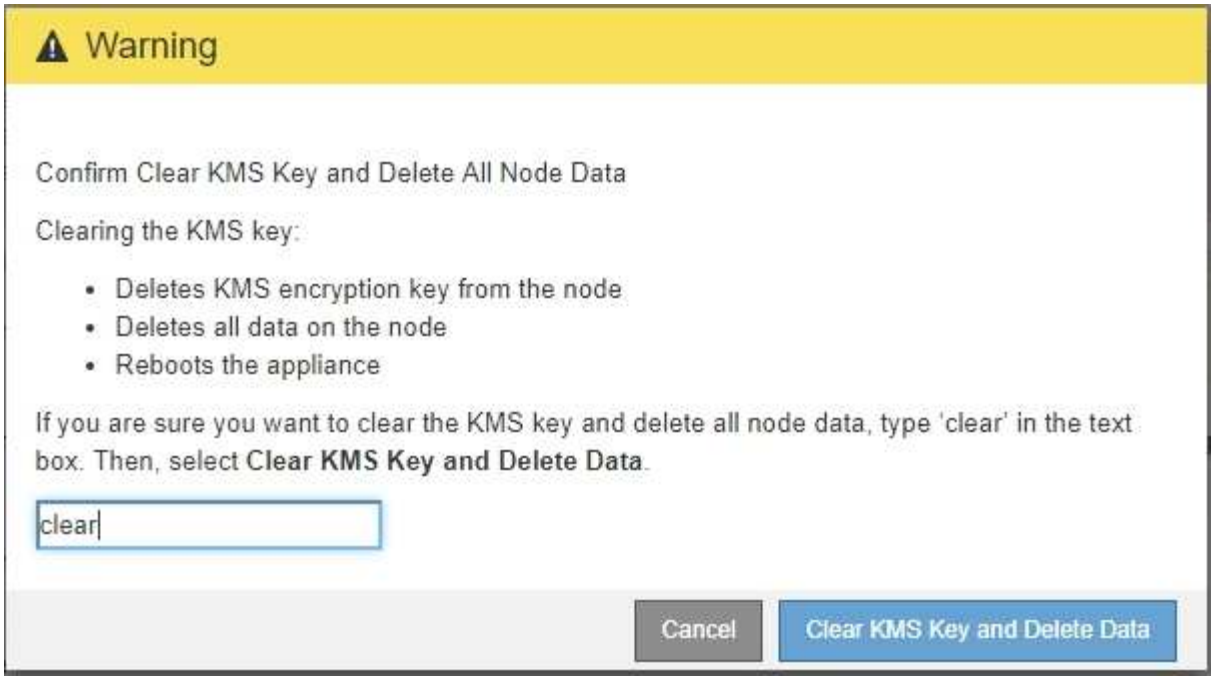
   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configure hardware Node Encryption**.



> Se a configuração do KMS for limpa, os dados no dispositivo serão excluídos permanentemente. Estes dados não são recuperáveis.

3. Na parte inferior da janela, selecione **Limpar chave KMS e Excluir dados**.
4. Se você tem certeza de que deseja limpar a configuração do KMS, digite **`clear`** e selecione **Limpar chave KMS e Excluir dados**.



A chave de criptografia KMS e todos os dados são excluídos do nó e o dispositivo é reinicializado. Isso pode levar até 20 minutos.

5. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

6. Selecione **Configure hardware Node Encryption**.
7. Verifique se a criptografia do nó está desativada e se as informações de chave e certificado em **Key Management Server Details** e **Clear KMS Key e Delete Data** control são removidas da janela.

   A criptografia do nó não pode ser reativada no dispositivo até que seja reinstalada em uma grade.

Depois de terminar

Depois de o aparelho reiniciar e verificar se o KMS foi limpo e se o aparelho está num estado de pré-instalação, pode remover fisicamente o aparelho do sistema StorageGRID. Consulte as instruções de recuperação e manutenção para obter informações sobre como preparar um aparelho para reinstalação.

Informações relacionadas

"Administrar o StorageGRID"

"Manter recuperar"

SG5700 dispositivos de armazenamento

Saiba como instalar e manter dispositivos StorageGRID SG5712 e SG5760.

- "Visão geral do dispositivo StorageGRID"

- "Visão geral da instalação e implantação"
- "Preparando-se para a instalação"
- "Instalar o hardware"
- "Configurar o hardware"
- "Implantando um nó de storage de dispositivos"
- "Monitorização da instalação do dispositivo de armazenamento"
- "Automatizando a instalação e a configuração do dispositivo"
- "Visão geral das APIs REST de instalação"
- "Solução de problemas da instalação do hardware"
- "Manutenção do aparelho SG5700"

Visão geral do dispositivo StorageGRID

O dispositivo SG5700 StorageGRID é uma plataforma de storage e computação integrada que opera como nó de storage em uma grade StorageGRID. O dispositivo pode ser usado em um ambiente de grade híbrida que combina nós de storage do dispositivo e nós de storage virtuais (baseados em software).

O dispositivo StorageGRID SG5700 oferece os seguintes recursos:

- Integra os elementos de storage e computação de um nó de storage da StorageGRID.
- Inclui o instalador do dispositivo StorageGRID para simplificar a implantação e a configuração do nó de storage.
- Inclui o e-Series SANtricity System Manager para gerenciamento e monitoramento de hardware.
- Suporta até quatro conexões de 10 GbE ou 25 GbE à rede de Grade StorageGRID e à rede de cliente.
- Compatível com unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS). Quando essas unidades são usadas com o recurso de Segurança da Unidade no Gerenciador de sistema do SANtricity, o acesso não autorizado aos dados é impedido.

O aparelho SG5700 está disponível em dois modelos: O SG5712 e o SG5760. Ambos os modelos incluem os seguintes componentes:

Componente	SG5712	SG5760
Controlador de computação	Controlador E5700SG	Controlador E5700SG
Controlador de storage	Controlador e-Series E2800	Controlador e-Series E2800
Chassis	Compartimento e-Series DE212C, um compartimento de duas unidades de rack (2UU)	Compartimento e-Series DE460C, um compartimento de quatro unidades de rack (4UU)
Unidades	Unidades NL-SAS de 12 TB (3,5 polegadas)	Unidades NL-SAS de 60 TB (3,5 polegadas)

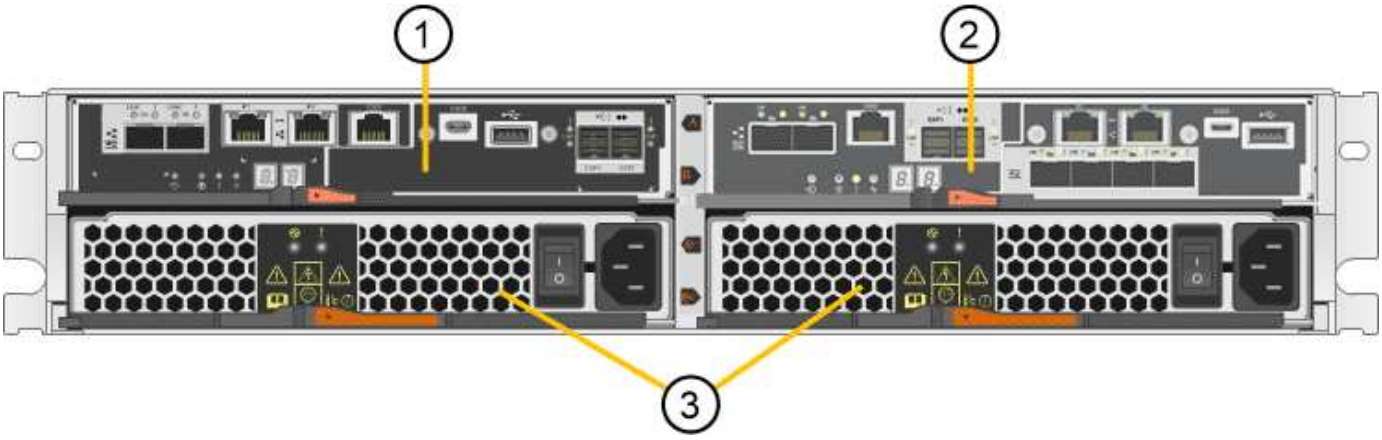
Componente	SG5712	SG5760
Fontes de alimentação e ventiladores redundantes	Dois coletores de ventilador de potência	Dois coletores de energia e dois coletores de ventilador

O storage bruto máximo disponível no dispositivo StorageGRID é fixo, com base no número de unidades em cada compartimento. Não é possível expandir o storage disponível adicionando uma gaveta com unidades adicionais.

Modelo SG5712

Esta figura mostra a parte frontal e traseira do modelo SG5712, um compartimento 2U com capacidade para 12 unidades.

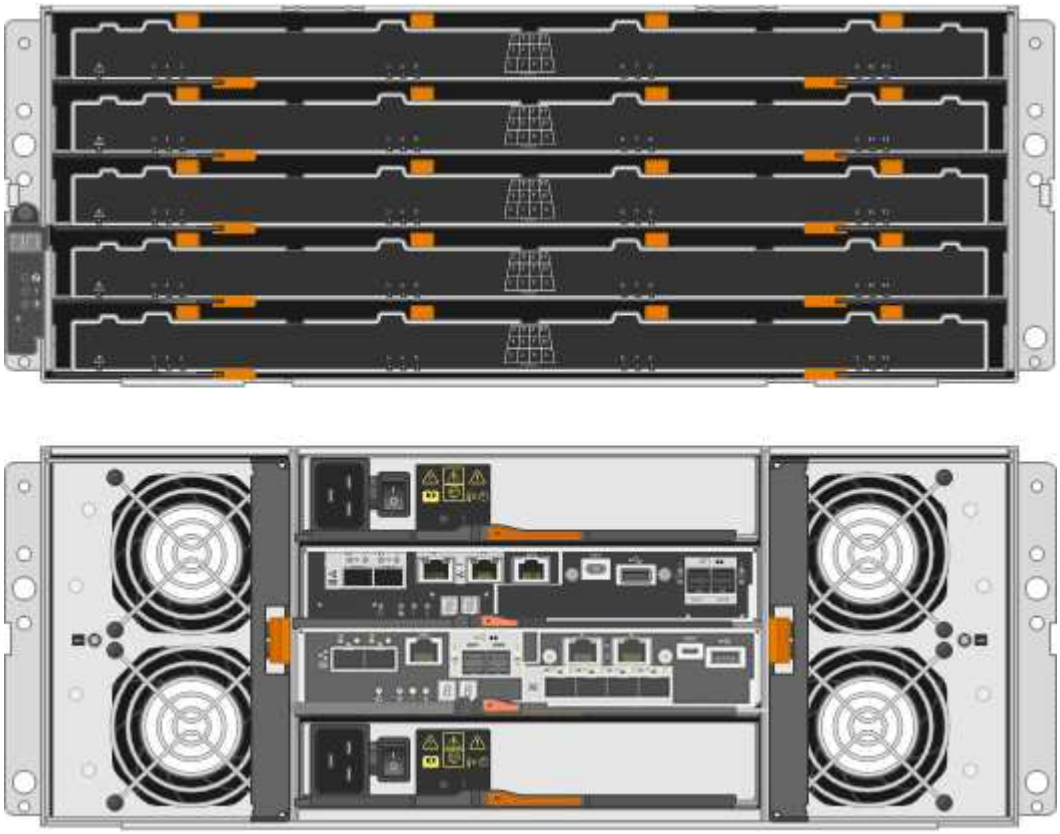
O SG5712 inclui dois controladores e dois coletores de ventilador.



	Descrição
1	Controlador E2800 (controlador de storage)
2	Controladora E5700SG (controlador de computação)
3	Coletores do ventilador de potência

Modelo SG5760

Esta figura mostra a parte frontal e traseira do modelo SG5760, um compartimento 4U que contém 60 unidades em 5 gavetas de unidade.



O SG5760 inclui dois controladores, dois coletores de ventilador e dois coletores de energia.

	Descrição
1	Controlador E2800 (controlador de storage)
2	Controladora E5700SG (controlador de computação)
3	Recipiente da ventoinha (1 de 2)
4	Recipiente de alimentação (1 de 2)

Informações relacionadas

"Site de Documentação de sistemas NetApp e-Series"

Controladores no dispositivo StorageGRID

Os modelos SG5712 e SG5760 do dispositivo StorageGRID incluem um controlador E5700SG e um controlador E2800. Você deve rever os diagramas para aprender as diferenças entre os controladores.

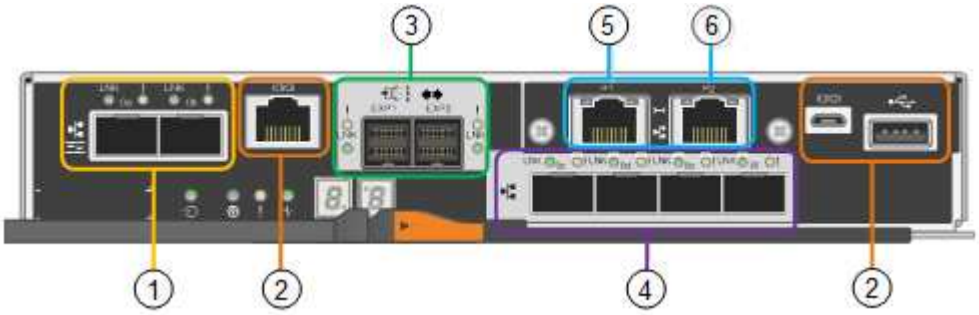
Controlador E5700SG

- Opera como o servidor de computação do dispositivo.
- Inclui o instalador do dispositivo StorageGRID.

> O software StorageGRID não está pré-instalado no dispositivo. Este software é acessado a partir do Admin Node quando você implantar o dispositivo.

- Pode se conetar a todas as três redes StorageGRID, incluindo a rede de Grade, a rede Admin e a rede cliente.
- Liga-se ao controlador E2800 e funciona como iniciador.

Esta figura mostra os conetores na parte de trás do controlador E5700SG.



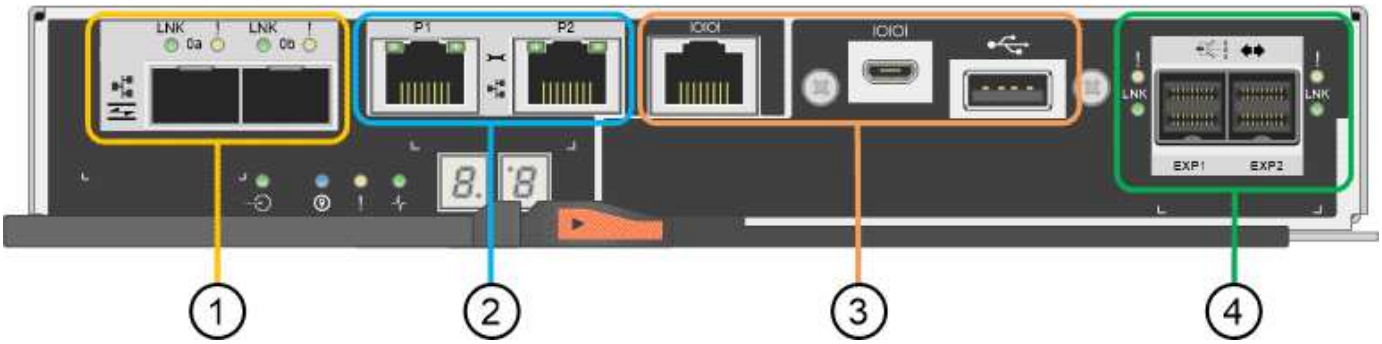
	Porta	Tipo	Utilização
1	Portas de interconexão 1 e 2	Canal de fibra (FC) de 16GB GB/s, SFPa ótico	Ligue o controlador E5700SG ao controlador E2800.
2	Portas de diagnóstico e suporte	• Porta serial RJ-45 • Porta serial micro USB • Porta de USB	Reservado para suporte técnico.
3	Portas de expansão da unidade	SAS de 12GB GB/s.	Não utilizado. Os dispositivos StorageGRID não são compatíveis com gavetas de unidades de expansão.
4	Portas de rede 1-4	10 GbE ou 25 GbE, com base no tipo de transcetor SFP, na velocidade do switch e na velocidade do link configurada	Conete-se à rede de grade e à rede de cliente para StorageGRID.
5	Porta de gerenciamento 1	Ethernet de 1 GB (RJ-45)	Conete-se à rede de administração para StorageGRID.

	Porta	Tipo	Utilização
6	Porta de gerenciamento 2	Ethernet de 1 GB (RJ-45)	Opções: • Vincular com a porta de gerenciamento 1 para uma conexão redundante com a rede de administração para StorageGRID. • Deixe desconetado e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, utilize a porta 2 para a configuração IP se os endereços IP atribuídos pelo DHCP não estiverem disponíveis.

Controlador E2800

- Funciona como o controlador de armazenamento do dispositivo.
- Gerencia o armazenamento de dados nas unidades.
- Funciona como um controlador padrão da série e no modo simplex.
- Inclui o software SANtricity os (firmware do controlador).
- Inclui o Gerenciador de sistema do SANtricity para monitorar o hardware do dispositivo e gerenciar alertas, o recurso AutoSupport e o recurso de segurança da unidade.
- Liga-se ao controlador E5700SG e funciona como alvo.

Esta figura mostra os conetores na parte de trás do controlador E2800.



	Porta	Tipo	Utilização
1	Portas de interconexão 1 e 2	SFPa ótico FC de 16GB GB/s	Ligue o controlador E2800 ao controlador E5700SG.

	Porta	Tipo	Utilização
2	Portas de gerenciamento 1 e 2	Ethernet de 1 GB (RJ-45)	• A porta 1 coneta-se à rede onde você acessa o Gerenciador de sistema do SANtricity em um navegador. • A porta 2 está reservada para uso de suporte técnico.
3	Portas de diagnóstico e suporte	• Porta serial RJ-45 • Porta serial micro USB • Porta de USB	Reservado para uso de suporte técnico.
4	Portas de expansão da unidade.	SAS de 12GB GB/s.	Não utilizado. Os dispositivos StorageGRID não são compatíveis com gavetas de unidades de expansão.

Visão geral da instalação e implantação

Você pode instalar um ou mais dispositivos StorageGRID quando implantar o StorageGRID pela primeira vez ou adicionar nós de storage do dispositivo posteriormente como parte de uma expansão. Você também pode precisar instalar um nó de armazenamento de dispositivos como parte de uma operação de recuperação.

Adicionar um dispositivo de storage StorageGRID a um sistema StorageGRID inclui quatro etapas principais:

1. Preparação para a instalação:
   - Preparar o local de instalação
   - Desembalar as caixas e verificar o conteúdo
   - Obtenção de equipamentos e ferramentas adicionais
   - Recolha de endereços IP e informações de rede
   - Opcional: Configurando um servidor de gerenciamento de chaves externo (KMS) se você planeja criptografar todos os dados do dispositivo. Consulte detalhes sobre o gerenciamento de chaves externas nas instruções de administração do StorageGRID.
2. Instalar o hardware:
   - Registar o hardware
   - Instalar o aparelho num armário ou num rack
   - Instalar as unidades (apenas SG5760)
   - Fazer o cabeamento do dispositivo
   - Conexão dos cabos de energia e alimentação
   - Exibindo códigos de status de inicialização
3. Configurar o hardware:

- Acessando o Gerenciador de sistema do SANtricity, definindo um endereço IP estático para a porta de gerenciamento 1 no controlador E2800 e configurando as configurações do Gerenciador de sistema do SANtricity
- Acessando o Instalador do StorageGRID Appliance e configurando as configurações de IP de rede e link necessárias para se conetar a redes StorageGRID
- Opcional: Habilitando a criptografia de nó se você planeja usar um KMS externo para criptografar dados do dispositivo.
- Opcional: Alterar o modo RAID.

4. Implantando o dispositivo como nó de storage:

Tarefa	Instruções
Implantando um nó de storage de dispositivos em um novo sistema StorageGRID	"Implantando um nó de storage de dispositivos"
Adicionando um nó de storage de dispositivo a um sistema StorageGRID existente	Instruções para expandir um sistema StorageGRID
Implantando um nó de storage de dispositivos como parte de uma operação de recuperação de nó de storage	Instruções para recuperação e manutenção

Informações relacionadas

"Preparando-se para a instalação"

"Instalar o hardware"

"Configurar o hardware"

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Aparelhos de serviços SG100 SG1000"

"Expanda sua grade"

"Manter recuperar"

"Administrar o StorageGRID"

Preparando-se para a instalação

Preparar a instalação de um dispositivo StorageGRID implica preparar o local e obter todo o hardware, cabos e ferramentas necessários. Você também deve coletar endereços IP e informações de rede.

Passos

- "Preparação do local (SG5700)"
- "Desembalar as caixas (SG5700)"
- "Obtenção de equipamentos e ferramentas adicionais (SG5700)"
- "Requisitos do navegador da Web"
- "Rever as ligações de rede do dispositivo"
- "Recolha de informações de instalação (SG5700)"

Preparação do local (SG5700)

Antes de instalar o aparelho, certifique-se de que o local e o gabinete ou rack que pretende utilizar cumprem as especificações de um dispositivo StorageGRID.

Passos

1. Confirme se o local atende aos requisitos de temperatura, umidade, faixa de altitude, fluxo de ar, dissipação de calor, fiação, energia e aterramento. Consulte o NetApp Hardware Universe para obter mais informações.
2. Se estiver a instalar o modelo SG5760, confirme se a sua localização fornece alimentação CA de 240 volts.
3. Obtenha um gabinete ou rack de 19 polegadas (48,3 cm) para encaixar prateleiras deste tamanho (sem cabos):

Modelo do aparelho	Altura	Largura	Profundidade	Peso máximo
SG5712 (12 unidades)	3,41 pol. (8,68 cm)	17,6 pol. (44,7 cm)	21,1 pol. (53,6 cm)	13 63,9 lb (29,0 kg)
SG5760 (60 unidades)	6,87 pol. (17,46 cm)	17,66 pol. (44,86 cm)	38,25 pol. (97,16 cm)	13 250 lb. (113 kg)

4. Instale todos os switches de rede necessários. Consulte a ferramenta de Matriz de interoperabilidade do NetApp para obter informações sobre compatibilidade.

Informações relacionadas

"NetApp Hardware Universe"

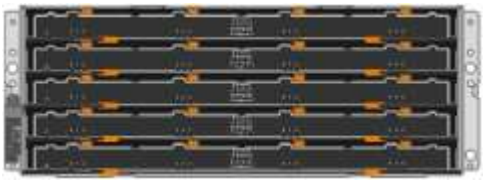
"Ferramenta de Matriz de interoperabilidade do NetApp"

Desembalar as caixas (SG5700)

Antes de instalar o dispositivo StorageGRID, desembale todas as caixas e compare o conteúdo com os itens no saco de embalagem.

- * SG5712 dispositivo com 12 unidades instaladas*

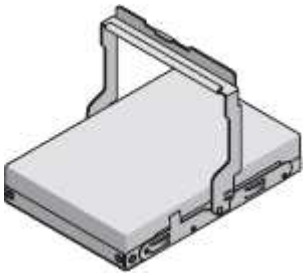
- * SG5760 dispositivo sem unidades instaladas*



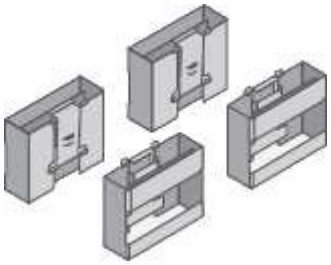
- **Moldura frontal para o aparelho**

- **Kit de trilho com instruções**

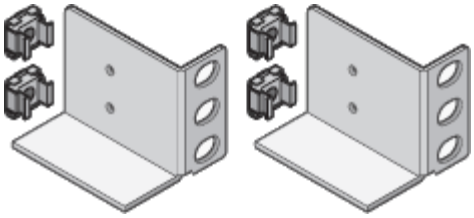
- **SG5760: Sessenta unidades**



- **SG5760: Alças**



- * SG5760: Suportes traseiros e porcas de gaiola para instalação de rack de furo quadrado*



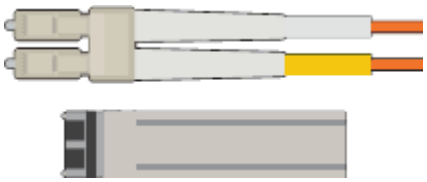
Cabos e conetores

O envio para o dispositivo StorageGRID inclui os seguintes cabos e conetores:

- * Dois cabos de alimentação para o seu país*

O gabinete pode ter cabos de alimentação especiais que você usa em vez dos cabos de alimentação fornecidos com o aparelho.

- * Cabos óticos e transcetores SFP*



Dois cabos óticos para as portas de interconexão FC

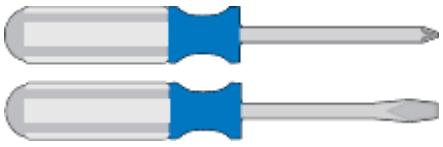
Oito transcetores SFP mais, compatíveis com as quatro portas de interconexão FC de 16GB GB/s e as quatro portas de rede de 10 GbE

Obtenção de equipamentos e ferramentas adicionais (SG5700)

Antes de instalar o dispositivo StorageGRID, confirme se tem todo o equipamento e ferramentas adicionais de que necessita.

Você precisa do seguinte equipamento adicional para instalar e configurar o hardware:

- **Chaves de fenda**

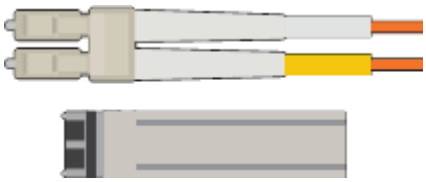


Chave de fendas Phillips n.o 2

Chave de parafusos plana média

- * Pulseira antiestática*

- * Cabos óticos e transcetores SFP*



Cabos óticos para as portas de 10/25 GbE que você planeja usar

Opcional: SFP28 transcetores se você quiser usar a velocidade de link de 25 GbE

- **Cabos Ethernet**

- * Serviço de laptop*

Navegador da Web suportado

Cliente SSH, como PuTTY

Porta Ethernet de 1 GB (RJ-45)

- **Ferramentas opcionais**

Broca elétrica com ponta Phillips

Lanterna

Elevador mecanizado para SG5760

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Rever as ligações de rede do dispositivo

Antes de instalar o dispositivo StorageGRID, você deve entender quais redes podem ser conetadas ao dispositivo e como as portas em cada controlador são usadas.

Redes de dispositivos StorageGRID

Ao implantar um dispositivo StorageGRID como nó de storage em uma grade StorageGRID, você pode conectá-lo às seguintes redes:

- **Rede de grade para StorageGRID**: A rede de grade é usada para todo o tráfego interno de StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes. A rede de Grade é necessária.
- **Rede de administração para StorageGRID**: A rede de administração é uma rede fechada usada para administração e manutenção do sistema. A rede Admin é normalmente uma rede privada e não precisa

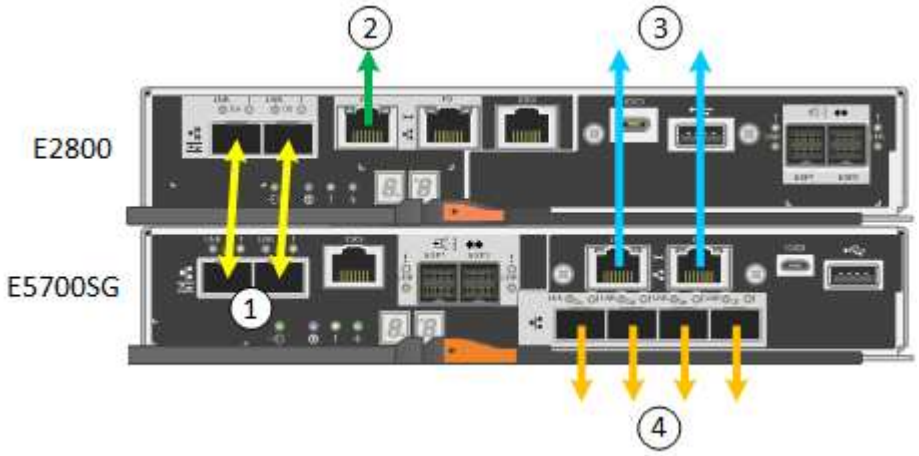
ser roteável entre sites. A rede de administração é opcional.

- **Rede de clientes para StorageGRID:** a rede de clientes é uma rede aberta usada para fornecer acesso a aplicativos clientes, incluindo S3 e Swift. A rede do cliente fornece acesso ao protocolo do cliente à grade, de modo que a rede da grade possa ser isolada e protegida. A rede do cliente é opcional.
- **Rede de gerenciamento para o Gerenciador de sistema SANtricity**: Essa rede fornece acesso ao Gerenciador de sistema SANtricity no controlador E2800, permitindo que você monitore e gerencie os componentes de hardware no dispositivo. Essa rede de gerenciamento pode ser a mesma rede de administração para StorageGRID ou pode ser uma rede de gerenciamento independente.

Para obter informações detalhadas sobre redes StorageGRID, consulte *Primer*.

Conexões de dispositivos StorageGRID

Ao instalar um dispositivo StorageGRID, você deve conetar os dois controladores entre si e às redes necessárias. A figura mostra os dois controladores no SG5760, com o controlador E2800 na parte superior e o controlador E5700SG na parte inferior. No SG5712, o controlador E2800 está à esquerda do controlador E5700SG.



	Porta	Tipo de porta	Função
1	Duas portas de interconexão em cada controlador	SFP ótico FC de 16GB GB/s.	Conete os dois controladores um ao outro.
2	Porta de gerenciamento 1 no controlador E2800	1 GbE (RJ-45)	Liga-se à rede onde acede ao Gestor de sistema SANtricity. Pode utilizar a rede de administração para StorageGRID ou uma rede de gestão independente.
2	Porta de gerenciamento 2 no controlador E2800	1 GbE (RJ-45)	Reservado para suporte técnico.
3	Porta de gerenciamento 1 no controlador E5700SG	1 GbE (RJ-45)	Liga o controlador E5700SG à rede de administração para StorageGRID.

	Porta	Tipo de porta	Função
3	Porta de gerenciamento 2 no controlador E5700SG	1 GbE (RJ-45)	• Pode ser ligado com a porta de gerenciamento 1 se você quiser uma conexão redundante com a rede de administração. • Pode ser deixado sem fios e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, pode ser utilizado para ligar o controlador E5700SG a um computador portátil de serviço se os endereços IP atribuídos por DHCP não estiverem disponíveis.
4	Portas 10/25-GbE 1-4 na controladora E5700SG	10-GbE ou 25-GbE **Observação:** os transcetores SFP incluídos com o dispositivo suportam velocidades de link de 10 GbE. Se você quiser usar velocidades de link de 25 GbE para as quatro portas de rede, você deve fornecer transcetores de SFP28 GbE.	Conete-se à rede de grade e à rede de cliente para StorageGRID. Consulte ""conexões de porta 10/25-GbE para o controlador E5700SG".

Informações relacionadas

"Recolha de informações de instalação (SG5700)"

"Cabeamento do aparelho (SG5700)"

"Modos de ligação de porta para E5700SG portas de controlador"

"Diretrizes de rede"

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Modos de ligação de porta para E5700SG portas de controlador

Ao configurar links de rede para as portas do controlador E5700SG, você pode usar a ligação de portas para as portas 10/25-GbE que se conetam à rede de Grade e à rede cliente opcional, e as portas de gerenciamento de 1 GbE que se conetam à rede Admin opcional. A ligação de portas ajuda a proteger os seus dados fornecendo caminhos

redundantes entre as redes StorageGRID e o dispositivo.

Informações relacionadas

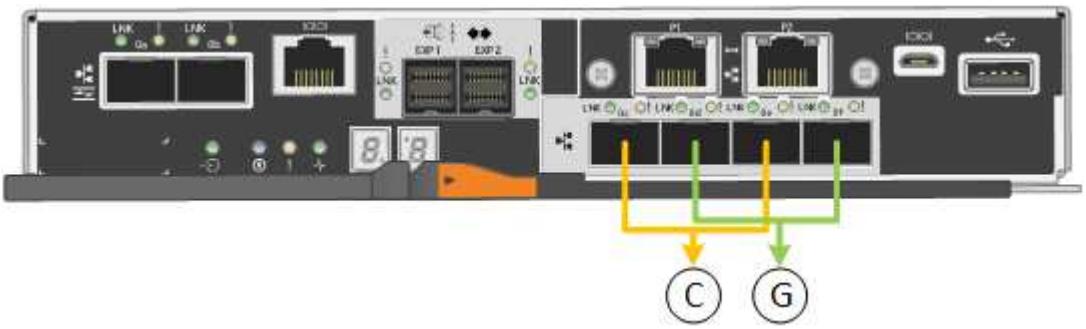
"Configurando links de rede (SG5700)"

Modos de ligação de rede para as portas 10/25-GbE

As portas de rede 10/25-GbE no controlador E5700SG suportam o modo de ligação de porta fixa ou o modo de ligação de porta agregada para as conexões de rede de Grade e rede de Cliente.

Modo de ligação de porta fixa

O modo fixo é a configuração padrão para as portas de rede 10/25-GbE.



	Quais portas estão coladas
C	As portas 1 e 3 são Unidas para a rede do cliente, se esta rede for utilizada.
G	As portas 2 e 4 são Unidas para a rede de Grade.

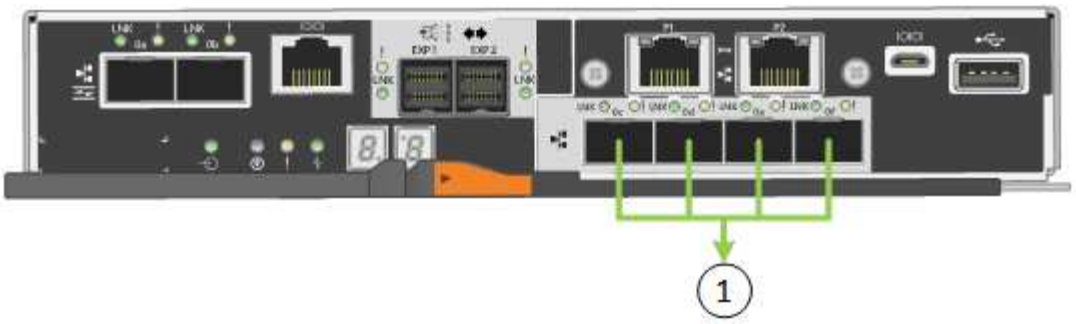
Ao usar o modo de ligação de porta fixa, você pode usar um dos dois modos de ligação de rede: Ative-Backup ou Link Aggregation Control Protocol (LACP).

- No modo ative-Backup (predefinição), apenas uma porta está ativa de cada vez. Se a porta ativa falhar, sua porta de backup fornecerá automaticamente uma conexão de failover. A porta 4 fornece um caminho de backup para a porta 2 (rede de Grade) e a porta 3 fornece um caminho de backup para a porta 1 (rede de cliente).
- No modo LACP, cada par de portas forma um canal lógico entre o controlador e a rede, permitindo maior produtividade. Se uma porta falhar, a outra continua a fornecer o canal. A taxa de transferência é reduzida, mas a conetividade não é afetada.

> Se não precisar de ligações redundantes, pode utilizar apenas uma porta para cada rede. No entanto, esteja ciente de que um alarme será gerado no Gerenciador de Grade após a instalação do StorageGRID, indicando que um cabo está desconetado. Pode reconhecer este alarme em segurança para o limpar.

Modo de ligação de porta agregada

O modo de ligação de porta agregada aumenta significativamente o em toda a rede StorageGRID e fornece caminhos de failover adicionais.



	Quais portas estão coladas
1	Todas as portas conetadas são agrupadas em uma única ligação LACP, permitindo que todas as portas sejam usadas para o tráfego de rede de Grade e rede de Cliente.

Se você planeja usar o modo de ligação de porta agregada:

- Você deve usar o modo de ligação de rede LACP.
- Você deve especificar uma tag VLAN exclusiva para cada rede. Essa tag VLAN será adicionada a cada pacote de rede para garantir que o tráfego de rede seja roteado para a rede correta.
- As portas devem ser conetadas a switches que possam suportar VLAN e LACP. Se vários switches estiverem participando da ligação LACP, os switches devem suportar grupos de agregação de links de vários gabinetes (MLAG) ou equivalente.
- Você deve entender como configurar os switches para usar VLAN, LACP e MLAG, ou equivalente.

Se você não quiser usar todas as quatro portas 10/25 GbE, poderá usar uma, duas ou três portas. O uso de mais de uma porta maximiza a chance de que alguma conetividade de rede permaneça disponível se uma das portas 10/25-GbE falhar.

> Se você optar por usar menos de quatro portas, esteja ciente de que um ou mais alarmes serão levantados no Gerenciador de Grade após a instalação do StorageGRID, indicando que os cabos estão desconetados. Você pode reconhecer os alarmes com segurança para limpá-los.

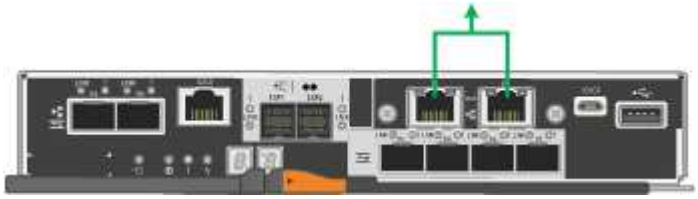
Modos de ligação de rede para as portas de gerenciamento de 1 GbE

Para as duas portas de gerenciamento de 1 GbE no controlador E5700SG, você pode escolher o modo de ligação de rede independente ou o modo de ligação de rede ative-Backup para se conetar à rede Admin opcional.

No modo independente, apenas a porta de gerenciamento 1 está conetada à rede de administração. Este modo não fornece um caminho redundante. A porta de gerenciamento 2 é deixada desconetada e disponível para conexões locais temporárias (use o endereço IP 169.254.0.1)

No modo ative-Backup, as portas de gerenciamento 1 e 2 estão conetadas à rede de administração. Apenas uma porta está ativa de cada vez. Se a porta ativa falhar, sua porta de backup fornecerá automaticamente uma conexão de failover. A ligação dessas duas portas físicas em uma porta de gerenciamento lógico fornece um caminho redundante para a rede de administração.

Se você precisar fazer uma conexão local temporária ao controlador E5700SG quando as portas de gerenciamento de 1 GbE estiverem configuradas para o modo ative-Backup, remova os cabos de ambas as portas de gerenciamento, conete o cabo temporário à porta de gerenciamento 2 e acesse o dispositivo usando o endereço IP 169.254.0.1.



Recolha de informações de instalação (SG5700)

À medida que você instala e configura o dispositivo StorageGRID, você deve tomar decisões e coletar informações sobre portas de switch Ethernet, endereços IP e modos de ligação de porta e rede.

Sobre esta tarefa

Você pode usar as tabelas a seguir para gravar as informações necessárias para cada rede conetada ao aparelho. Esses valores são necessários para instalar e configurar o hardware.

Informações necessárias para se conetar ao Gerenciador de sistemas SANtricity no controlador E2800

Você deve conetar o controlador E2800 à rede de gerenciamento que você usará para o Gerenciador de sistema do SANtricity.

Informações necessárias	O seu valor
Porta do switch Ethernet, você se conetará à porta de gerenciamento 1	
Endereço MAC da porta de gerenciamento 1 (impresso em uma etiqueta próxima à porta P1)	
Endereço IP atribuído pelo DHCP para a porta de gerenciamento 1, se disponível após a ativação **Observação:** se a rede que você se conetará ao controlador E2800 incluir um servidor DHCP, o administrador da rede poderá usar o endereço MAC para determinar o endereço IP atribuído pelo servidor DHCP.	
Velocidade e modo duplex **Observação:** você deve certificar-se de que o switch Ethernet da rede de gerenciamento do Gerenciador de sistema do SANtricity esteja definido como negociação automática.	Deve ser: • Negociação automática (padrão)

Informações necessárias	O seu valor
Formato do endereço IP	Escolha uma: • IPv4 • IPv6
Endereço IP estático que pretende utilizar para o dispositivo na rede de gestão	Para IPv4: • Endereço IPv4: • Máscara de sub-rede: • Gateway: Para IPv6: • Endereço IPv6: • Endereço IP roteável: • Endereço IP do router do controlador E2800:

Informações necessárias para conetar o controlador E5700SG à rede de administração

A rede de administração para StorageGRID é uma rede opcional, usada para administração e manutenção do sistema. O dispositivo se coneta à rede Admin usando as portas de gerenciamento de 1 GbE no controlador E5700SG.

Informações necessárias	O seu valor
Rede de administração ativada	Escolha uma: • Não • Sim (predefinição)
Modo de ligação de rede	Escolha uma: • Independente • Ative-Backup
Porta do switch para a porta 1	
Porta do switch para a porta 2 (apenas modo de ligação de rede ative-Backup)	

Informações necessárias	O seu valor
Endereço IP atribuído pelo DHCP para a porta de gerenciamento 1, se disponível após a ativação **Observação:** se a rede Admin incluir um servidor DHCP, o controlador E5700SG exibirá o endereço IP atribuído pelo DHCP em sua tela de sete segmentos depois que ele for inicializado. Você também pode determinar o endereço IP atribuído pelo DHCP usando o endereço MAC para procurar o IP atribuído.	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede de administração **Nota:** se a rede não tiver um gateway, especifique o mesmo endereço IPv4 estático para o gateway.	• Endereço IPv4 (CIDR): • Gateway:
Sub-redes de rede Admin (CIDR)	

Informações necessárias para conetar e configurar as portas 10/25-GbE no controlador E5700SG

As quatro portas 10/25-GbE no controlador E5700SG conetam-se à rede de Grade StorageGRID e à rede do cliente.

Consulte "conexões de porta 10/25-GbE para o controlador E5700SG" para obter mais informações sobre as opções dessas portas.

Informações necessárias	O seu valor
Velocidade da ligação **Nota:** se você selecionar 25 GbE, você deve instalar SPF28 transcetores. A negociação automática não é suportada, portanto você também deve configurar as portas e os switches conetados para 25GbE.	Escolha uma: • 10 GbE (padrão) • 25 GbE
Modo de ligação da porta	Escolha uma: • Fixo (padrão) • Agregado
Porta do switch para a porta 1 (rede do cliente)	
Porta do switch para a porta 2 (rede de grade)	
Porta do switch para a porta 3 (rede do cliente)	

Informações necessárias	O seu valor
Porta do switch para a porta 4 (rede de grade)	

Informações necessárias para conetar o controlador E5700SG à rede de Grade

A rede de Grade para StorageGRID é uma rede necessária, usada para todo o tráfego interno de StorageGRID. O dispositivo se coneta à rede de Grade usando as portas 10/25-GbE no controlador E5700SG.

Consulte "conexões de porta 10/25-GbE para o controlador E5700SG" para obter mais informações sobre as opções dessas portas.

Informações necessárias	O seu valor
Modo de ligação de rede	Escolha uma: • Ative-Backup (padrão) • Bola de Futsal (802,3ad)
Marcação de VLAN ativada	Escolha uma: • Não (predefinição) • Sim
Tag VLAN (se a marcação VLAN estiver ativada)	Introduza um valor entre 0 e 4095:
Endereço IP atribuído pelo DHCP para a rede de Grade, se disponível após a ativação **Observação:** se a rede de Grade incluir um servidor DHCP, o controlador E5700SG exibirá o endereço IP atribuído pelo DHCP para a rede de Grade em sua tela de sete segmentos após a inicialização.	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede de grelha **Nota:** se a rede não tiver um gateway, especifique o mesmo endereço IPv4 estático para o gateway.	• Endereço IPv4 (CIDR): • Gateway:
Sub-redes de rede de rede (CIDR) **Nota:** se a rede do cliente não estiver ativada, a rota padrão no controlador usará o gateway especificado aqui.	

Informações necessárias para conetar o controlador E5700SG à rede do cliente

A rede de cliente para StorageGRID é uma rede opcional, normalmente usada para fornecer acesso de protocolo de cliente à grade. O dispositivo se coneta à rede do cliente usando as portas 10/25-GbE no

controlador E5700SG.

Consulte "conexões de porta 10/25-GbE para o controlador E5700SG" para obter mais informações sobre as opções dessas portas.

Informações necessárias	O seu valor
Rede cliente ativada	Escolha uma: • Não (predefinição) • Sim
Modo de ligação de rede	Escolha uma: • Ative-Backup (padrão) • Bola de Futsal (802,3ad)
Marcação de VLAN ativada	Escolha uma: • Não (predefinição) • Sim
Etiqueta VLAN (Se a marcação VLAN estiver ativada)	Introduza um valor entre 0 e 4095:
Endereço IP atribuído pelo DHCP para a rede do cliente, se disponível após a ligação	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede do cliente **Nota:** se a rede do cliente estiver ativada, a rota padrão no controlador usará o gateway especificado aqui.	• Endereço IPv4 (CIDR): • Gateway:

Informações relacionadas

"Rever as ligações de rede do dispositivo"

"Modos de ligação de porta para E5700SG portas de controlador"

"Configurar o hardware"

Instalar o hardware

A instalação de hardware implica a instalação do aparelho em um gabinete ou rack, a conexão dos cabos e a aplicação de energia.

Passos

- "Registar o hardware"
- "Instalar o aparelho em um gabinete ou rack (SG5700)"
- "Cabeamento do aparelho (SG5700)"
- "Conexão dos cabos de alimentação e alimentação de energia (SG5700)"
- "Exibindo códigos de status de inicialização do SG5700"

Registar o hardware

Registrar o hardware do aparelho fornece benefícios de suporte.

Passos

1. Localize o número de série do chassi.

   Pode encontrar o número no folheto de embalagem, no seu e-mail de confirmação ou no aparelho depois de o desembalar.

2. Vá para o site de suporte da NetApp em "mysupport.NetApp.com".
3. Determine se você precisa Registrar o hardware:

Se você é um…	Siga estes passos…
Cliente NetApp existente	a. Inicie sessão com o seu nome de utilizador e palavra-passe. b. Selecione **Produtos Meus Produtos**. c. Confirme se o novo número de série está listado. d. Se não estiver, siga as instruções para novos clientes NetApp.
Novo cliente da NetApp	a. Clique em **Registe-se agora** e crie uma conta. b. Selecione **Produtos Registe produtos**. c. Insira o número de série do produto e os detalhes solicitados. Após a aprovação do seu registo, pode transferir qualquer software necessário. O processo de aprovação pode demorar até 24 horas.

Instalar o aparelho em um gabinete ou rack (SG5700)

Tem de instalar calhas no armário ou no rack e, em seguida, deslizar o aparelho sobre os trilhos. Se você tiver um SG5760, você também deve instalar as unidades depois de instalar o aparelho.

O que você vai precisar

- Você revisou o documento de Avisos de segurança incluído na caixa e entendeu as precauções para mover e instalar hardware.
- Você tem as instruções fornecidas com o kit de trilho.
- Você tem as *instruções de instalação e configuração* para o aparelho.

> Instale o hardware a partir da parte inferior do rack ou gabinete ou rack para cima para evitar que o equipamento tombe.

> O SG5712 pesa aproximadamente 64 lb (29 kg) quando totalmente carregado com unidades. Duas pessoas ou um elevador mecanizado são necessários para mover com segurança o SG5712.

> O SG5760 pesa aproximadamente 132 lb (60 kg) sem unidades instaladas. Quatro pessoas ou um elevador mecanizado são necessários para mover com segurança um SG5760 vazio.

> Para evitar danificar o hardware, nunca mova um SG5760 se as unidades estiverem instaladas. É necessário remover todas as unidades antes de mover a gaveta.

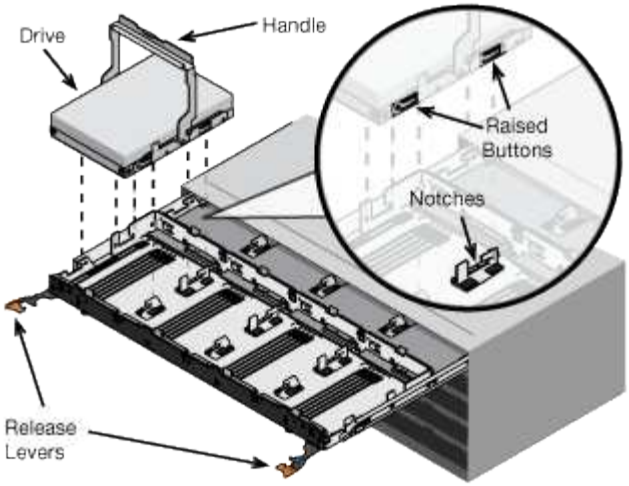
Passos

1. Siga cuidadosamente as instruções para o kit de trilho para instalar os trilhos em seu gabinete ou rack.
2. Se tiver um SG5760, siga estes passos para se preparar para mover o aparelho.
   a. Retire a caixa de embalagem exterior. Em seguida, dobre as abas na caixa interna.
   b. Se estiver a levantar o SG5760 manualmente, fixe as quatro pegas nas laterais do chassis.

      Retire estas pegas enquanto desliza o aparelho sobre os trilhos.
3. Consulte as *instruções de instalação e configuração* e deslize o aparelho para dentro do gabinete ou rack.
4. Consulte as *instruções de instalação e configuração* e fixe o aparelho ao gabinete ou rack.

   Se tiver um SG5760, utilize os suportes traseiros para fixar o aparelho à parte de trás do rack ou armário. Use as porcas da gaiola se seu rack ou gabinete tiver orifícios quadrados.
5. Se você tiver um SG5760, instale 12 unidades em cada uma das 5 gavetas de unidade.

   Você deve instalar todas as unidades 60 para garantir o funcionamento correto.
   a. Coloque a pulseira ESD e remova as unidades da embalagem.
   b. Solte as alavancas na gaveta superior da unidade e deslize a gaveta para fora usando as alavancas.
   c. Levante a alça da unidade para a vertical e alinhe os botões da unidade com os entalhes na gaveta.



d. Pressionando suavemente a parte superior da unidade, gire a alça da unidade para baixo até que ela se encaixe no lugar.

e. Depois de instalar as primeiras 12 unidades, deslize a gaveta para dentro, empurrando o centro e fechando ambas as alavancas com cuidado.

f. Repita estes passos para as outras quatro gavetas.

6. Fixe a moldura frontal.

Cabeamento do aparelho (SG5700)

Você deve conetar os dois controladores um ao outro, conetar as portas de gerenciamento em cada controlador e conetar as portas 10/25-GbE do controlador E5700SG à rede de Grade e à rede de cliente opcional para StorageGRID.

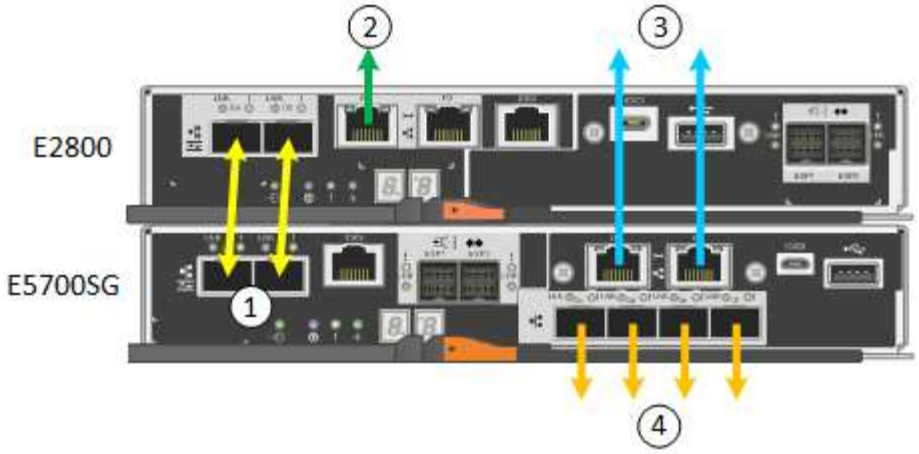
O que você vai precisar

- Desembalou os seguintes itens, que estão incluídos no aparelho:
  - Dois cabos de energia.
  - Dois cabos óticos para as portas de interconexão FC nas controladoras.
  - Oito transcetores SFP mais, que suportam FC de 10 GbE ou 16 Gbps. Os transcetores podem ser usados com as duas portas de interconexão em ambos os controladores e com as quatro portas de rede 10/25-GbE no controlador E5700SG, supondo que você queira que as portas de rede usem uma velocidade de link de 10 GbE.
- Obteve os seguintes itens, que não estão incluídos no aparelho:
  - Um a quatro cabos óticos para as portas de 10/25 GbE que você planeja usar.
  - Um a quatro transcetores SFP28, se você planeja usar a velocidade de link de 25 GbE.
  - Cabos Ethernet para conexão das portas de gerenciamento.

Risco de exposição à radiação laser — não desmonte nem remova qualquer parte de um transcetor SFP. Você pode estar exposto à radiação laser.

Sobre esta tarefa

A figura mostra os dois controladores no SG5760, com o controlador E2800 na parte superior e o controlador E5700SG na parte inferior. No SG5712, o controlador E2800 fica à esquerda do controlador E5700SG quando visto a partir da parte de trás.



	Porta	Tipo de porta	Função
1	Duas portas de interconexão em cada controlador	SFP ótico FC de 16GB GB/s.	Conete os dois controladores um ao outro.
2	Porta de gerenciamento 1 no controlador E2800	1 GbE (RJ-45)	Liga-se à rede onde acede ao Gestor de sistema SANtricity. Pode utilizar a rede de administração para StorageGRID ou uma rede de gestão independente.
2	Porta de gerenciamento 2 no controlador E2800	1 GbE (RJ-45)	Reservado para suporte técnico.
3	Porta de gerenciamento 1 no controlador E5700SG	1 GbE (RJ-45)	Liga o controlador E5700SG à rede de administração para StorageGRID.

	Porta	Tipo de porta	Função
3	Porta de gerenciamento 2 no controlador E5700SG	1 GbE (RJ-45)	• Pode ser ligado com a porta de gerenciamento 1 se você quiser uma conexão redundante com a rede de administração. • Pode ser deixado sem fios e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, pode ser utilizado para ligar o controlador E5700SG a um computador portátil de serviço se os endereços IP atribuídos por DHCP não estiverem disponíveis.
4	Portas 10/25-GbE 1-4 na controladora E5700SG	10-GbE ou 25-GbE **Observação:** os transcetores SFP incluídos com o dispositivo suportam velocidades de link de 10 GbE. Se você quiser usar velocidades de link de 25 GbE para as quatro portas de rede, você deve fornecer transcetores de SFP28 GbE.	Conete-se à rede de grade e à rede de cliente para StorageGRID. Consulte ""conexões de porta 10/25-GbE para o controlador E5700SG".

Passos

1. Conete o controlador E2800 ao controlador E5700SG usando dois cabos óticos e quatro dos oito transcetores SFP.

Ligar esta porta…	Para este porto…
Porta de interconexão 1 no controlador E2800	Porta de interconexão 1 no controlador E5700SG
Porta de interconexão 2 no controlador E2800	Porta de interconexão 2 no controlador E5700SG

2. Conete a porta de gerenciamento 1 (P1) no controlador E2800 (a porta RJ-45 à esquerda) à rede de gerenciamento do Gerenciador de sistemas SANtricity, usando um cabo Ethernet.

Não use a porta de gerenciamento 2 (P2) no controlador E2800 (a porta RJ-45 à direita). Esta porta está reservada para suporte técnico.

3. Se você planeja usar a rede de administração para StorageGRID, conete a porta de gerenciamento 1 no controlador E5700SG (a porta RJ-45 à esquerda) à rede de administração, usando um cabo Ethernet.

   Se você planeja usar o modo de ligação de rede de backup ativo para a rede Admin, conete a porta de gerenciamento 2 no controlador E5700SG (a porta RJ-45 à direita) à rede Admin, usando um cabo Ethernet.

4. Conete as portas 10/25-GbE no controlador E5700SG aos switches de rede apropriados, usando cabos óticos e transcetores SFP ou SFP28.

   Todas as portas devem usar a mesma velocidade de link. Instale transcetores SFP se você planeja usar velocidades de link de 10 GbE. Instale os transcetores SFP28 se você planeja usar velocidades de link de 25 GbE.

   - Se você planeja usar o modo de ligação de porta fixa (padrão), conete as portas à rede StorageGRID e às redes de clientes, conforme mostrado na tabela.

Porta	Liga a…
Porta 1	Rede cliente (opcional)
Porta 2	Rede de rede
Porta 3	Rede cliente (opcional)
Porta 4	Rede de rede

   - Se você planeja usar o modo de ligação de porta agregada, conete uma ou mais portas de rede a um ou mais switches. Você deve conetar pelo menos duas das quatro portas para evitar ter um único ponto de falha. Se você usar mais de um switch para uma única ligação LACP, os switches devem suportar MLAG ou equivalente.

Informações relacionadas

"Acessando o instalador do StorageGRID Appliance"

"Modos de ligação de porta para E5700SG portas de controlador"

Conexão dos cabos de alimentação e alimentação de energia (SG5700)

Quando você aplica energia ao aparelho, ambos os controladores inicializam.

O que você vai precisar

Ambos os interrutores de alimentação do aparelho devem estar desligados antes de ligar a alimentação.

Risco de choque elétrico — antes de ligar os cabos de alimentação, certifique-se de que os dois interrutores de alimentação do aparelho estão desligados.

Passos

1. Confirme se os dois interrutores de alimentação do aparelho estão desligados.
2. Ligue os dois cabos de alimentação ao aparelho.
3. Conete os dois cabos de alimentação a diferentes unidades de distribuição de energia (PDUs) no gabinete ou no rack.
4. Ligue os dois interrutores de alimentação do aparelho.
   - Não desligue os interrutores de alimentação durante o processo de ativação.
   - Os fãs são muito barulhentos quando eles começam a trabalhar. O ruído alto durante o arranque é normal.
5. Depois que os controladores iniciarem, verifique suas telas de sete segmentos.

Exibindo códigos de status de inicialização do SG5700

Os ecrãs de sete segmentos em cada controlador mostram os códigos de estado e de erro à medida que o aparelho liga.

Sobre esta tarefa

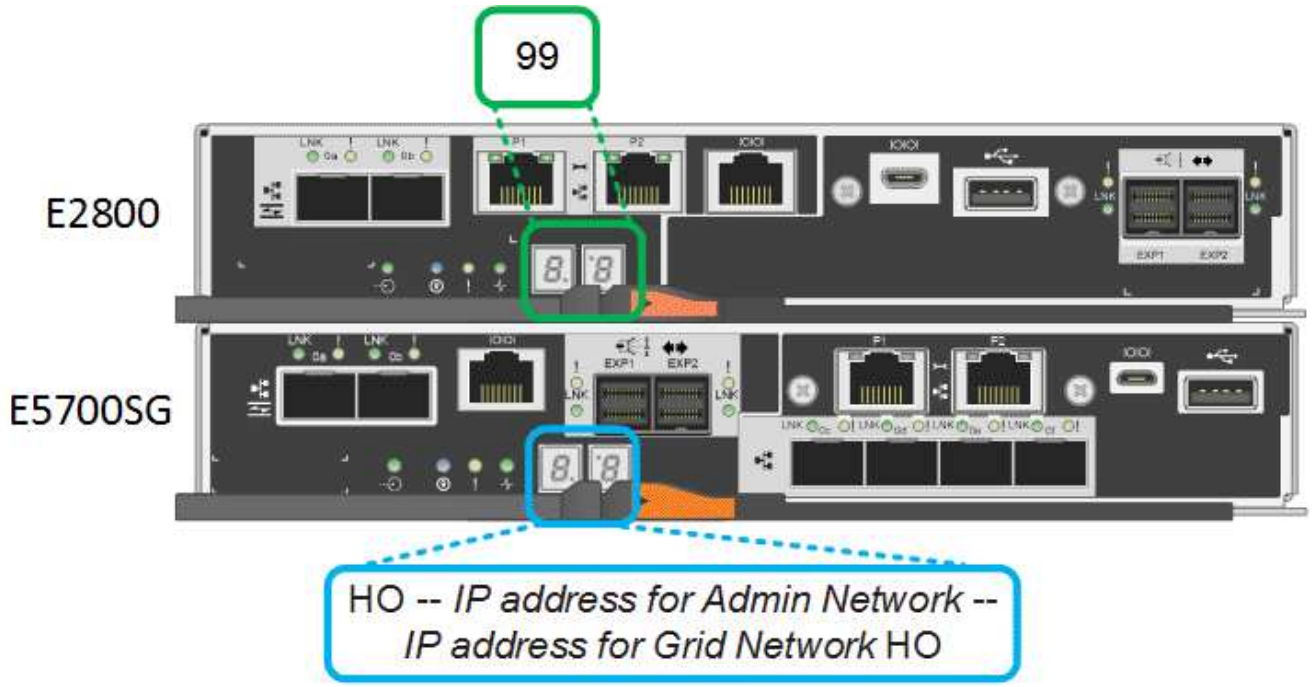
O controlador E2800 e o controlador E5700SG apresentam diferentes Estados e códigos de erro.

Para entender o que esses códigos significam, consulte os seguintes recursos:

Controlador	Referência
Controlador E2800	*Guia de monitorização do sistema E5700 e E2800* **Nota:** os códigos listados para o controlador e-Series E5700 não se aplicam ao controlador E5700SG no aparelho.
Controlador E5700SG	"Indicadores de status no controlador E5700SG"

Passos

1. Durante o arranque, monitorize o progresso visualizando os códigos apresentados nos ecrãs de sete segmentos.
   - O visor de sete segmentos no controlador E2800 mostra a sequência de repetição **os**, **SD**, ***blank*** para indicar que está a efetuar o processamento de início do dia.
   - O visor de sete segmentos no controlador E5700SG mostra uma sequência de códigos, terminando com **AA** e **FF**.
2. Depois que os controladores iniciarem, confirme se as exibições de sete segmentos mostram o seguinte:



Controlador	Visor de sete segmentos
Controlador E2800	A mostra 99, que é o ID padrão de um compartimento de controladora e-Series.
Controlador E5700SG	Mostra **HO**, seguido de uma sequência repetida de dois números. `HO -- IP address for Admin Network -- IP address for Grid Network HO` Na sequência, o primeiro conjunto de números é o endereço IP atribuído pelo DHCP para a porta de gerenciamento 1 do controlador. Este endereço é utilizado para ligar o controlador à rede de administração para StorageGRID. O segundo conjunto de números é o endereço IP atribuído pelo DHCP utilizado para ligar o dispositivo à rede de grelha para StorageGRID. **Nota:** se um endereço IP não puder ser atribuído usando DHCP, 0.0.0.0 será exibido.

3. Se o sete segmentos exibir outros valores, consulte "'solução de problemas da instalação de hardware'" e confirme que você concluiu as etapas de instalação corretamente. Se não conseguir resolver o problema, contacte o suporte técnico.

Informações relacionadas

"Indicadores de status no controlador E5700SG"

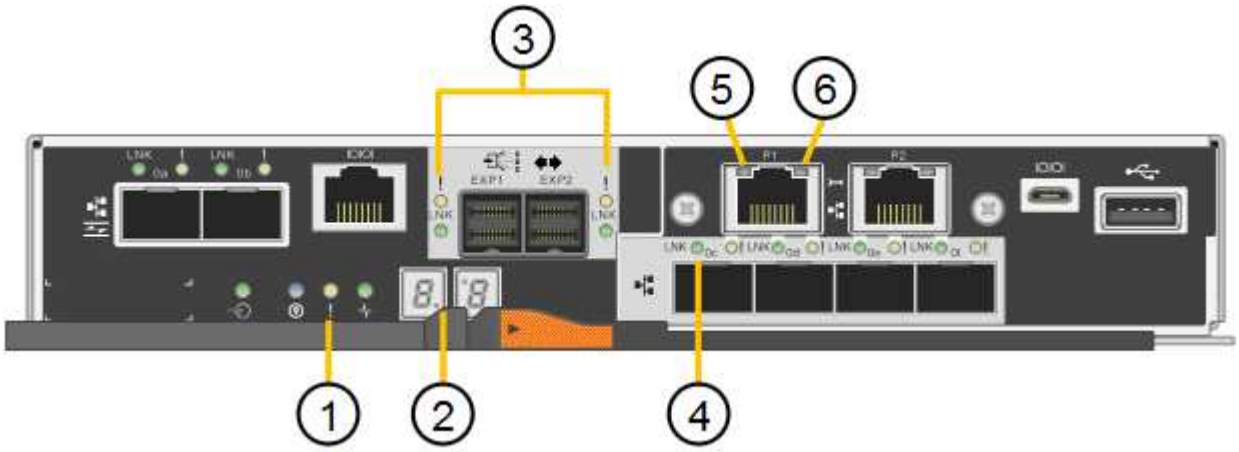
"Solução de problemas da instalação do hardware"

"Guia de monitorização do sistema E5700 e E2800"

Indicadores de status no controlador E5700SG

O visor de sete segmentos e os LEDs no controlador E5700SG mostram códigos de estado e erro enquanto o aparelho liga e enquanto o hardware está a ser inicializado. Você pode usar esses monitores para determinar o status e solucionar erros.

Após o instalador do StorageGRID Appliance ter iniciado, você deve revisar periodicamente os indicadores de status no controlador E5700SG.



	Visor	Descrição
1	LED de atenção	Âmbar: O controlador está com defeito e requer atenção do operador, ou o script de instalação não foi encontrado. Desligado: O controlador está operando normalmente.
2	Visor de sete segmentos	Mostra um código de diagnóstico As sequências de visualização de sete segmentos permitem compreender os erros e o estado operacional do aparelho.
3	LEDs de atenção da porta de expansão	Âmbar: Estes LEDs são sempre âmbar (sem ligação estabelecida) porque o aparelho não utiliza as portas de expansão.
4	LEDs de Status do Link da porta do host	Verde: O link está ativo. Desligado: O link está inativo.

	Visor	Descrição
5	LEDs de estado da ligação Ethernet	Verde: Um link é estabelecido. Desligado: Nenhum link é estabelecido.
6	LEDs de atividade Ethernet	Verde: O link entre a porta de gerenciamento e o dispositivo ao qual está conetado (como um switch Ethernet) está ativado. Desligado: Não existe ligação entre o controlador e o dispositivo ligado. Verde intermitente: Existe atividade Ethernet.

Códigos gerais de arranque

Durante a inicialização ou após uma reinicialização forçada do aparelho, ocorre o seguinte:

1. O visor de sete segmentos no controlador E5700SG apresenta uma sequência geral de códigos que não é específica do controlador. A sequência geral termina com os códigos AA e FF.
2. São apresentados códigos de arranque específicos do controlador E5700SG.

Códigos de inicialização do controlador E5700SG

Durante uma inicialização normal do aparelho, o visor de sete segmentos no controlador E5700SG mostra os seguintes códigos na ordem indicada:

Código	Indica
OLÁ	O script de inicialização mestre foi iniciado.
DE PP	O sistema está verificando se o FPGA precisa ser atualizado.
HP	O sistema está verificando se o firmware da controladora 10/25-GbE precisa ser atualizado.
RB	O sistema está reiniciando após a aplicação de atualizações de firmware.
FP	As verificações de atualização do firmware do subsistema de hardware foram concluídas. Os serviços de comunicação entre controladores estão a iniciar.
ELE	O sistema aguarda conetividade com o controlador E2800 e sincronização com o sistema operativo SANtricity. **Nota:** se este procedimento de arranque não passar por esta fase, verifique as ligações entre os dois controladores.
HC	O sistema está a verificar se existem dados de instalação do StorageGRID.

Código	Indica
HO	O Instalador de dispositivos StorageGRID está em execução.
HA	O StorageGRID está em execução.

E5700SG códigos de erro do controlador

Estes códigos representam condições de erro que podem ser apresentadas no controlador E5700SG à medida que o aparelho arranca. Códigos hexadecimais de dois dígitos adicionais são exibidos se ocorrerem erros específicos de hardware de baixo nível. Se algum destes códigos persistir durante mais de um segundo ou dois, ou se não conseguir resolver o erro seguindo um dos procedimentos de resolução de problemas prescritos, contacte o suporte técnico.

Código	Indica
22	Nenhum Registro mestre de inicialização encontrado em qualquer dispositivo de inicialização.
23	O disco flash interno não está ligado.
2A, 2B	Barramento preso, não é possível ler dados SPD do DIMM.
40	DIMMs inválidos.
41	DIMMs inválidos.
42	Falha no teste de memória.
51	Falha na leitura de SPD.
92 a 96	Inicialização do barramento PCI.
A0 a A3	Inicialização da unidade SATA.
AB	Código de inicialização alternativo.
AE	A arrancar o SO.
EA	DDR4 a formação falhou.
E8	Nenhuma memória instalada.
UE	O script de instalação não foi encontrado.
EP	A instalação ou comunicação com o controlador E2800 falhou.

Informações relacionadas

"Solução de problemas da instalação do hardware"

"Suporte à NetApp"

Configurar o hardware

Depois de aplicar energia ao dispositivo, você deve configurar o Gerenciador de sistema do SANtricity, que é o software que você usará para monitorar o hardware. Você também deve configurar as conexões de rede que serão usadas pelo StorageGRID.

Passos

- "Configurando conexões StorageGRID"
- "Acessando e configurando o Gerenciador do sistema do SANtricity"
- "Opcional: Habilitando a criptografia de nó"
- "Opcional: Alterar o modo RAID (apenas SG5760)"
- "Opcional: Remapeamento de portas de rede para o dispositivo"

Configurando conexões StorageGRID

Antes de implantar um dispositivo StorageGRID como nó de armazenamento em uma grade StorageGRID, você deve configurar as conexões entre o dispositivo e as redes que você planeja usar. Você pode configurar a rede navegando até o Instalador de dispositivos StorageGRID, que está incluído no controlador E5700SG (o controlador de computação no dispositivo).

Passos

- "Acessando o instalador do StorageGRID Appliance"
- "Verificando e atualizando a versão do Instalador de dispositivos StorageGRID"
- "Configurando links de rede (SG5700)"
- "Definir a configuração IP"
- "Verificando conexões de rede"
- "Verificando conexões de rede no nível da porta"

Acessando o instalador do StorageGRID Appliance

Você deve acessar o Instalador do StorageGRID Appliance para configurar as conexões entre o appliance e as três redes StorageGRID: A rede de grade, a rede de administração (opcional) e a rede de cliente (opcional).

O que você vai precisar

- Você está usando um navegador da Web compatível.
- O dispositivo está ligado a todas as redes StorageGRID que pretende utilizar.
- Você sabe o endereço IP, o gateway e a sub-rede do dispositivo nessas redes.
- Configurou os comutadores de rede que pretende utilizar.

Sobre esta tarefa

Ao acessar pela primeira vez o Instalador do StorageGRID Appliance, você pode usar o endereço IP atribuído pelo DHCP para a rede Admin (assumindo que o dispositivo esteja conetado à rede Admin) ou o endereço IP atribuído pelo DHCP para a rede de Grade. É preferível utilizar o endereço IP da rede de administração. Caso contrário, se você acessar o Instalador do StorageGRID Appliance usando o endereço DHCP da rede de Grade, poderá perder a conexão com o Instalador do StorageGRID Appliance ao alterar as configurações de link e ao inserir um IP estático.

Passos

1. Obtenha o endereço DHCP do dispositivo na rede Admin (se estiver ligado) ou na rede Grid (se a rede Admin não estiver ligada).

   Você pode fazer um dos seguintes procedimentos:

   - Observe o visor de sete segmentos no controlador E5700SG. Se as portas de gerenciamento 1 e 10/25-GbE 2 e 4 no controlador E5700SG estiverem conetadas a redes com servidores DHCP, o controlador tentará obter endereços IP atribuídos dinamicamente ao ligar o gabinete. Depois que o controlador tiver concluído o processo de ativação, o visor de sete segmentos mostra **HO**, seguido de uma sequência repetida de dois números.

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     Na sequência:

     - O primeiro conjunto de números é o endereço DHCP para o nó de armazenamento do dispositivo na rede Admin, se estiver conetado. Este endereço IP é atribuído à porta de gerenciamento 1 no controlador E5700SG.
     - O segundo conjunto de números é o endereço DHCP para o nó de armazenamento do dispositivo na rede de Grade. Esse endereço IP é atribuído às portas 2 e 4 de 10/25 GbE quando você primeiro aplica energia ao dispositivo.

       Se um endereço IP não puder ser atribuído usando DHCP, 0.0.0.0 será exibido.

   - Forneça o endereço MAC da porta de gerenciamento 1 ao administrador da rede, para que ele possa procurar o endereço DHCP dessa porta na rede de administração. O endereço MAC é impresso em uma etiqueta no controlador E5700SG, ao lado da porta.

2. Se você conseguiu obter um dos endereços DHCP:

   a. Abra um navegador da Web no laptop de serviço.

   b. Digite este URL para o instalador do StorageGRID Appliance
   `https://E5700SG_Controller_IP:8443`

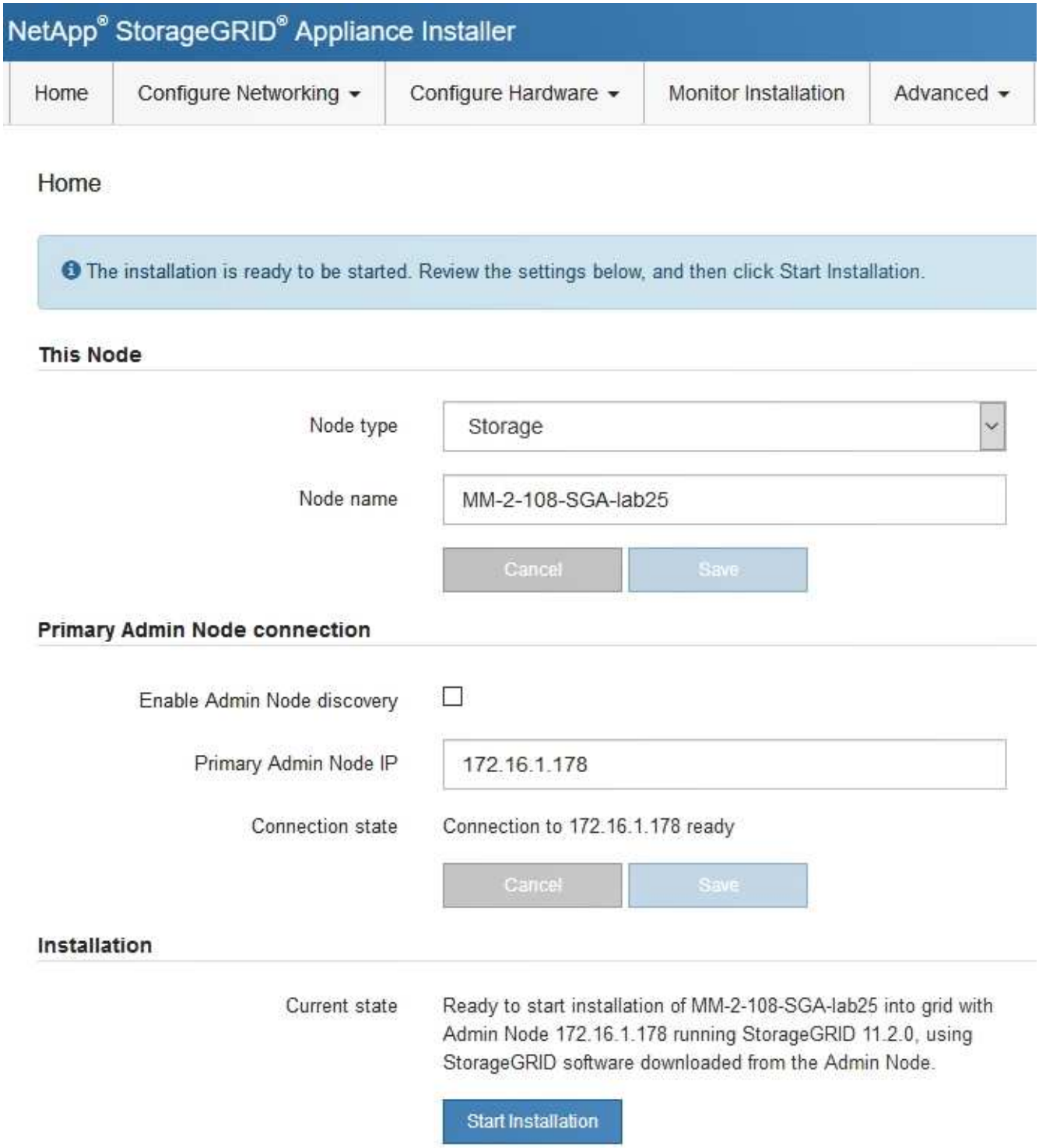
   Para *`E5700SG_Controller_IP`*, utilize o endereço DHCP do controlador (utilize o endereço IP da rede de administração, se o tiver).

   c. Se for solicitado um alerta de segurança, exiba e instale o certificado usando o assistente de instalação do navegador.

   O alerta não aparecerá na próxima vez que você acessar este URL.

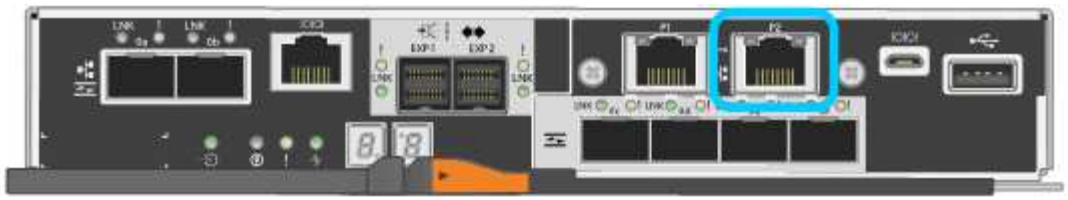
   A página inicial do instalador do dispositivo StorageGRID é exibida. As informações e as mensagens

mostradas quando você acessa esta página pela primeira vez dependem de como o dispositivo está conetado atualmente às redes StorageGRID. Podem aparecer mensagens de erro que serão resolvidas em etapas posteriores.



3. Se o controlador E5700SG não conseguir adquirir um endereço IP utilizando DHCP:

   a. Conete o notebook de serviço à porta de gerenciamento 2 no controlador E5700SG, usando um cabo Ethernet.



b. Abra um navegador da Web no laptop de serviço.

c. Digite este URL para o instalador do StorageGRID Appliance
`https://169.254.0.1:8443`

A página inicial do instalador do dispositivo StorageGRID é exibida. As informações e as mensagens apresentadas quando acede pela primeira vez a esta página dependem da forma como o seu aparelho está atualmente ligado.

Se não conseguir aceder à página inicial através de uma ligação local, configure o endereço IP do computador portátil de serviço como `169.254.0.2`, e tente novamente.

4. Reveja as mensagens apresentadas na página inicial e configure a configuração da ligação e a configuração IP, conforme necessário.

Informações relacionadas

"Requisitos do navegador da Web"

Verificando e atualizando a versão do Instalador de dispositivos StorageGRID

A versão do Instalador de dispositivos StorageGRID no dispositivo deve corresponder à versão de software instalada no sistema StorageGRID para garantir que todos os recursos do StorageGRID sejam suportados.

O que você vai precisar

Você acessou o Instalador de dispositivos StorageGRID.

Sobre esta tarefa

Os dispositivos StorageGRID vêm da fábrica pré-instalados com o Instalador de dispositivos StorageGRID. Se você estiver adicionando um dispositivo a um sistema StorageGRID atualizado recentemente, talvez seja necessário atualizar manualmente o Instalador de dispositivos StorageGRID antes de instalar o dispositivo como um novo nó.

O Instalador de dispositivos StorageGRID é atualizado automaticamente quando você atualiza para uma nova versão do StorageGRID. Não é necessário atualizar o Instalador de dispositivos StorageGRID nos nós de dispositivos instalados. Este procedimento só é necessário quando estiver a instalar um dispositivo que contenha uma versão anterior do Instalador de dispositivos StorageGRID.

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Avançado Atualização de firmware**.
2. Compare a versão atual do firmware com a versão de software instalada no seu sistema StorageGRID (no Gerenciador de Grade, selecione **Ajuda sobre**).

   O segundo dígito nas duas versões deve corresponder. Por exemplo, se o seu sistema StorageGRID estiver executando a versão 11.**5**.*x*.*y*, a versão do Instalador de dispositivos StorageGRID deve ser 3.**5**.*z*.

3. Se o aparelho tiver uma versão de nível inferior do instalador do dispositivo StorageGRID, vá para a página de downloads do NetApp para StorageGRID.

   "NetApp Downloads: StorageGRID"

   Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.

4. Baixe a versão apropriada do arquivo **suporte para dispositivos StorageGRID** e o arquivo de checksum correspondente.

   O arquivo de suporte para dispositivos StorageGRID é um `.zip` arquivo que contém as versões de firmware atuais e anteriores para todos os modelos de dispositivos StorageGRID, em subdiretórios para cada tipo de controlador.

   Depois de baixar o arquivo de suporte para o arquivo de dispositivos StorageGRID, extraia o `.zip` arquivo e consulte o arquivo README para obter informações importantes sobre a instalação do Instalador de dispositivos StorageGRID.

5. Siga as instruções na página Atualizar firmware do Instalador de dispositivos StorageGRID para executar estas etapas:
   a. Carregue o ficheiro de suporte apropriado (imagem de firmware) para o seu tipo de controlador e o ficheiro de checksum.
   b. Atualize a partição inativa.
   c. Reinicie e troque partições.
   d. Atualize a segunda partição.

Informações relacionadas

"Acessando o instalador do StorageGRID Appliance"

Configurando links de rede (SG5700)

Você pode configurar links de rede para as portas usadas para conetar o dispositivo à rede de Grade, à rede de cliente e à rede de administração. Você pode definir a velocidade do link, bem como os modos de ligação de porta e rede.

O que você vai precisar

Se você planeja usar a velocidade de link de 25 GbE para as portas de 10/25 GbE:

- Você instalou transcetores SFP28 nas portas que você pretende usar.
- Você conetou as portas a switches que podem suportar esses recursos.
- Você entende como configurar os interrutores para usar essa velocidade mais alta.

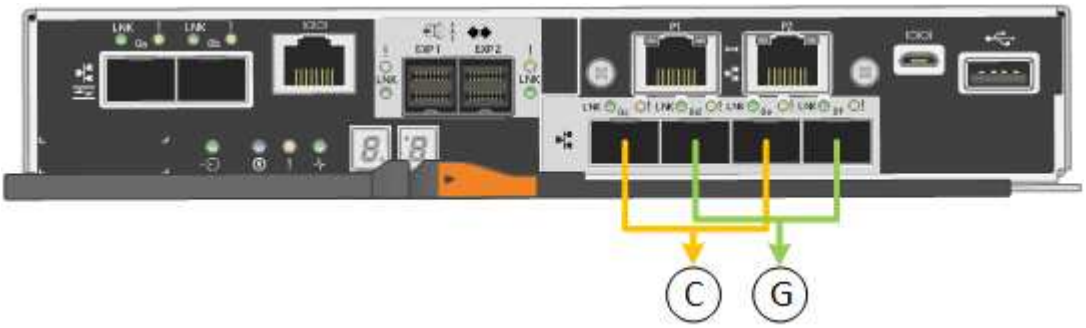
Se você planeja usar o modo de ligação de porta agregada, o modo de ligação de rede LACP ou a marcação de VLAN para as portas 10/25-GbE:

- Você conetou as portas do dispositivo a switches que podem suportar VLAN e LACP.
- Se vários switches estiverem participando da ligação LACP, os switches suportam grupos de agregação de links de vários gabinetes (MLAG) ou equivalente.
- Você entende como configurar os switches para usar VLAN, LACP e MLAG ou equivalente.

- Você conhece a tag VLAN exclusiva a ser usada para cada rede. Essa tag VLAN será adicionada a cada pacote de rede para garantir que o tráfego de rede seja roteado para a rede correta.
- Se você planeja usar o modo ative-Backup para a rede Admin, conetou cabos Ethernet a ambas as portas de gerenciamento no controlador.

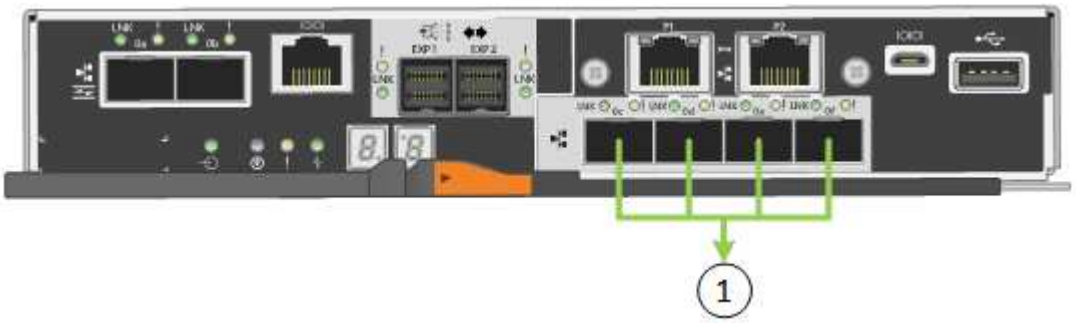
Sobre esta tarefa

Esta figura mostra como as quatro portas 10/25-GbE são ligadas no modo de ligação de porta fixa (configuração padrão).



	Quais portas estão coladas
C	As portas 1 e 3 são Unidas para a rede do cliente, se esta rede for utilizada.
G	As portas 2 e 4 são Unidas para a rede de Grade.

Esta figura mostra como as quatro portas 10/25-GbE são ligadas no modo de ligação de porta agregada.



	Quais portas estão coladas
1	Todas as quatro portas são agrupadas em uma única ligação LACP, permitindo que todas as portas sejam usadas para o tráfego de rede de Grade e rede de Cliente.

A tabela resume as opções de configuração das quatro portas 10/25 GbE. As predefinições são apresentadas a negrito. Só é necessário configurar as definições na página Configuração de ligação se pretender utilizar uma definição não predefinida.

- **Modo de ligação de porta fixo (padrão)**

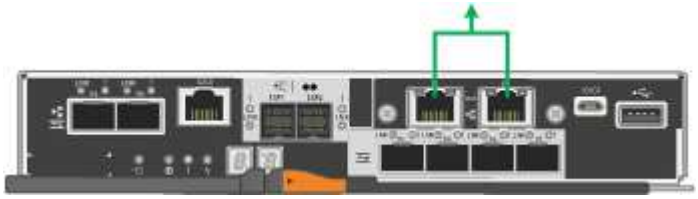
Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Ative-Backup (padrão)	• As portas 2 e 4 usam uma ligação de backup ativo para a rede de Grade. • As portas 1 e 3 não são usadas. • Uma etiqueta VLAN é opcional.	• As portas 2 e 4 usam uma ligação de backup ativo para a rede de Grade. • As portas 1 e 3 usam uma ligação de backup ativo para a rede do cliente. • Tags VLAN podem ser especificadas para ambas as redes para a conveniência do administrador de rede.
Bola de Futsal (802,3ad)	• As portas 2 e 4 usam uma ligação LACP para a rede de Grade. • As portas 1 e 3 não são usadas. • Uma etiqueta VLAN é opcional.	• As portas 2 e 4 usam uma ligação LACP para a rede de Grade. • As portas 1 e 3 usam uma ligação LACP para a rede de clientes. • Tags VLAN podem ser especificadas para ambas as redes para a conveniência do administrador de rede.

- **Modo de ligação de porta agregada**

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Apenas LACP (802,3ad)	• As portas 1-4 usam uma única ligação LACP para a rede de Grade. • Uma única etiqueta VLAN identifica pacotes de rede de Grade.	• As portas 1-4 usam uma única ligação LACP para a rede de Grade e a rede do Cliente. • Duas etiquetas VLAN permitem que os pacotes de rede de Grade sejam segregados dos pacotes de rede de Cliente.

Consulte as informações sobre conexões de porta 10/25-GbE para o controlador E5700SG para obter mais informações sobre os modos de ligação de porta e ligação de rede.

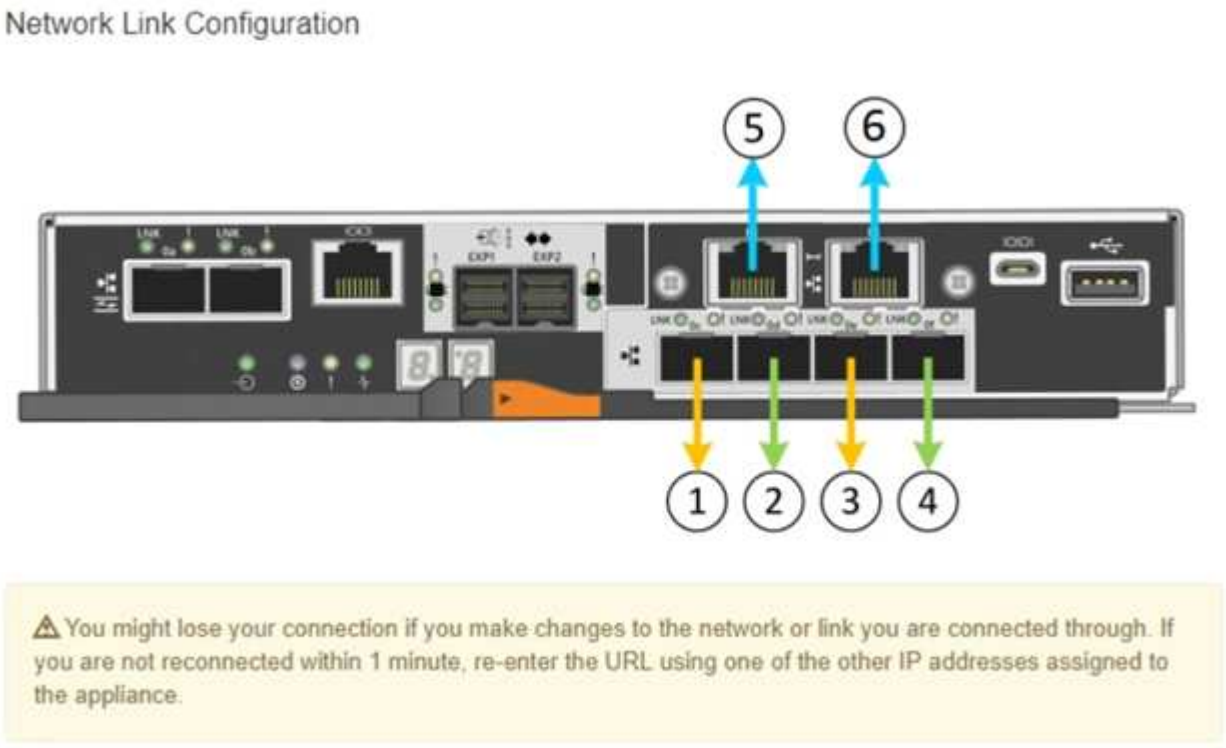
Esta figura mostra como as duas portas de gerenciamento de 1 GbE na controladora E5700SG são ligadas no modo de ligação de rede ative-Backup para a rede Admin.



Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Configuração de ligação**.

A página Network Link Configuration (Configuração da ligação de rede) apresenta um diagrama do seu dispositivo com as portas de rede e de gestão numeradas.



A tabela Status da ligação lista o estado da ligação (para cima/para baixo) e a velocidade (1/10/25/40/100 Gbps) das portas numeradas.

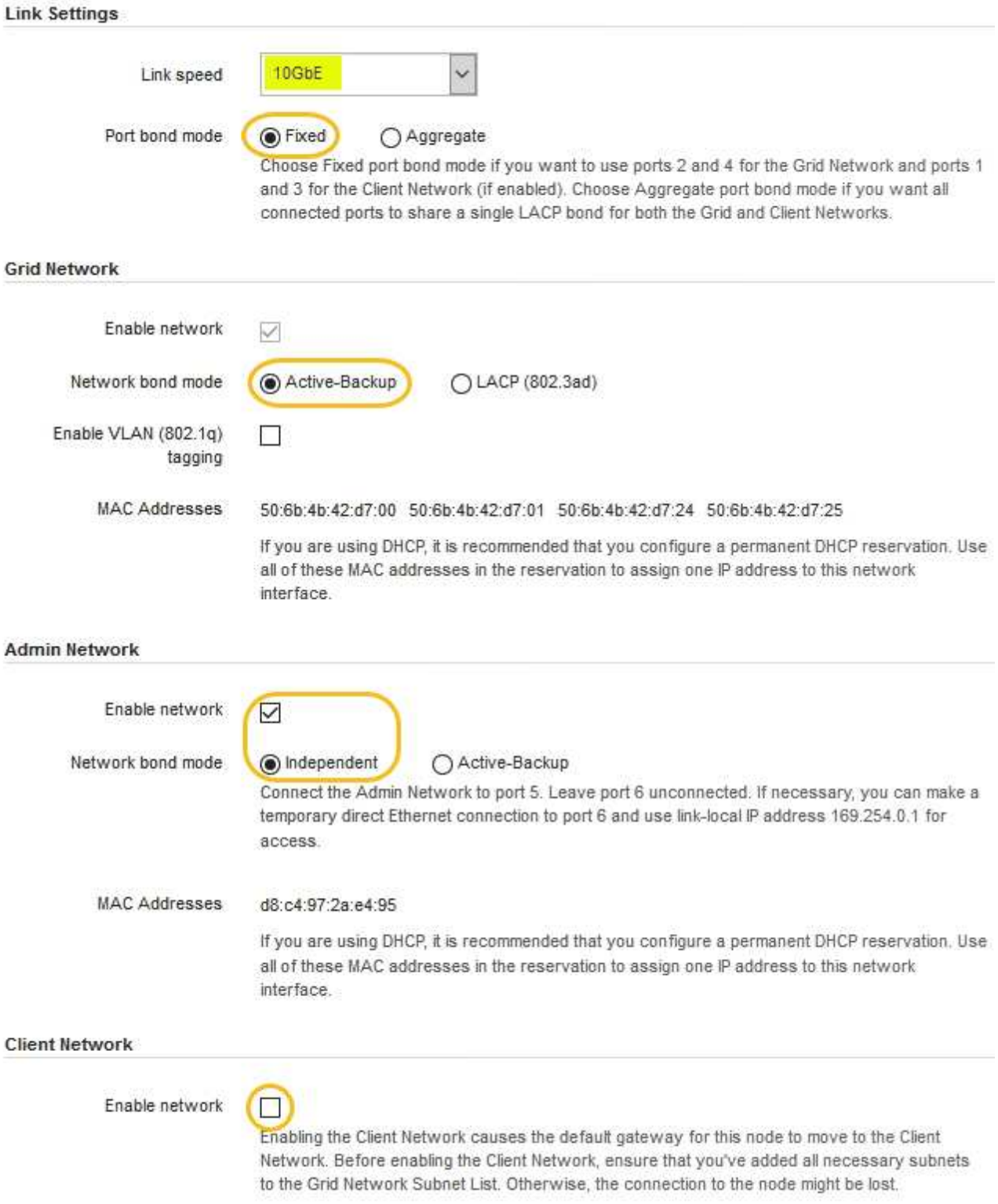
Link Status

Link	State	Speed (Gbps)
1	Up	25
2	Up	25
3	Up	25
4	Up	25
5	Up	1
6	Up	1

A primeira vez que aceder a esta página:

- **Link Speed** está definido para **10GbE**.
- **Port bond mode** está definido como **Fixed**.
- **O modo de ligação de rede** para a rede de Grade está definido como **ative-Backup**.

- A **Admin Network** está ativada e o modo de ligação de rede está definido como **Independent**.
- A **rede do cliente** está desativada.



2. Se você planeja usar a velocidade de link de 25 GbE para as portas de 10/25 GbE, selecione **25GbE** na lista suspensa velocidade de link.

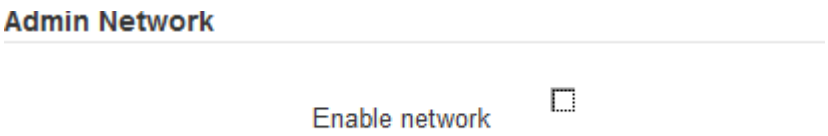
   Os switches de rede que você está usando para a rede de Grade e a rede do cliente também devem

suportar e ser configurados para essa velocidade. Os transcetores SFP28 devem ser instalados nas portas.

3. Ative ou desative as redes StorageGRID que pretende utilizar.

   A rede de Grade é necessária. Não é possível desativar esta rede.

   a. Se o dispositivo não estiver conetado à rede Admin, desmarque a caixa de seleção **Ativar rede** para a rede Admin.

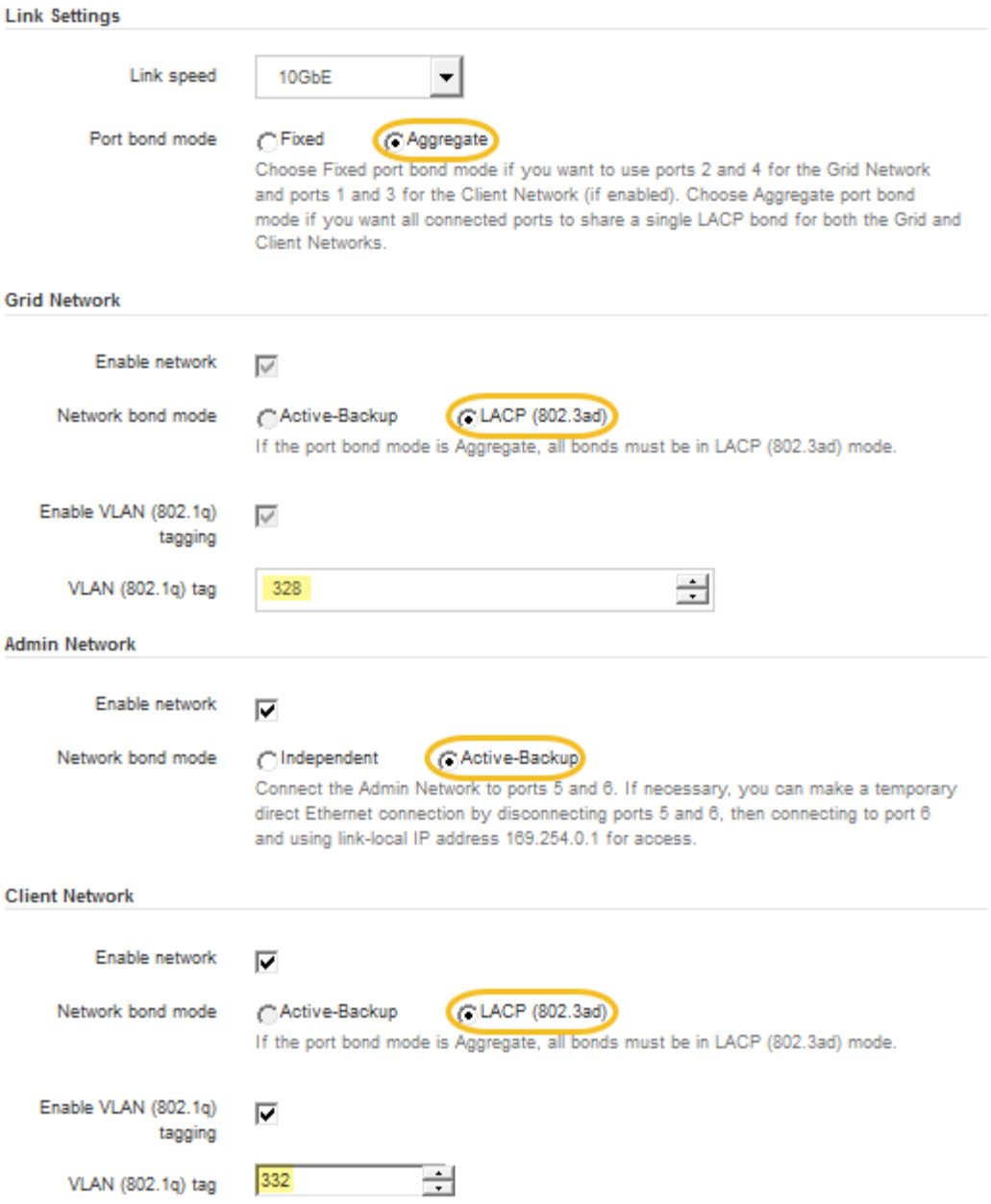
   b. Se o dispositivo estiver conetado à rede do cliente, marque a caixa de seleção **Ativar rede** para a rede do cliente.

      As configurações de rede do cliente para as portas 10/25-GbE são agora mostradas.

4. Consulte a tabela e configure o modo de ligação de porta e o modo de ligação de rede.

   O exemplo mostra:

   - **Aggregate** e **LACP** selecionados para as redes Grid e Client. Você deve especificar uma tag VLAN exclusiva para cada rede. Pode selecionar valores entre 0 e 4095.
   - **Ative-Backup** selecionado para a rede Admin.



5. Quando estiver satisfeito com suas seleções, clique em **Salvar**.

> Poderá perder a ligação se tiver efetuado alterações à rede ou à ligação através da qual está ligado. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do Instalador de appliance StorageGRID usando um dos outros endereços IP atribuídos ao appliance
> **`https://E5700SG_Controller_IP:8443`**

Informações relacionadas

"Modos de ligação de porta para E5700SG portas de controlador"

Definir a configuração IP

Você usa o Instalador de dispositivos StorageGRID para configurar os endereços IP e as informações de roteamento usados para o nó de armazenamento de dispositivos nas

redes StorageGRID, Admin e cliente.

Sobre esta tarefa

Você deve atribuir um IP estático para o dispositivo em cada rede conetada ou atribuir uma concessão permanente para o endereço no servidor DHCP.

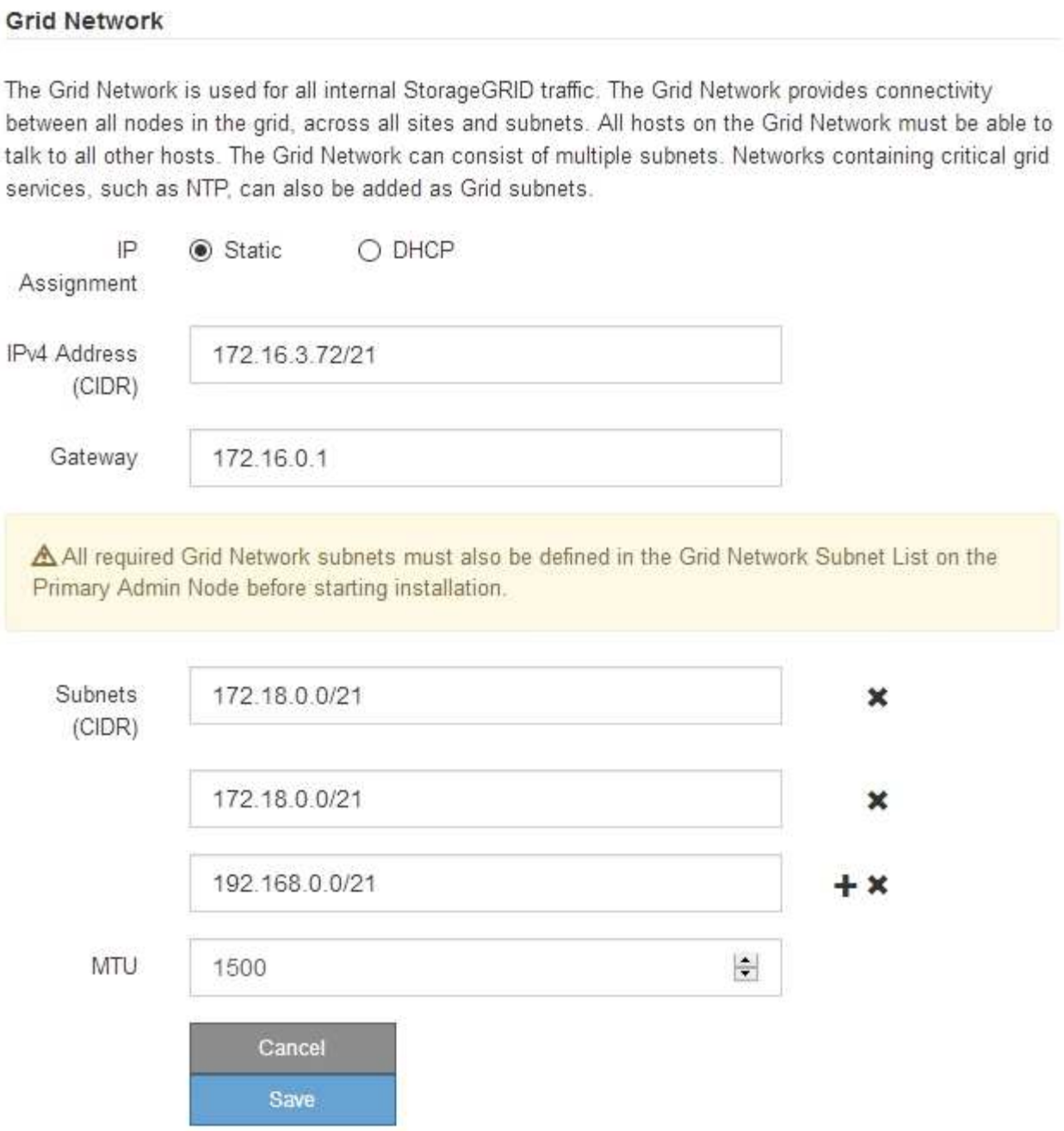
Se você quiser alterar a configuração do link, consulte as instruções para alterar a configuração do link do controlador E5700SG.

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração IP**.

   É apresentada a página Configuração IP.

2. Para configurar a rede de Grade, selecione **Static** ou **DHCP** na seção **Grid Network** da página.



3. Se você selecionou **Static**, siga estas etapas para configurar a rede de Grade:
   a. Insira o endereço IPv4 estático, usando a notação CIDR.
   b. Entre no gateway.

      Se a rede não tiver um gateway, insira novamente o mesmo endereço IPv4 estático.

   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

      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.

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.

d. Clique em **Salvar**.

Quando você altera o endereço IP, o gateway e a lista de sub-redes também podem mudar.

Se você perder a conexão com o Instalador do StorageGRID Appliance, insira novamente o URL usando o novo endereço IP estático que você acabou de atribuir. Por exemplo `https://services_appliance_IP:8443`

e. Confirme se a lista de sub-redes da rede de Grade está correta.

Se você tiver 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. Essas sub-redes de rede de grade também devem ser definidas na lista de sub-redes de rede de grade no nó de administração principal quando você iniciar a instalação do StorageGRID.

A rota padrão não está listada. Se a rede do cliente não estiver ativada, a rota padrão usará o gateway de rede de grade.

- Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
- Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

f. Clique em **Salvar**.

4. Se você selecionou **DHCP**, siga estas etapas para configurar a rede de Grade:

a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

Os campos **IPv4 Address**, **Gateway** e **sub-redes** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

b. Confirme se a lista de sub-redes da rede de Grade está correta.

Se você tiver 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. Essas sub-redes de rede de grade também devem ser definidas na lista de sub-redes de rede de grade no nó de administração principal quando você iniciar a instalação do StorageGRID.

A rota padrão não está listada. Se a rede do cliente não estiver ativada, a rota padrão usará o gateway de rede de grade.

- Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
- Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros

jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

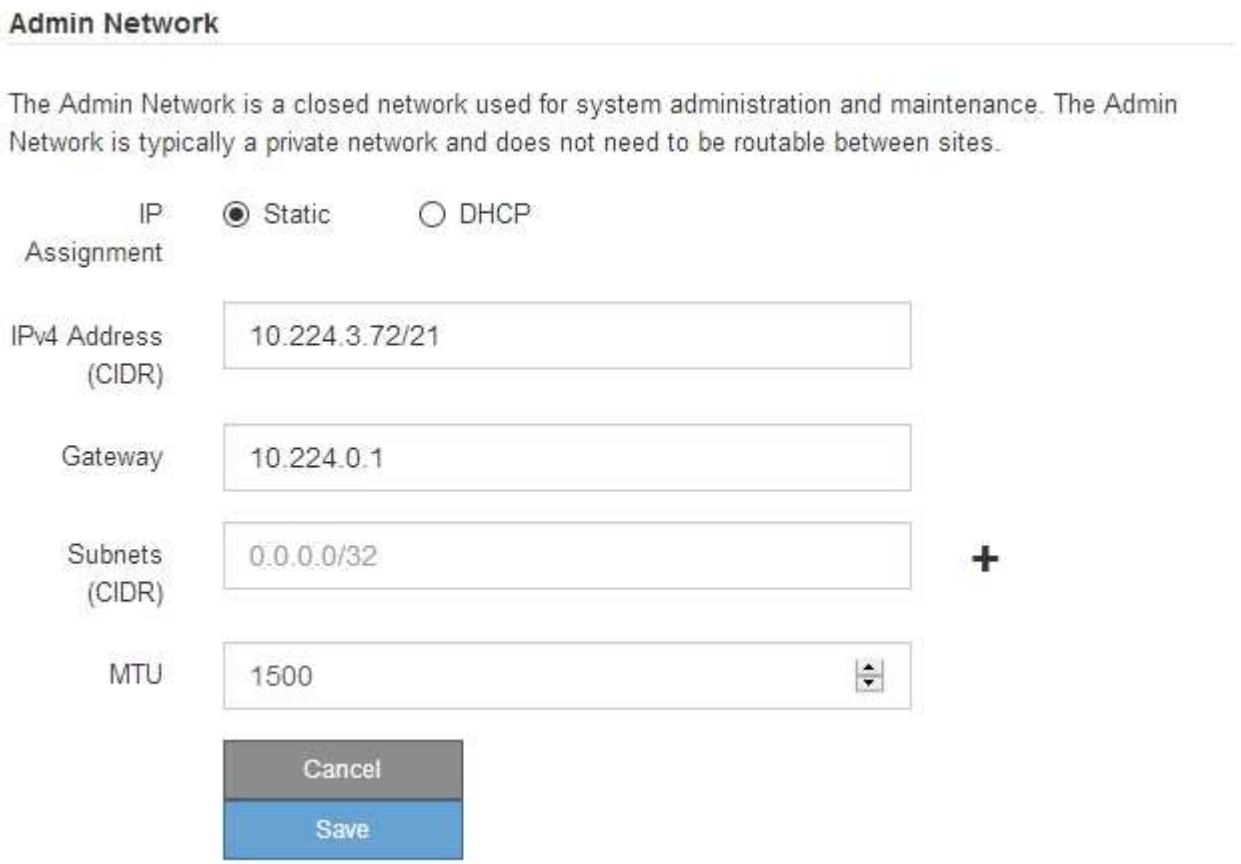
> O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

> 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.

a. Clique em **Salvar**.

5. Para configurar a rede Admin, selecione **Static** (estático) ou **DHCP** (DHCP) na secção Admin Network (rede Admin) da página.

> Para configurar a rede de administração, você deve ativar a rede de administração na página Configuração de ligação.



6. Se você selecionou **Static**, siga estas etapas para configurar a rede Admin:

a. Introduza o endereço IPv4 estático, utilizando a notação CIDR, para a porta de gestão 1 no dispositivo.

A porta de gerenciamento 1 fica à esquerda das duas portas RJ45 de 1 GbE na extremidade direita do dispositivo.

b. Entre no gateway.

   Se a rede não tiver um gateway, insira novamente o mesmo endereço IPv4 estático.

c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

   > 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.

d. Clique em **Salvar**.

   Quando você altera o endereço IP, o gateway e a lista de sub-redes também podem mudar.

   Se você perder a conexão com o Instalador do StorageGRID Appliance, insira novamente o URL usando o novo endereço IP estático que você acabou de atribuir. Por exemplo `https://services_appliance:8443`

e. Confirme se a lista de sub-redes Admin Network está correta.

   Você deve verificar se todas as sub-redes podem ser alcançadas usando o gateway fornecido.

   > A rota padrão não pode ser feita para usar o gateway de rede Admin.

   - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
   - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

f. Clique em **Salvar**.

7. Se você selecionou **DHCP**, siga estas etapas para configurar a rede Admin:

   a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

      Os campos **IPv4 Address**, **Gateway** e **sub-redes** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

      O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

   b. Confirme se a lista de sub-redes Admin Network está correta.

      Você deve verificar se todas as sub-redes podem ser alcançadas usando o gateway fornecido.

      > A rota padrão não pode ser feita para usar o gateway de rede Admin.

      - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
      - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

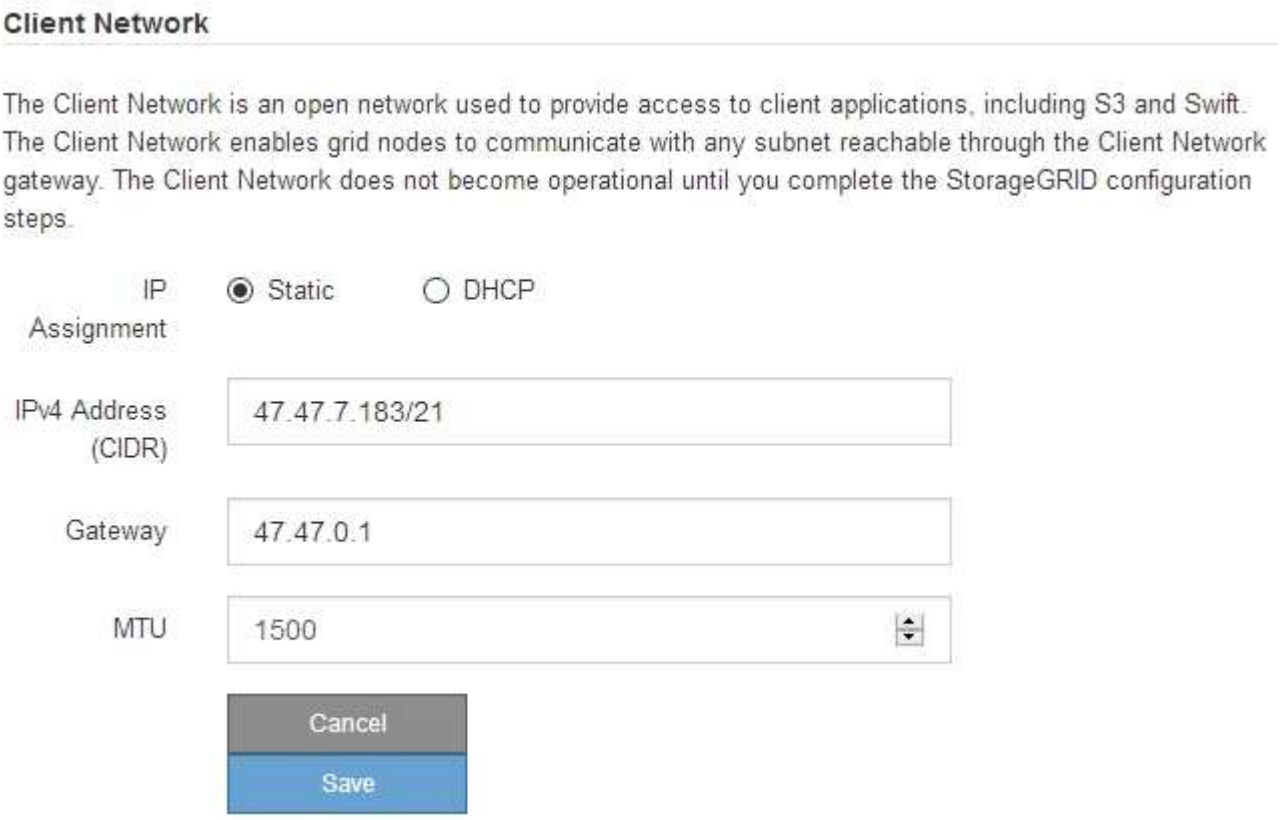
   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

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.

d. Clique em **Salvar**.

8. Para configurar a rede do cliente, selecione **estático** ou **DHCP** na seção **rede do cliente** da página.

Para configurar a rede do cliente, tem de ativar a rede do cliente na página Configuração da ligação.



9. Se você selecionou **Static**, siga estas etapas para configurar a rede do cliente:

a. Insira o endereço IPv4 estático, usando a notação CIDR.

b. Clique em **Salvar**.

c. Confirme se o endereço IP do gateway de rede do cliente está correto.

Se a rede do cliente estiver ativada, é apresentada a rota predefinida. A rota padrão usa o gateway de rede do cliente e não pode ser movida para outra interface enquanto a rede do cliente está ativada.

d. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

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.

e. Clique em **Salvar**.

10. Se você selecionou **DHCP**, siga estas etapas para configurar a rede do cliente:

    a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

       Os campos **IPv4 Address** e **Gateway** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

    O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

    a. Confirme se o gateway está correto.

       > ⓘ Se a rede do cliente estiver ativada, é apresentada a rota predefinida. A rota padrão usa o gateway de rede do cliente e não pode ser movida para outra interface enquanto a rede do cliente está ativada.

    b. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

       > ⓘ 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.

Informações relacionadas

"Alterar a configuração do link do controlador E5700SG"

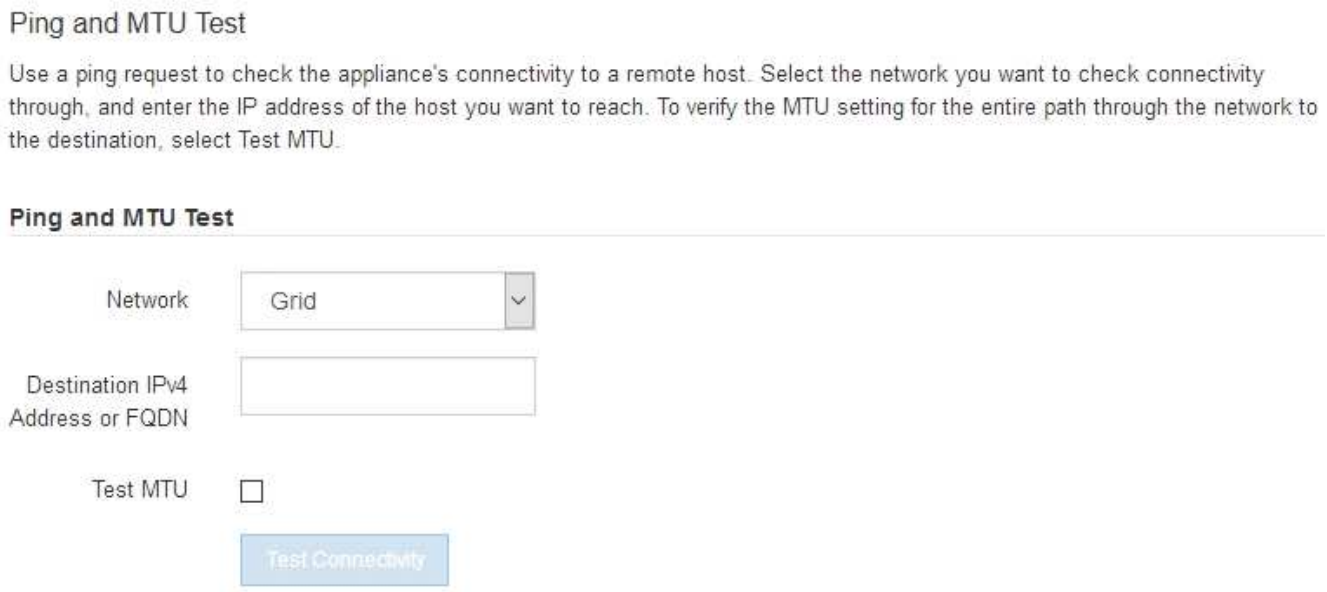
Verificando conexões de rede

Confirme que pode aceder às redes StorageGRID que está a utilizar a partir do dispositivo. Para validar o roteamento por meio de gateways de rede, você deve testar a conetividade entre o Instalador de dispositivos StorageGRID e endereços IP em diferentes sub-redes. Você também pode verificar a configuração MTU.

Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Teste de Ping e MTU**.

   A página Ping e MTU Test (Teste de Ping e MTU) é exibida.



2. Na caixa suspensa **rede**, selecione a rede que deseja testar: Grade, Admin ou Cliente.
3. Insira o endereço IPv4 ou o nome de domínio totalmente qualificado (FQDN) para um host nessa rede.

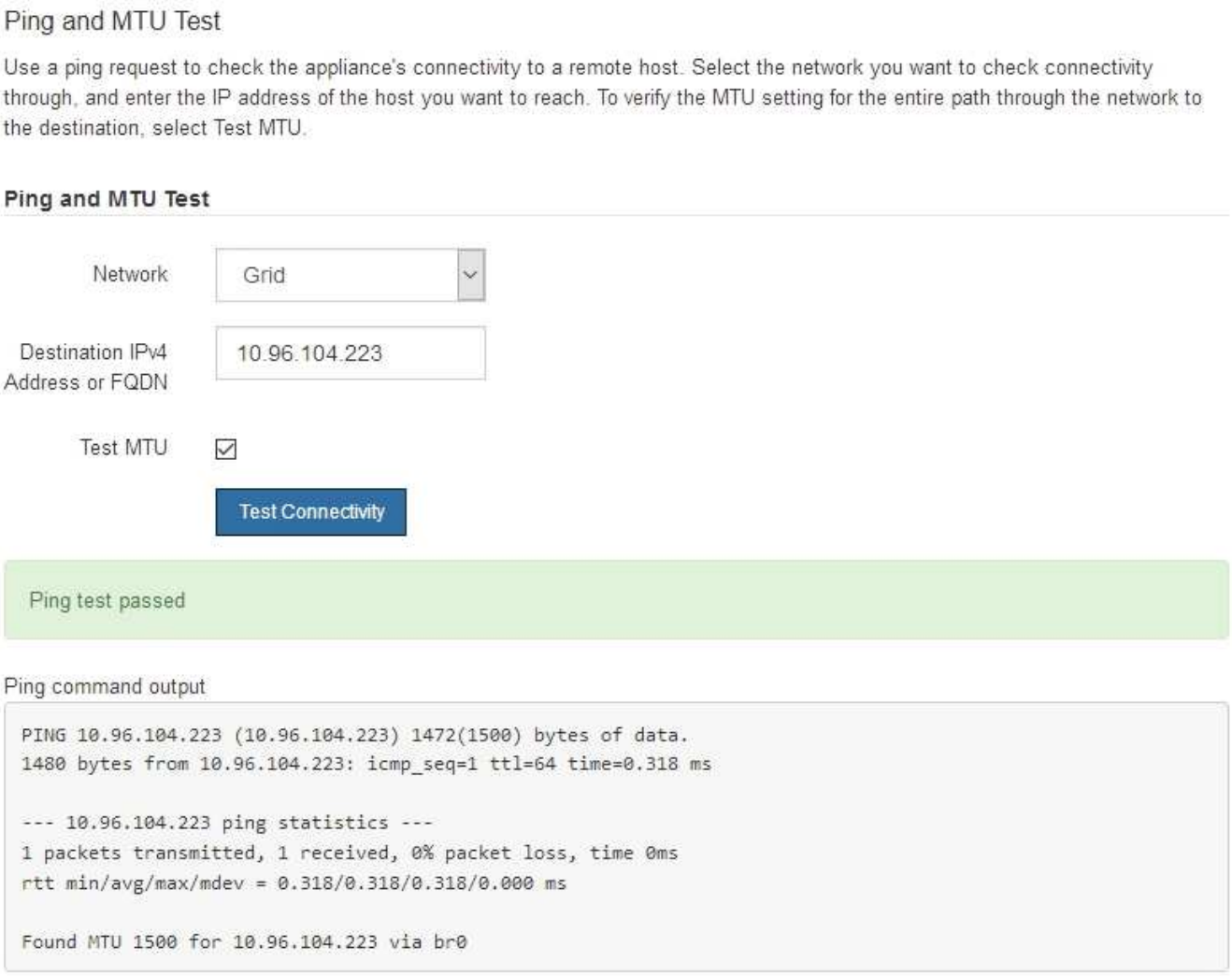
   Por exemplo, você pode querer fazer ping no gateway na rede ou no nó de administração principal.

4. Opcionalmente, marque a caixa de seleção **Test MTU** para verificar a configuração de MTU para todo o caminho através da rede até o destino.

   Por exemplo, você pode testar o caminho entre o nó do dispositivo e um nó em um local diferente.

5. Clique em **testar conetividade**.

   Se a conexão de rede for válida, a mensagem "Teste de ping aprovado" será exibida, com a saída do comando ping listada.



Informações relacionadas

"Configurando links de rede (SG5700)"

"Alterar a definição MTU"

Verificando conexões de rede no nível da porta

Para garantir que o acesso entre o Instalador de dispositivos StorageGRID e outros nós não esteja obstruído por firewalls, confirme se o Instalador de dispositivos StorageGRID pode se conetar a uma porta TCP específica ou conjunto de portas no endereço IP ou intervalo de endereços especificado.

Sobre esta tarefa

Usando a lista de portas fornecida no Instalador de dispositivos StorageGRID, você pode testar a conetividade entre o dispositivo e os outros nós da rede de Grade.

Além disso, você pode testar a conetividade nas redes Admin e Client e nas portas UDP, como as usadas para servidores NFS ou DNS externos. Para obter uma lista dessas portas, consulte a referência de porta nas diretrizes de rede do StorageGRID.

As portas de rede de grade listadas na tabela de conetividade de portas são válidas apenas para o StorageGRID versão 11,5.0. Para verificar quais portas estão corretas para cada tipo de nó, você deve sempre consultar as diretrizes de rede para sua versão do StorageGRID.

Passos

1. No Instalador de dispositivos StorageGRID, clique em **Configurar rede Teste de conetividade de porta (nmap)**.

   A página Teste de conetividade de porta é exibida.

   A tabela de conetividade de porta lista os tipos de nós que exigem conetividade TCP na rede de Grade. Para cada tipo de nó, a tabela lista as portas de rede de Grade que devem ser acessíveis ao seu dispositivo.

   The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

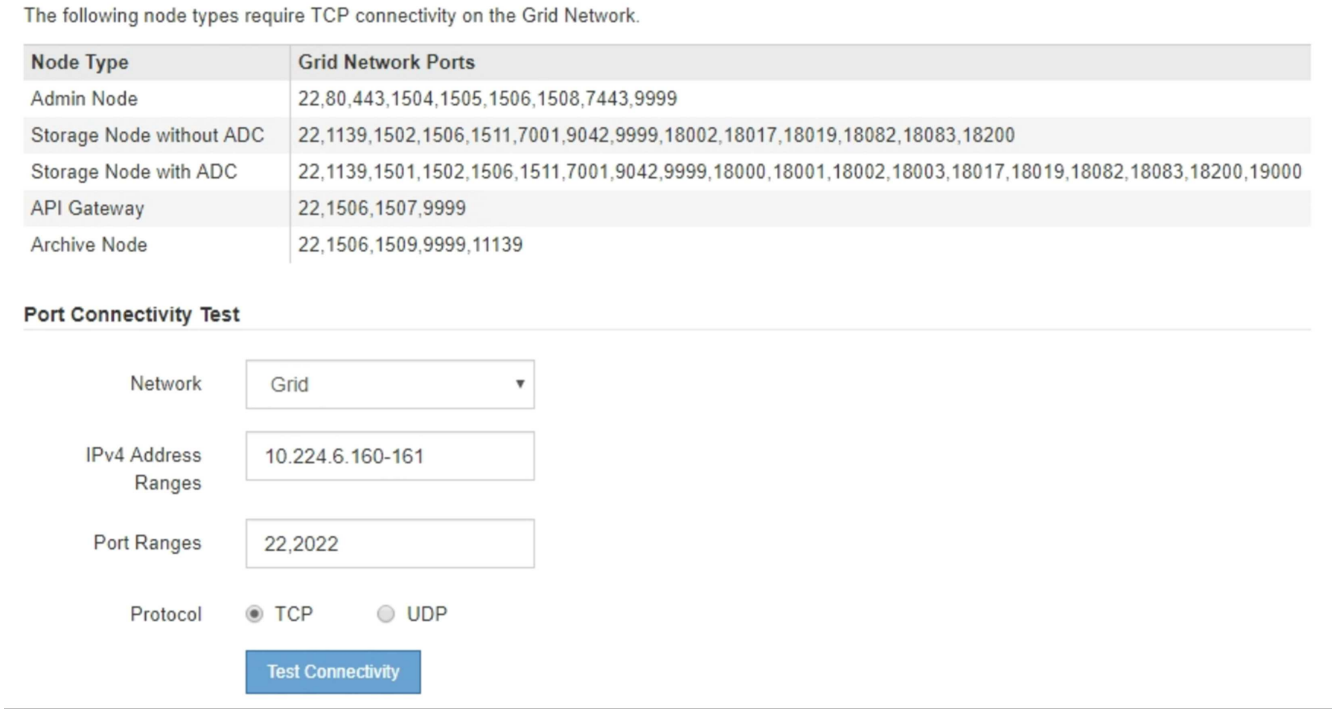
   Você pode testar a conetividade entre as portas do dispositivo listadas na tabela e os outros nós da rede de Grade.

2. Na lista suspensa **Network**, selecione a rede que deseja testar: **Grid**, **Admin** ou **Client**.
3. Especifique um intervalo de endereços IPv4 para os hosts nessa rede.

   Por exemplo, você pode querer pesquisar o gateway na rede ou no nó de administração principal.

   Especifique um intervalo usando um hífen, como mostrado no exemplo.

4. Insira um número de porta TCP, uma lista de portas separadas por vírgulas ou um intervalo de portas.



5. Clique em **testar conetividade**.

   - Se as conexões de rede no nível da porta selecionadas forem válidas, a mensagem ""Teste de conetividade de porta aprovado"" aparecerá em um banner verde. A saída do comando nmap está listada abaixo do banner.

   - Se uma conexão de rede no nível da porta for feita ao host remoto, mas o host não estiver ouvindo em uma ou mais das portas selecionadas, a mensagem ""Falha no teste de conetividade da porta"" aparecerá em um banner amarelo. A saída do comando nmap está listada abaixo do banner.

     Qualquer porta remota que o host não esteja ouvindo tem um estado de "fechado". Por exemplo, você pode ver esse banner amarelo quando o nó ao qual você está tentando se conetar estiver em um estado pré-instalado e o serviço StorageGRID NMS ainda não estiver sendo executado nesse nó.

- Se uma conexão de rede no nível de porta não puder ser feita para uma ou mais portas selecionadas, a mensagem "Falha no teste de conetividade de porta" aparecerá em um banner vermelho. A saída do comando nmap está listada abaixo do banner.

  O banner vermelho indica que uma tentativa de conexão TCP para uma porta no host remoto foi feita, mas nada foi retornado ao remetente. Quando nenhuma resposta é retornada, a porta tem um estado de "filtrada" e é provavelmente bloqueada por um firewall.

  Os portos com "fechado" também são listados.

Informações relacionadas

"Diretrizes de rede"

Acessando e configurando o Gerenciador do sistema do SANtricity

Você pode usar o Gerenciador de sistemas do SANtricity para monitorar o status das

controladoras de storage, discos de storage e outros componentes de hardware no compartimento de controladora de storage. Você também pode configurar um proxy para o e-Series AutoSupport que permite enviar mensagens AutoSupport do dispositivo sem o uso da porta de gerenciamento.

Configuração e acesso ao Gerenciador de sistema do SANtricity

Talvez seja necessário acessar o Gerenciador de sistema do SANtricity no controlador de storage para monitorar o hardware no compartimento de controladora de storage ou para configurar o e-Series AutoSupport.

O que você vai precisar

- Você está usando um navegador da Web compatível.
- Para acessar o Gerenciador de sistema do SANtricity por meio do Gerenciador de Grade, você deve ter instalado o StorageGRID e ter a permissão Administrador do dispositivo de armazenamento ou a permissão de acesso à raiz.
- Para acessar o Gerenciador de sistema do SANtricity usando o Instalador de dispositivos do StorageGRID, você deve ter o nome de usuário e a senha do administrador do Gerenciador de sistema do SANtricity.
- Para acessar diretamente o Gerenciador de sistema do SANtricity usando um navegador da Web, você deve ter o nome de usuário e a senha do administrador do Gerenciador de sistema do SANtricity.

> Você deve ter o firmware 8,70 ou superior do SANtricity para acessar o Gerenciador de sistema do SANtricity usando o Gerenciador de Grade ou o Instalador de dispositivos StorageGRID. Você pode verificar a versão do firmware usando o Instalador do StorageGRID Appliance e selecionando **Ajuda sobre**.

> O acesso ao Gerenciador de sistema do SANtricity a partir do Gerenciador de Grade ou do Instalador de dispositivos é geralmente destinado apenas para monitorar seu hardware e configurar o e-Series AutoSupport. Muitos recursos e operações no Gerenciador de sistemas do SANtricity, como atualização de firmware, não se aplicam ao monitoramento do dispositivo StorageGRID. Para evitar problemas, siga sempre as instruções de instalação e manutenção do hardware do seu aparelho.

Sobre esta tarefa

Há três maneiras de acessar o Gerenciador de sistema do SANtricity, dependendo de qual estágio do processo de instalação e configuração você está:

- Se o dispositivo ainda não tiver sido implantado como um nó no sistema StorageGRID, você deve usar a guia Avançado no Instalador de dispositivos StorageGRID.

  > Depois que o nó for implantado, você não poderá mais usar o Instalador de dispositivos StorageGRID para acessar o Gerenciador de sistemas do SANtricity.

- Se o dispositivo tiver sido implantado como um nó em seu sistema StorageGRID, use a guia Gerenciador de sistema do SANtricity na página nós no Gerenciador de Grade.
- Se você não puder usar o Instalador de dispositivos StorageGRID ou o Gerenciador de Grade, poderá acessar o Gerenciador de sistema do SANtricity diretamente usando um navegador da Web conetado à porta de gerenciamento.

Este procedimento inclui etapas para o seu acesso inicial ao Gerenciador de sistema do SANtricity. Se você já tiver configurado o Gerenciador de sistema do SANtricity, vá para a Configurar alertas de hardware etapa.

> O uso do Gerenciador de Grade ou do Instalador de dispositivos StorageGRID permite que você acesse o Gerenciador de sistema do SANtricity sem ter que configurar ou conetar a porta de gerenciamento do dispositivo.

Você usa o Gerenciador de sistema do SANtricity para monitorar o seguinte:

- Dados de performance, como performance em nível de storage array, latência de e/S, utilização de CPU e taxa de transferência
- Status do componente de hardware
- Funções de suporte, incluindo visualização de dados de diagnóstico

Você pode usar o Gerenciador de sistema do SANtricity para configurar as seguintes configurações:

- Alertas de e-mail, alertas SNMP ou alertas syslog para os componentes no compartimento do controlador de armazenamento
- Configurações do e-Series AutoSupport para os componentes no compartimento do controlador de storage.

  Para obter detalhes adicionais sobre o e-Series AutoSupport, consulte o centro de documentação do e-Series.

  "Site de Documentação de sistemas NetApp e-Series"

- Chaves de segurança da unidade, que são necessárias para desbloquear unidades seguras (esta etapa é necessária se o recurso Segurança da unidade estiver ativado)
- Senha de administrador para acessar o Gerenciador de sistema do SANtricity

Passos

1. Execute um dos seguintes procedimentos:

   - Use o Instalador do StorageGRID Appliance e selecione **Avançado Gerenciador do sistema SANtricity**
   - Use o Gerenciador de Grade e selecione **nós** * `***appliance Storage Node***`Gerenciador de sistema SANtricity*

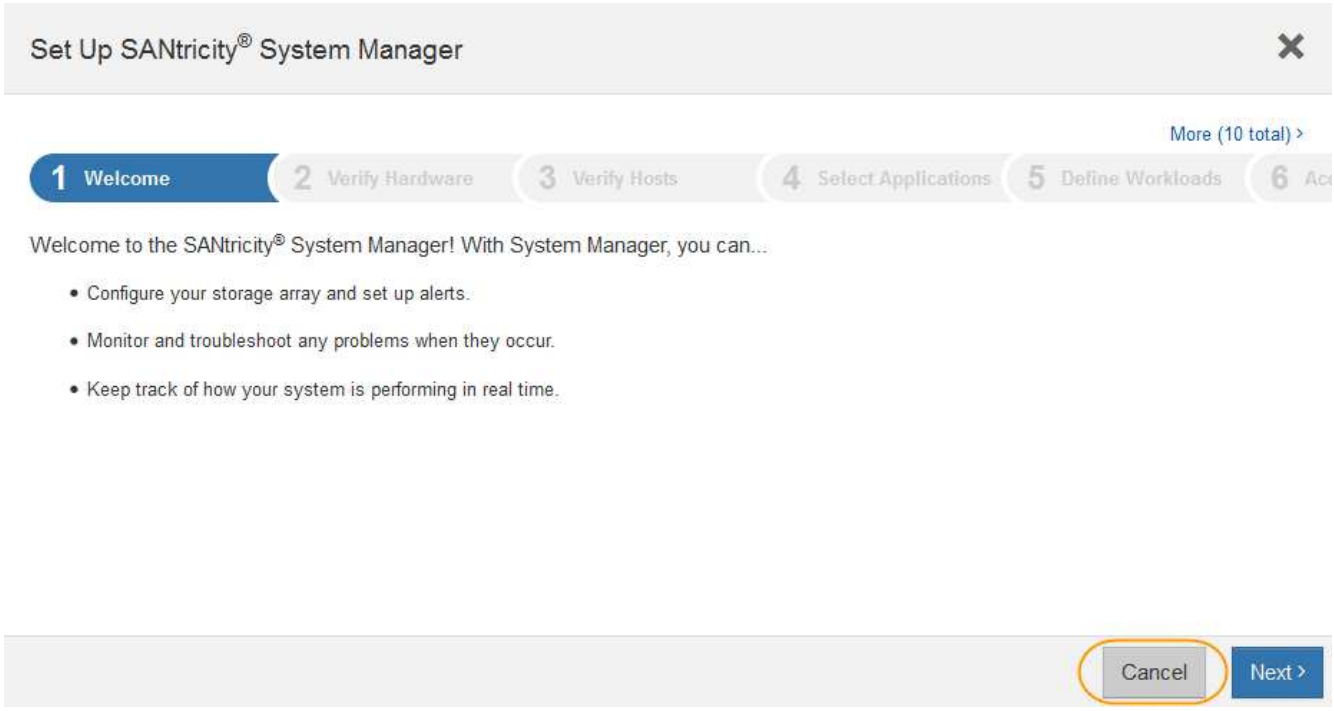
     > Se essas opções não estiverem disponíveis ou a página de login não aparecer, você deverá usar o endereço IP do controlador de armazenamento. Acesse o Gerenciador de sistema do SANtricity navegando para o IP do controlador de armazenamento `https://Storage_Controller_IP`

   É apresentada a página de início de sessão do Gestor do sistema SANtricity.

2. Defina ou introduza a palavra-passe do administrador.

   > O Gerenciador de sistema do SANtricity usa uma única senha de administrador que é compartilhada entre todos os usuários.

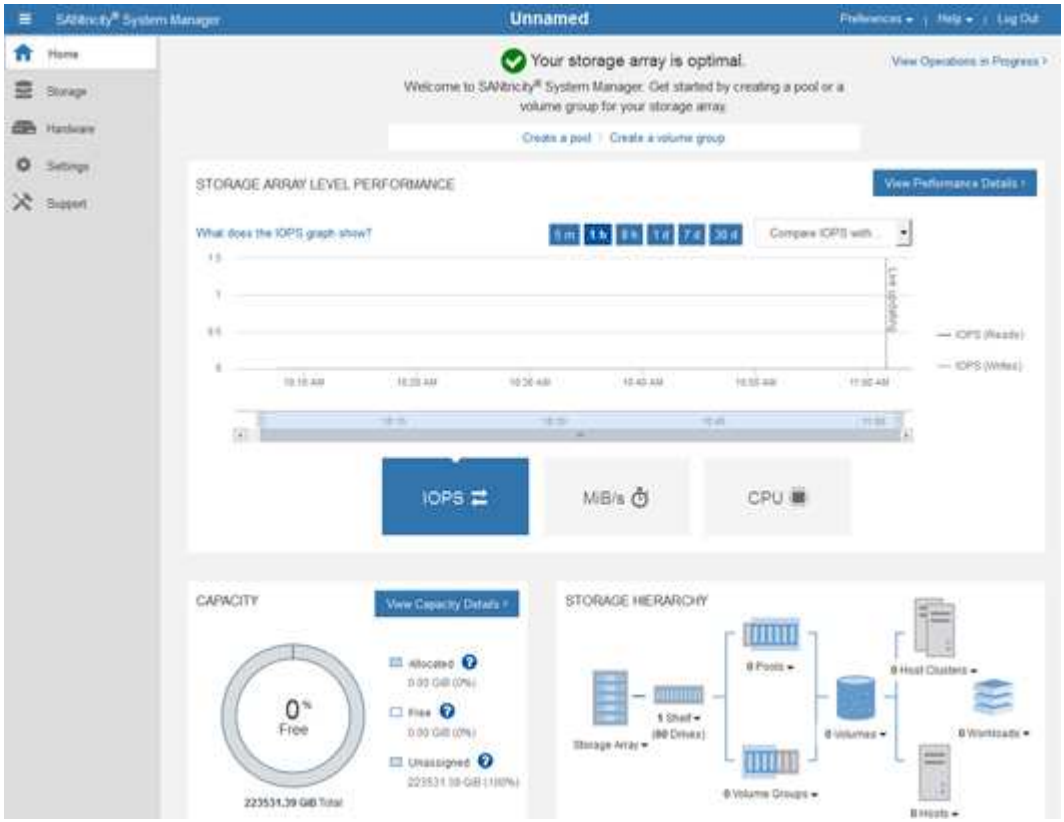
   O assistente de configuração é exibido.



3. Selecione **Cancelar** para fechar o assistente.

> Não conclua o assistente de configuração de um dispositivo StorageGRID.

É apresentada a página inicial do Gestor do sistema SANtricity.



1. Configurar alertas de hardware.

a. Selecione **Ajuda** para acessar a ajuda on-line do Gerenciador de sistemas do SANtricity.
b. Use a seção **Configurações Alertas** da ajuda on-line para saber mais sobre alertas.
c. Siga as instruções ""como fazer"" para configurar alertas de e-mail, alertas SNMP ou alertas syslog.

2. Gerenciar o AutoSupport para os componentes no compartimento do controlador de storage.

a. Selecione **Ajuda** para acessar a ajuda on-line do Gerenciador de sistemas do SANtricity.
b. Use a seção **suporte Centro de suporte** da ajuda on-line para saber mais sobre o recurso AutoSupport.
c. Siga as instruções ""como fazer"" para gerenciar o AutoSupport.

Para obter instruções específicas sobre como configurar um proxy StorageGRID para enviar mensagens AutoSupport da série e sem usar a porta de gerenciamento, vá para as instruções de administração do StorageGRID e procure "configurações de proxy para o e-Series AutoSupport".

"Administrar o StorageGRID"

3. Se o recurso Segurança da unidade estiver ativado para o dispositivo, crie e gerencie a chave de segurança.

a. Selecione **Ajuda** para acessar a ajuda on-line do Gerenciador de sistemas do SANtricity.
b. Use a seção **Configurações sistema Gerenciamento de chaves de segurança** da ajuda on-line para saber mais sobre a segurança da unidade.
c. Siga as instruções de "como fazer" para criar e gerenciar a chave de segurança.

4. Opcionalmente, altere a senha do administrador.

a. Selecione **Ajuda** para acessar a ajuda on-line do Gerenciador de sistemas do SANtricity.
b. Use a seção **Home Storage array Administration** da ajuda on-line para saber mais sobre a senha do administrador.
c. Siga as instruções "como" para alterar a senha.

Analisando o status do hardware no Gerenciador do sistema do SANtricity

Você pode usar o Gerenciador de sistema do SANtricity para monitorar e gerenciar componentes de hardware individuais no compartimento de controladora de storage e analisar informações ambientais e de diagnóstico de hardware, como temperaturas dos componentes, bem como problemas relacionados às unidades.

O que você vai precisar

- Você está usando um navegador da Web compatível.
- Para acessar o Gerenciador de sistema do SANtricity por meio do Gerenciador de Grade, você deve ter a permissão Administrador do dispositivo de armazenamento ou a permissão de acesso à raiz.
- Para acessar o Gerenciador de sistema do SANtricity usando o Instalador de dispositivos do StorageGRID, você deve ter o nome de usuário e a senha do administrador do Gerenciador de sistema do SANtricity.
- Para acessar diretamente o Gerenciador de sistema do SANtricity usando um navegador da Web, você deve ter o nome de usuário e a senha do administrador do Gerenciador de sistema do SANtricity.

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

O acesso ao Gerenciador de sistema do SANtricity a partir do Gerenciador de Grade ou do Instalador de dispositivos é geralmente destinado apenas para monitorar seu hardware e configurar o e-Series AutoSupport. Muitos recursos e operações no Gerenciador de sistemas do SANtricity, como atualização de firmware, não se aplicam ao monitoramento do dispositivo StorageGRID. Para evitar problemas, siga sempre as instruções de instalação e manutenção do hardware do seu aparelho.

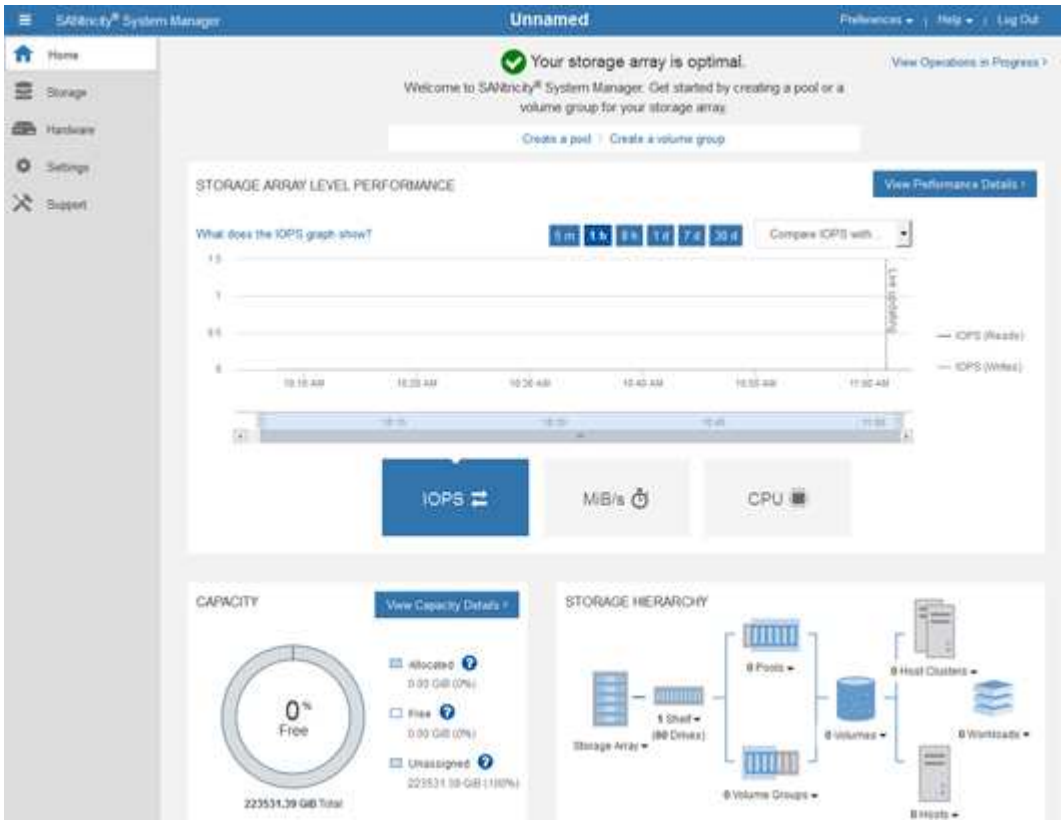
Passos

1. Acesse o Gerenciador do sistema do SANtricity.

   "Configuração e acesso ao Gerenciador de sistema do SANtricity"

2. Introduza o nome de utilizador e a palavra-passe do administrador, se necessário.
3. Clique em **Cancelar** para fechar o assistente de configuração e exibir a página inicial do Gerenciador do sistema SANtricity.

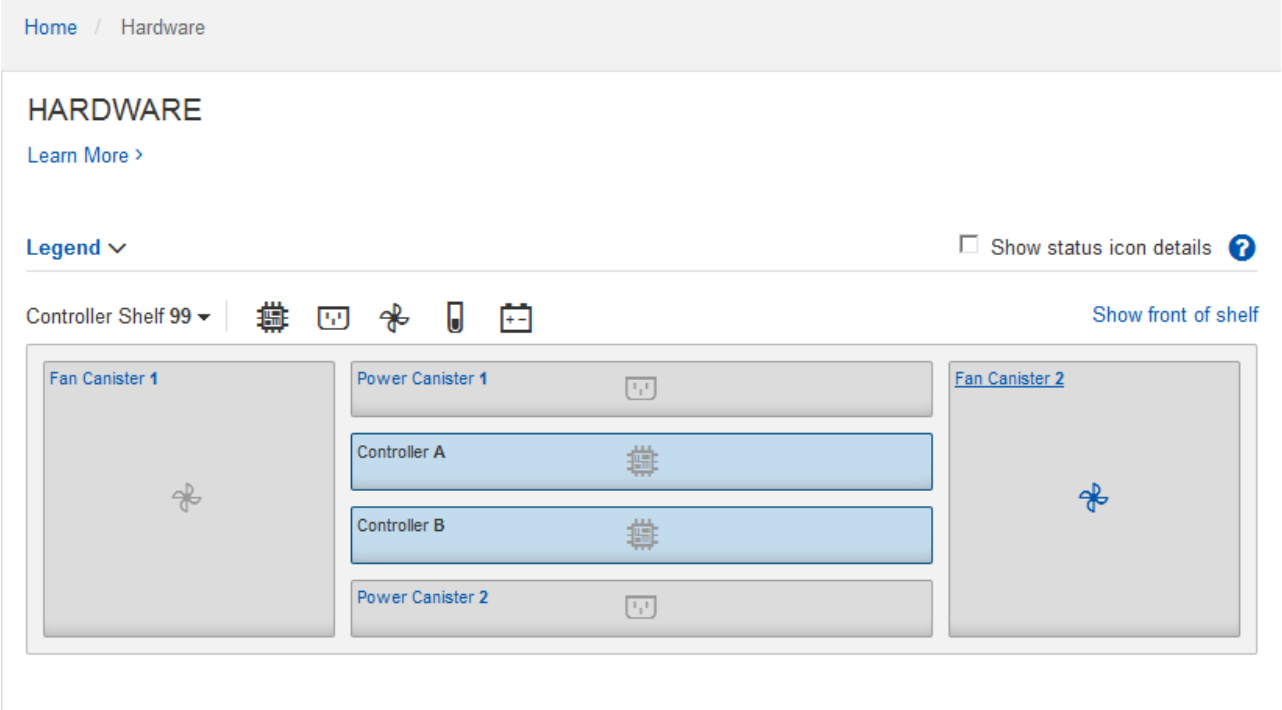
   É apresentada a página inicial do Gestor do sistema SANtricity. No Gerenciador de sistemas do SANtricity, o compartimento de controladora é chamado de storage array.



4. Revise as informações exibidas para o hardware do dispositivo e confirme se todos os componentes de hardware têm o status ideal.

   a. Clique na guia **hardware**.

   b. Clique em **Mostrar parte posterior da prateleira**.



Na parte de trás da gaveta, você pode visualizar os dois controladores de armazenamento, a bateria em cada controlador de armazenamento, os dois coletores de energia, os dois coletores de ventilador e os compartimentos de expansão (se houver). Também pode visualizar as temperaturas dos componentes.

a. Para ver as configurações de cada controlador de armazenamento, selecione o controlador e selecione **View settings** no menu de contexto.
b. Para ver as configurações de outros componentes na parte de trás da prateleira, selecione o componente que deseja exibir.
c. Clique em **Mostrar frente da prateleira** e selecione o componente que deseja exibir.

   Na parte da frente da gaveta, é possível visualizar as unidades e as gavetas de unidades da gaveta de controladora de armazenamento ou das gavetas de expansão (se houver).

Se o status de qualquer componente for necessário atenção, siga as etapas no Recovery Guru para resolver o problema ou entre em Contato com o suporte técnico.

Definir os endereços IP dos controladores de armazenamento utilizando o Instalador de dispositivos StorageGRID

A porta de gerenciamento 1 em cada controlador de storage coneta o dispositivo à rede de gerenciamento do Gerenciador de sistema do SANtricity. Se você não puder acessar o Gerenciador de sistema do SANtricity pelo Instalador de dispositivos StorageGRID, defina um endereço IP estático para cada controlador de armazenamento para garantir que não perca a conexão de gerenciamento com o hardware e o firmware da controladora no compartimento da controladora.

O que você vai precisar

- Você está usando qualquer cliente de gerenciamento que possa se conetar à rede de administração do StorageGRID ou tem um laptop de serviço.
- O cliente ou laptop de serviço tem um navegador da Web suportado.

Sobre esta tarefa

Os endereços atribuídos pelo DHCP podem ser alterados a qualquer momento. Atribua endereços IP estáticos aos controladores para garantir uma acessibilidade consistente.

Siga este procedimento somente se você não tiver acesso ao Gerenciador de sistemas SANtricity a partir do Instalador de dispositivos StorageGRID (**Avançado Gerenciador de sistemas SANtricity**) ou Gerenciador de Grade (**nós Gerenciador de sistemas SANtricity**).

Passos

1. No cliente, insira o URL para o instalador do StorageGRID Appliance
   `https://Appliance_Controller_IP:8443`

   Para *`Appliance_Controller_IP`*, use o endereço IP do dispositivo em qualquer rede StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configure hardware Storage Controller Network Configuration**.

   A página Configuração da rede do controlador de armazenamento é exibida.

3. Dependendo da configuração da rede, selecione **Enabled** para IPv4, IPv6 ou ambos.
4. Anote o endereço IPv4 que é exibido automaticamente.

   DHCP é o método padrão para atribuir um endereço IP à porta de gerenciamento do controlador de armazenamento.

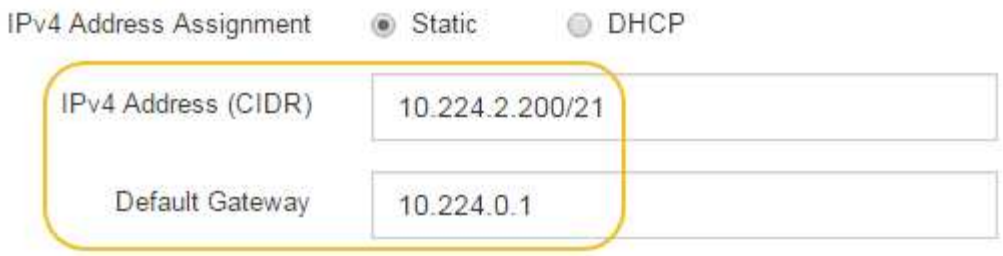
   Pode demorar alguns minutos para que os valores DHCP apareçam.

5. Opcionalmente, defina um endereço IP estático para a porta de gerenciamento do controlador de armazenamento.

   Você deve atribuir um IP estático para a porta de gerenciamento ou atribuir uma concessão permanente para o endereço no servidor DHCP.

   a. Selecione **estático**.
   b. Introduza o endereço IPv4, utilizando a notação CIDR.
   c. Introduza o gateway predefinido.



d. Clique em **Salvar**.

Pode levar alguns minutos para que suas alterações sejam aplicadas.

Quando você se conetar ao Gerenciador de sistema do SANtricity, você usará o novo endereço IP estático como URL
`https://Storage_Controller_IP`

Opcional: Habilitando a criptografia de nó

Se você ativar a criptografia de nó, os discos do seu dispositivo podem ser protegidos pela criptografia de servidor de gerenciamento de chaves (KMS) seguro contra perda física ou remoção do site. Você deve selecionar e ativar a criptografia de nó durante a instalação do dispositivo e não pode desmarcar a criptografia de nó depois que o processo de criptografia KMS for iniciado.

O que você vai precisar

Consulte as informações sobre o KMS nas instruções de administração do StorageGRID.

Sobre esta tarefa

Um dispositivo com criptografia de nó ativada se coneta ao servidor de gerenciamento de chaves externas (KMS) configurado para o site StorageGRID. Cada cluster KMS (ou KMS) gerencia as chaves de criptografia para todos os nós de dispositivo no local. Essas chaves criptografam e descriptografam os dados em cada disco em um dispositivo que tem criptografia de nó ativada.

Um KMS pode ser configurado no Gerenciador de Grade antes ou depois que o dispositivo é instalado no StorageGRID. Consulte as informações sobre a configuração do KMS e do appliance nas instruções de administração do StorageGRID para obter detalhes adicionais.

- Se um KMS for configurado antes de instalar o dispositivo, a criptografia controlada pelo KMS será iniciada quando você ativar a criptografia de nó no dispositivo e adicioná-la a um site do StorageGRID onde o KMS está configurado.
- Se um KMS não for configurado antes de instalar o dispositivo, a criptografia controlada por KMS é executada em cada dispositivo que tem criptografia de nó ativada assim que um KMS é configurado e disponível para o site que contém o nó do dispositivo.

> ⓘ Todos os dados existentes antes de um dispositivo que tenha criptografia de nó ativada se conetarem ao KMS configurado são criptografados com uma chave temporária que não é segura. O aparelho não está protegido contra remoção ou roubo até que a chave esteja definida para um valor fornecido pelo KMS.

Sem a chave KMS necessária para descriptografar o disco, os dados no dispositivo não podem ser recuperados e são efetivamente perdidos. Este é o caso sempre que a chave de descriptografia não pode ser

recuperada do KMS. A chave fica inacessível se um cliente limpar a configuração do KMS, uma chave KMS expira, a conexão com o KMS é perdida ou o dispositivo é removido do sistema StorageGRID onde suas chaves KMS são instaladas.

Passos

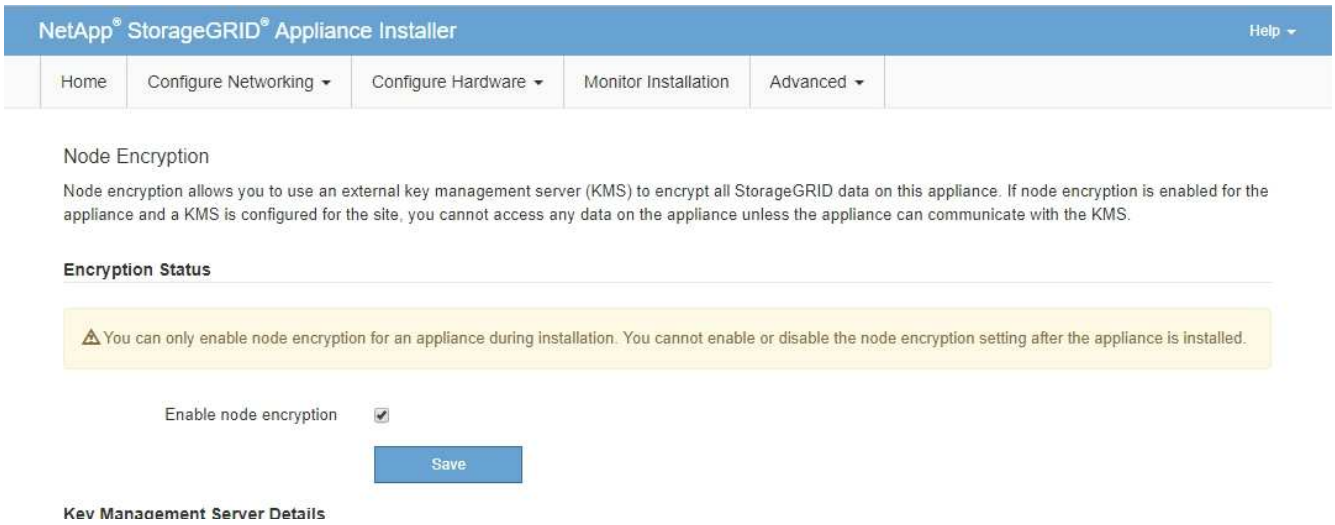
1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

   > Depois que o dispositivo tiver sido criptografado com uma chave KMS, os discos do appliance não podem ser descriptografados sem usar a mesma chave KMS.

2. Selecione **Configure hardware Node Encryption**.



3. Selecione **Ativar criptografia de nó**.

   Você pode desmarcar **Ativar criptografia de nó** sem risco de perda de dados até selecionar **Salvar** e o nó do dispositivo acessar as chaves de criptografia KMS em seu sistema StorageGRID e iniciar a criptografia de disco. Não é possível desativar a criptografia de nó após a instalação do dispositivo.

   > Depois de adicionar um dispositivo que tenha a criptografia de nó ativada a um site do StorageGRID que tenha um KMS, você não poderá parar de usar a criptografia KMS para o nó.

4. Selecione **Guardar**.
5. Implante o dispositivo como um nó no sistema StorageGRID.

   A encriptação controlada POR KMS começa quando o dispositivo acede às chaves KMS configuradas para o seu site StorageGRID. O instalador exibe mensagens de progresso durante o processo de criptografia KMS, o que pode levar alguns minutos, dependendo do número de volumes de disco no dispositivo.

Os dispositivos são configurados inicialmente com uma chave de criptografia aleatória não KMS atribuída a cada volume de disco. Os discos são criptografados usando essa chave de criptografia temporária, que não é segura, até que o dispositivo que tem criptografia de nó habilitada acesse as chaves KMS configuradas para o site do StorageGRID.

Depois de terminar

Você pode exibir o status da criptografia do nó, os detalhes do KMS e os certificados em uso quando o nó do dispositivo está no modo de manutenção.

Informações relacionadas

"Administrar o StorageGRID"

"Monitorização da encriptação do nó no modo de manutenção"

Opcional: Alterar o modo RAID (apenas SG5760)

Se tiver um SG5760 com 60 unidades, pode mudar para um modo RAID diferente para acomodar os seus requisitos de armazenamento e recuperação. Você só pode alterar o modo antes de implantar o nó de storage do dispositivo StorageGRID.

O que você vai precisar

- Você tem um SG5760. Se tiver um SG5712, tem de utilizar o modo DDP.
- Você está usando qualquer cliente que possa se conetar ao StorageGRID.
- O cliente tem um navegador da Web suportado.

Sobre esta tarefa

Antes de implantar o dispositivo SG5760 como nó de storage, você pode escolher uma das seguintes opções de configuração de volume:

- **DDP**: Esse modo usa duas unidades de paridade para cada oito unidades de dados. Este é o modo padrão e recomendado para todos os aparelhos. Em comparação com o RAID6, o DDP oferece melhor performance do sistema, tempos de reconstrução reduzidos após falhas de unidade e facilidade de gerenciamento. O DDP também fornece proteção contra perda de gaveta em dispositivos de 60 unidades.
- **DDP16**: Esse modo usa duas unidades de paridade para cada unidade de dados de 16 TB, o que resulta em maior eficiência de storage em comparação com o DDP. Em comparação com o RAID6, o DDP16 oferece melhor desempenho do sistema, tempos de reconstrução reduzidos após falhas de unidade, facilidade de gerenciamento e eficiência de storage comparável. Para usar o modo DDP16, sua configuração deve conter pelo menos 20 unidades. DDP16 não fornece proteção contra perda de gaveta.
- **RAID6**: Este modo usa duas unidades de paridade para cada 16 ou mais unidades de dados. Para usar o modo RAID 6, sua configuração deve conter pelo menos 20 unidades. Embora o RAID6 possa aumentar a eficiência de storage do dispositivo em comparação com o DDP, ele não é recomendado para a maioria dos ambientes StorageGRID.

Se algum volume já tiver sido configurado ou se o StorageGRID tiver sido instalado anteriormente, a alteração do modo RAID fará com que os volumes sejam removidos e substituídos. Quaisquer dados sobre esses volumes serão perdidos.

Passos

1. Usando o laptop de serviço, abra um navegador da Web e acesse o Instalador do StorageGRID Appliance

`https://E5700SG_Controller_IP:8443`

`_E5700SG_Controller_IP_`Onde está qualquer um dos endereços IP para o controlador E5700SG.

2. Selecione **Avançado modo RAID**.
3. Na página **Configurar modo RAID**, selecione o modo RAID desejado na lista suspensa modo.
4. Clique em **Salvar**.

Informações relacionadas

"Site de Documentação de sistemas NetApp e-Series"

Opcional: Remapeamento de portas de rede para o dispositivo

Talvez seja necessário remapear as portas internas no nó de armazenamento do dispositivo para diferentes portas externas. Por exemplo, talvez seja necessário remapear as portas devido a um problema de firewall.

O que você vai precisar

- Você acessou anteriormente o Instalador de dispositivos StorageGRID.
- Você não configurou e não planeja configurar pontos de extremidade do balanceador de carga.

> Se você remapear quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Se você quiser configurar pontos de extremidade do balanceador de carga e já tiver portas remapeadas, siga as etapas nas instruções de recuperação e manutenção para remover os remapes de portas.

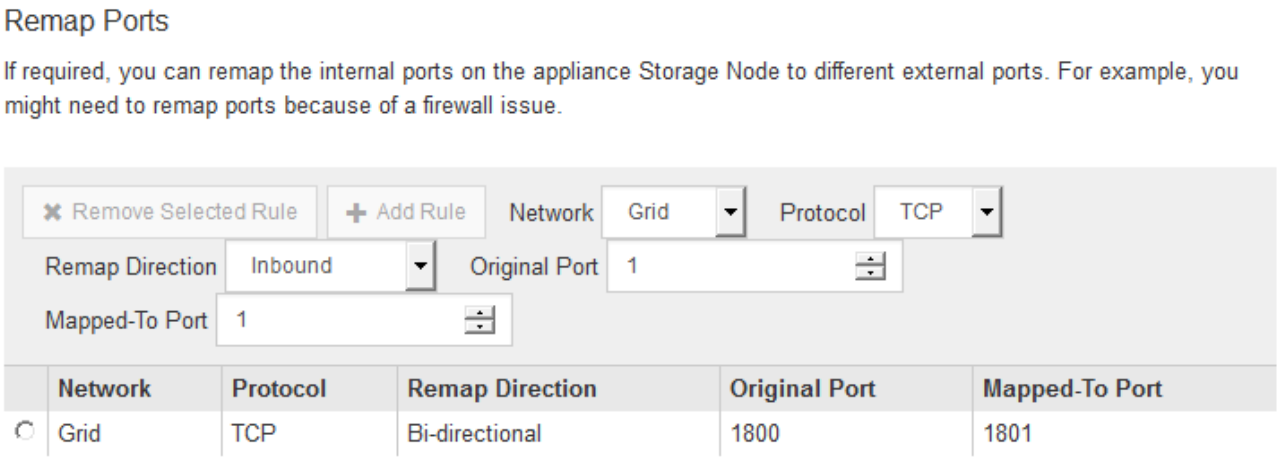
Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Remapear portas**.

   É apresentada a página Remapear porta.

2. Na caixa suspensa **rede**, selecione a rede para a porta que deseja remapear: Grade, Admin ou Cliente.
3. Na caixa suspensa **Protocol** (Protocolo), selecione o protocolo IP: TCP ou UDP.
4. Na caixa suspensa **Remap Direction**, selecione qual direção de tráfego você deseja remapear para esta porta: Inbound, Outbound ou Bi-direcional.
5. Para **original Port**, insira o número da porta que deseja remapear.
6. Para **Mapped-to Port**, insira o número da porta que deseja usar.
7. Clique em **Adicionar regra**.

   O novo mapeamento de portas é adicionado à tabela e o remapeamento entra em vigor imediatamente.



8. Para remover um mapeamento de portas, selecione o botão de opção da regra que deseja remover e clique em **Remover regra selecionada**.

Implantando um nó de storage de dispositivos

Depois de instalar e configurar o dispositivo de storage, você pode implantá-lo como um nó de storage em um sistema StorageGRID. Ao implantar um dispositivo como nó de storage, você usa o Instalador de dispositivos StorageGRID incluído no dispositivo.

O que você vai precisar

- Se você estiver clonando um nó de dispositivo, continue seguindo o processo de recuperação e manutenção.

  "Manter recuperar"

- O dispositivo foi instalado em um rack ou gabinete, conetado às redes e ligado.
- Links de rede, endereços IP e remapeamento de portas (se necessário) foram configurados para o dispositivo usando o Instalador de dispositivos StorageGRID.
- Você conhece um dos endereços IP atribuídos ao controlador de computação do dispositivo. Você pode usar o endereço IP de qualquer rede StorageGRID conetada.
- O nó de administração principal do sistema StorageGRID foi implantado.
- 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.
- Você tem um laptop de serviço com um navegador da Web suportado.

Sobre esta tarefa

Cada dispositivo de storage funciona como um nó de storage único. Qualquer dispositivo pode se conetar à rede de Grade, à rede Admin e à rede Cliente

Para implantar um nó de armazenamento de dispositivos em um sistema StorageGRID, você acessa o Instalador de dispositivos StorageGRID e executa as seguintes etapas:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do nó de armazenamento.
- Você inicia a implantação e espera à medida que os volumes são configurados e o software é instalado.

- Quando a instalação é interrompida parcialmente nas tarefas de instalação do dispositivo, você retoma a instalação iniciando sessão no Gerenciador de Grade, aprovando todos os nós de grade e concluindo os processos de instalação e implantação do StorageGRID.

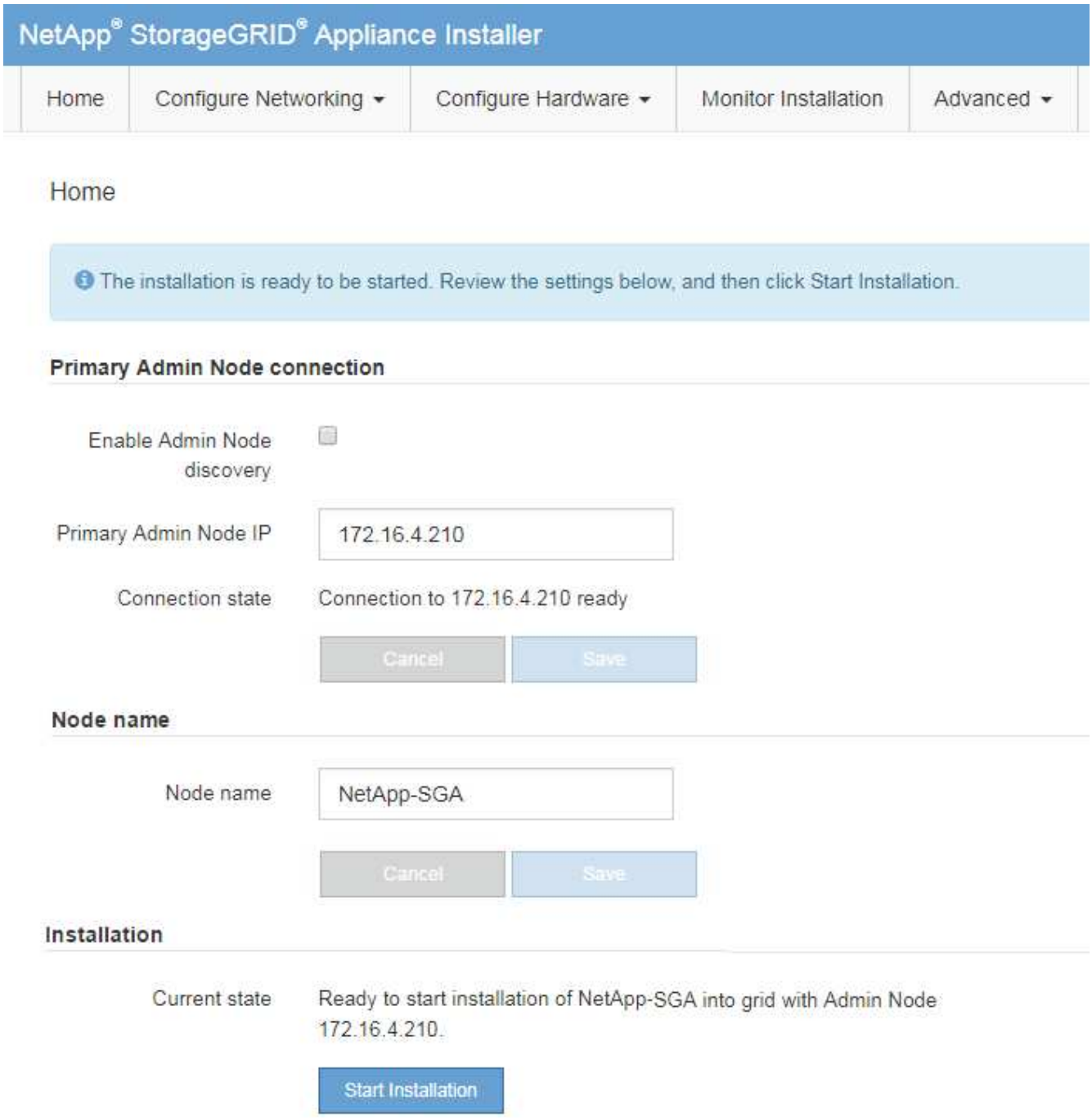
> Se você precisar implantar vários nós de dispositivo de uma só vez, você pode automatizar o processo de instalação usando o `configure-sga.py` script de instalação do dispositivo.

- Se você estiver executando uma operação de expansão ou recuperação, siga as instruções apropriadas:
  - Para adicionar um nó de storage do dispositivo a um sistema StorageGRID existente, consulte as instruções para expandir um sistema StorageGRID.
  - Para implantar um nó de armazenamento de dispositivos como parte de uma operação de recuperação, consulte as instruções para recuperação e manutenção.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `https://Controller_IP:8443`

   A página inicial do instalador do dispositivo StorageGRID é exibida.



2. Na seção **conexão do 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 clique em **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 `node name` na grade com nó Admin principal `*admin_ip*`" e se o botão **Iniciar instalação** está ativado.

   Se o botão **Start Installation** (Iniciar instalação) não estiver ativado, poderá ser necessário alterar a configuração da rede ou as definições da porta. Para obter instruções, consulte as instruções de instalação e manutenção do seu aparelho.

   > Se você estiver implantando o dispositivo Storage Node como um destino de clonagem de nós, interrompa o processo de implantação aqui e continue o procedimento de clonagem de nós no "Manter recuperar".

6. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.

   O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

   > Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor**.

7. Se a grade incluir vários nós de storage do dispositivo, repita estas etapas 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 `configure-sga.py` script de instalação do dispositivo. Este script se aplica somente aos nós de storage.

Informações relacionadas

"Expanda sua grade"

"Manter recuperar"

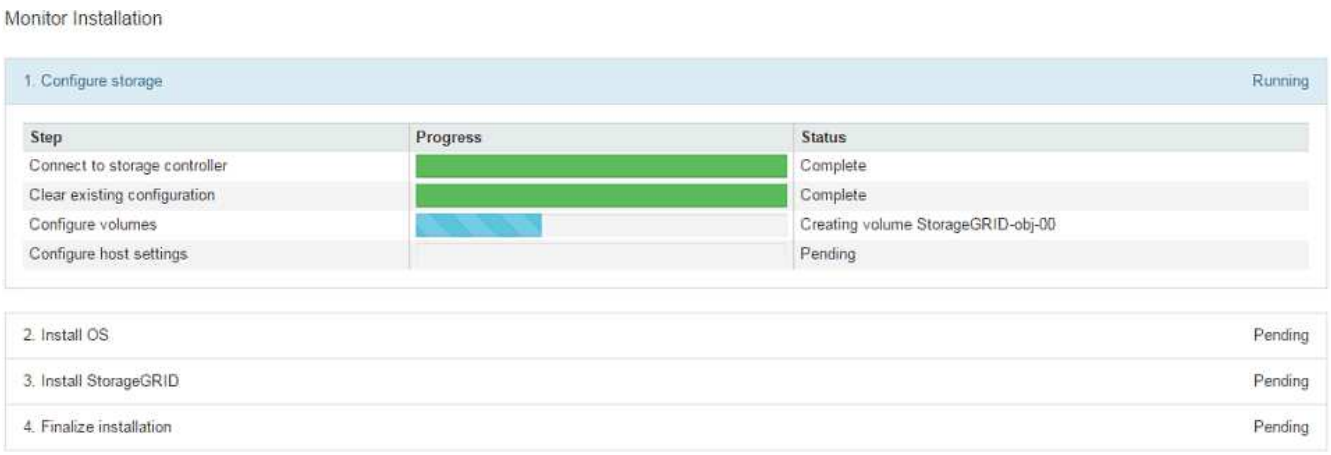
Monitorização da instalação do dispositivo de armazenamento

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**.

   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 serão mostradas com uma barra de status verde e um status de ""pulado"".

2. Reveja o progresso das duas primeiras fases de instalação.

   1. Configurar armazenamento

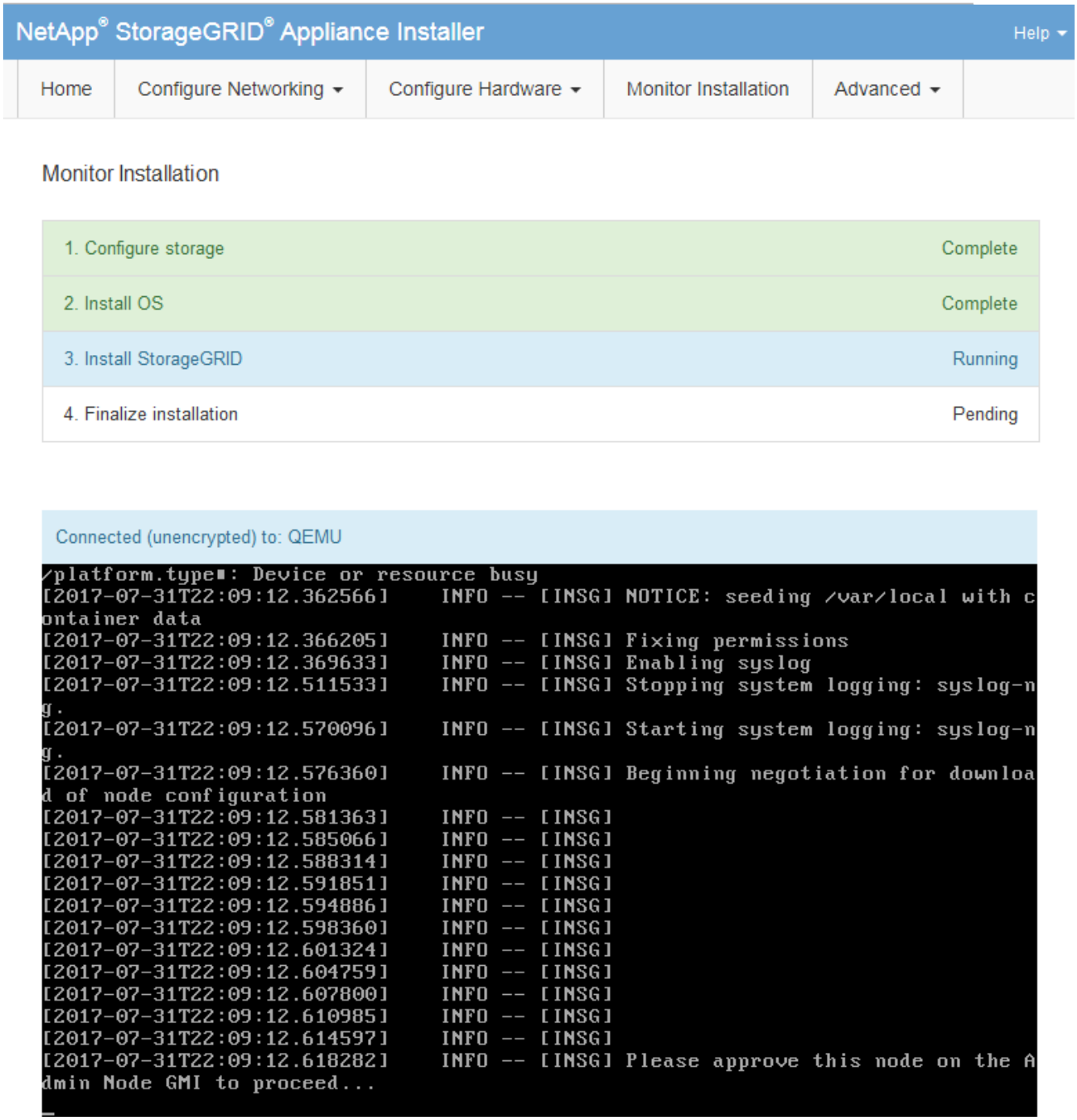
   Durante essa etapa, o instalador se coneta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o software SANtricity para configurar volumes e configura as configurações do host.

   2. Instale o os

   Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID para o dispositivo.

3. Continue monitorando o progresso da instalação até que o estágio **Install StorageGRID** pare e uma mensagem seja exibida no console incorporado, solicitando que você aprove esse nó no nó Admin usando

o Gerenciador de Grade. Vá para a próxima etapa.



4. Vá para o Gerenciador de Grade, aprove o nó de armazenamento pendente e conclua o processo de instalação do StorageGRID.

   Quando você clica em **Install** no Gerenciador de Grade, o estágio 3 é concluído e o estágio 4, **Finalize a instalação**, começa. Quando a fase 4 é concluída, o controlador é reinicializado.

Automatizando a instalação e a configuração do dispositivo

Você pode automatizar a instalação e configuração de seus dispositivos e a configuração de todo o sistema StorageGRID.

Sobre esta tarefa

A automação da instalação e configuração pode ser útil para implantar várias instâncias do StorageGRID ou uma instância grande e complexa do StorageGRID.

Para automatizar a instalação e a configuração, use uma ou mais das seguintes opções:

- Crie um arquivo JSON que especifique as configurações para seus dispositivos. Carregue o arquivo JSON usando o instalador do dispositivo StorageGRID.

  Você pode usar o mesmo arquivo para configurar mais de um dispositivo.

- Use o script Python do StorageGRID`configure-sga.py` para automatizar a configuração de seus dispositivos.
- Use scripts Python adicionais para configurar outros componentes de todo o sistema StorageGRID (a "grade").

Você pode usar os scripts Python de automação do StorageGRID diretamente ou usá-los como exemplos de como usar a API REST de instalação do StorageGRID nas ferramentas de implantação e configuração de grade que você mesmo desenvolve. Consulte as informações sobre como baixar e extrair os arquivos de instalação do StorageGRID nas instruções de recuperação e manutenção.

Automatizando a configuração do dispositivo usando o Instalador de dispositivos StorageGRID

Você pode automatizar a configuração de um appliance usando um arquivo JSON que contém as informações de configuração. Você carrega o arquivo usando o Instalador do StorageGRID Appliance.

O que você vai precisar

- O seu dispositivo tem de estar no firmware mais recente compatível com o StorageGRID 11,5 ou superior.
- Você deve estar conetado ao Instalador do StorageGRID Appliance no dispositivo que você está configurando usando um navegador compatível.

Sobre esta tarefa

É possível automatizar as tarefas de configuração do dispositivo, como configurar o seguinte:

- Rede de grade, rede de administração e endereços IP da rede de cliente
- Interface BMC
- Ligações de rede
  - Modo de ligação da porta
  - Modo de ligação de rede
  - Velocidade da ligação

Configurar o dispositivo usando um arquivo JSON carregado geralmente é mais eficiente do que executar a configuração manualmente usando várias páginas no Instalador de dispositivos StorageGRID, especialmente se você tiver que configurar muitos nós. Você deve aplicar o arquivo de configuração para cada nó um de cada vez.

Usuários experientes que desejam automatizar tanto a instalação quanto a configuração de seus dispositivos podem usar o `configure-sga.py` script. E "Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py"

Passos

1. Gere o arquivo JSON usando um dos seguintes métodos:
   - O aplicativo ConfigBuilder

     "ConfigBuilder.NetApp.com"

   - O `configure-sga.py` script de configuração do dispositivo. Você pode baixar o script do Instalador do StorageGRID Appliance (**Ajuda Script de configuração do appliance**). Consulte as instruções sobre como automatizar a configuração usando o script configure-sga.py.

     "Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py"

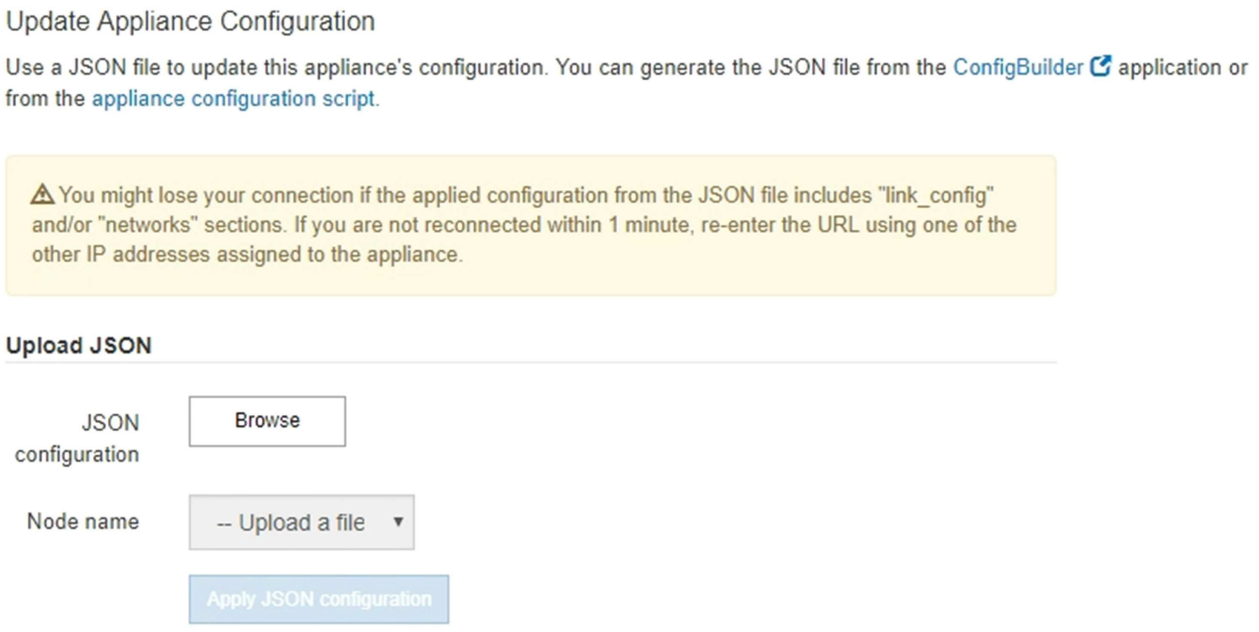
     Os nomes de nós no arquivo JSON devem seguir estes requisitos:

     - Deve ser um nome de host válido contendo pelo menos 1 e não mais de 32 carateres
     - Pode usar letras, números e hífens são permitidos
     - Não é possível iniciar ou terminar com um hífen ou conter apenas números

     Certifique-se de que os nomes dos nós (os nomes de nível superior) no arquivo JSON sejam únicos, ou você não poderá configurar mais de um nó usando o arquivo JSON.

2. Selecione **Avançado Atualizar Configuração do dispositivo**.

   É apresentada a página Update Appliance Configuration (Atualizar configuração do dispositivo).



3. Selecione o arquivo JSON com a configuração que você deseja carregar.

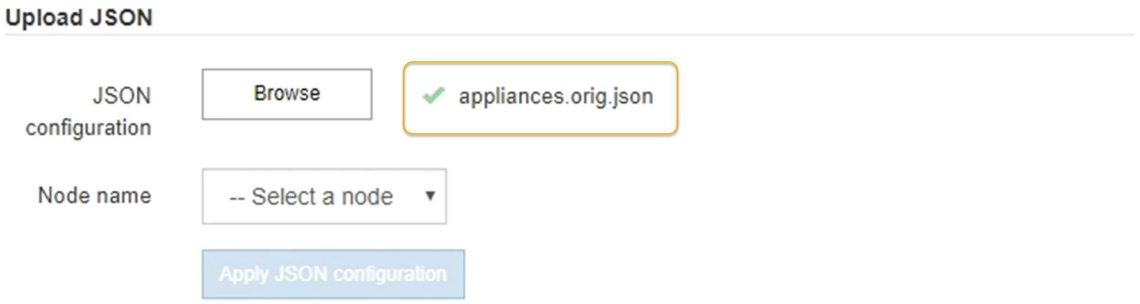
   a. Selecione **Procurar**.

   b. Localize e selecione o ficheiro.

   c. Selecione **Open**.

   O arquivo é carregado e validado. Quando o processo de validação estiver concluído, o nome do ficheiro é apresentado junto a uma marca de verificação verde.

   > Você pode perder a conexão com o dispositivo se a configuração do arquivo JSON incluir seções para "link_config", "redes" ou ambos. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do dispositivo usando um dos outros endereços IP atribuídos ao dispositivo.

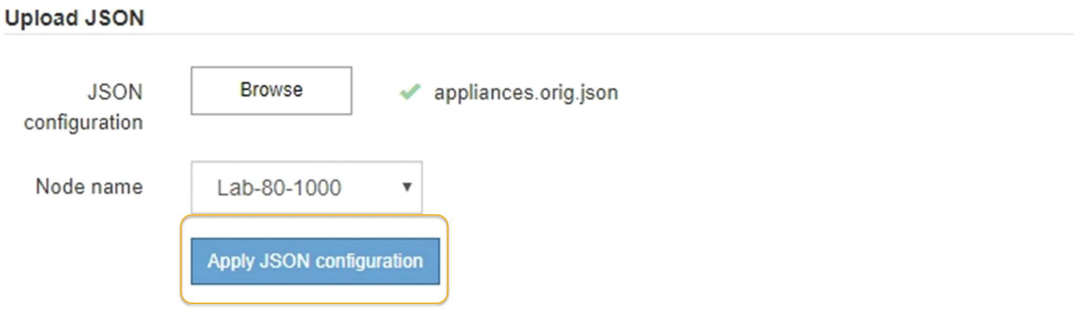


   A lista suspensa **Nome do nó** é preenchida com os nomes de nós de nível superior definidos no arquivo JSON.

   > Se o arquivo não for válido, o nome do arquivo será exibido em vermelho e uma mensagem de erro será exibida em um banner amarelo. O ficheiro inválido não é aplicado ao dispositivo. Você pode usar o ConfigBuilder para garantir que você tenha um arquivo JSON válido.

4. Selecione um nó na lista suspensa **Nome do nó**.

   O botão **Apply JSON Configuration** está ativado.



5. Selecione **Apply JSON Configuration**.

   A configuração é aplicada ao nó selecionado.

Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py

Você pode usar `configure-sga.py` o script para automatizar muitas das tarefas de instalação e configuração para os nós de dispositivos StorageGRID, incluindo a instalação e configuração de um nó de administrador principal. Este script pode ser útil se você tiver um grande número de dispositivos para configurar. Você também pode usar o script para gerar um arquivo JSON que contém informações de configuração do dispositivo.

Sobre esta tarefa

- O dispositivo foi instalado em um rack, conetado às redes e ligado.
- Links de rede e endereços IP foram configurados para o nó de administração principal usando o instalador do dispositivo StorageGRID.
- Se você estiver instalando o nó Admin principal, você saberá seu endereço IP.
- Se você estiver instalando e configurando outros nós, o nó Admin principal foi implantado e você sabe seu endereço IP.
- Para todos os nós que não o nó de administração principal, 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.
- Você baixou o `configure-sga.py` arquivo. O arquivo está incluído no arquivo de instalação, ou você pode acessá-lo clicando em **Ajuda Script de Instalação do dispositivo** no Instalador do StorageGRID Appliance.

> ⓘ Este procedimento é para usuários avançados com alguma experiência usando interfaces de linha de comando. Como alternativa, você também pode usar o Instalador de dispositivos StorageGRID para automatizar a configuração. E "Automatizando a configuração do dispositivo usando o Instalador de dispositivos StorageGRID"

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Para obter ajuda geral com a sintaxe do script e para ver uma lista dos parâmetros disponíveis, digite o seguinte:

   ```
   configure-sga.py --help
   ```

   O `configure-sga.py` script usa cinco subcomandos:

   - `advanced` Para interações avançadas do StorageGRID Appliance, incluindo a configuração do BMC e a criação de um arquivo JSON contendo a configuração atual do dispositivo
   - `configure` Para configurar o modo RAID, o nome do nó e os parâmetros de rede
   - `install` Para iniciar uma instalação do StorageGRID
   - `monitor` Para monitorar uma instalação do StorageGRID
   - `reboot` para reiniciar o aparelho

   Se você inserir um argumento de subcomando (avançado, configurar, instalar, monitorar ou reiniciar)

seguido da `--help` opção, você receberá um texto de ajuda diferente fornecendo mais detalhes sobre as opções disponíveis dentro desse subcomando
`configure-sga.py` *`subcommand`* `--help`

3. Para confirmar a configuração atual do nó do dispositivo, digite o seguinte local *`SGA-install-ip`* onde está qualquer um dos endereços IP do nó do dispositivo
`configure-sga.py configure` *`SGA-INSTALL-IP`*

   Os resultados mostram informações de IP atuais para o dispositivo, incluindo o endereço IP do nó de administração principal e informações sobre as redes de administração, grade e cliente.

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
```

```
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4

        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

####################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
####################################################################
```

4. Se você precisar alterar qualquer um dos valores na configuração atual, use o `configure` subcomando

para atualizá-los. Por exemplo, se você quiser alterar o endereço IP que o dispositivo usa para conexão com o nó Admin principal para `172.16.2.99`, digite o seguinte
`configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP`

5. Se você quiser fazer backup da configuração do appliance em um arquivo JSON, use os `advanced` subcomandos e `backup-file` . Por exemplo, se você quiser fazer backup da configuração de um dispositivo com endereço IP *`SGA-INSTALL-IP`* para um arquivo chamado `appliance-SG1000.json`, digite o seguinte
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

   O arquivo JSON contendo as informações de configuração é gravado no mesmo diretório do qual você executou o script.

   > Verifique se o nome do nó de nível superior no arquivo JSON gerado corresponde ao nome do dispositivo. Não faça alterações neste arquivo, a menos que você seja um usuário experiente e tenha uma compreensão completa das APIs do StorageGRID.

6. Quando estiver satisfeito com a configuração do aparelho, utilize os `install` subcomandos e `monitor` para instalar o aparelho
`configure-sga.py install --monitor SGA-INSTALL-IP`

7. Se pretender reiniciar o aparelho, introduza o seguinte
`configure-sga.py reboot SGA-INSTALL-IP`

Automatizando a configuração do StorageGRID

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

O que você vai precisar

- 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 amostra (`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
   ```

Depois de terminar

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, você precisa extrair o `Passwords.txt` arquivo e procurar 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.
```

Visão geral das APIs REST de instalação

O StorageGRID fornece duas APIs REST para executar tarefas de instalação: A API de instalação do StorageGRID e a API do instalador do dispositivo StorageGRID.

Ambas as APIs usam 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 (JavaScript Object Notation).

> Todas as operações de API que você executa usando a página da Web do API Docs 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 seu sistema StorageGRID e, caso precise 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.

API do instalador do dispositivo StorageGRID

A API do instalador do dispositivo StorageGRID pode ser acessada por HTTPS a partir `*Controller_IP*:8443`do .

Para acessar a documentação da API, vá para o Instalador do StorageGRID Appliance no appliance e

selecione **Ajuda Documentação da API** na barra de menus.

A API do instalador do StorageGRID Appliance inclui as seguintes seções:

- **Clone** — operações para configurar e controlar a clonagem de nós.
- **Encryption** — operações para gerenciar a criptografia e visualizar o status da criptografia.
- **Configuração de hardware** — operações para configurar as configurações do sistema no hardware conetado.
- **Installation** — operações para iniciar a instalação do aparelho e para monitorar o status da instalação.
- **Networking** — operações relacionadas à configuração de rede, administrador e rede cliente para um dispositivo StorageGRID e configurações de porta de dispositivo.
- **Setup** — operações para ajudar na configuração inicial da instalação do dispositivo, incluindo solicitações para obter informações sobre o sistema e atualizar o IP do nó de administração principal.
- **Support** — operações para reiniciar o controlador e obter logs.
- **Upgrade** — operações relacionadas à atualização do firmware do appliance.
- * Uploadsg* — operações para upload de arquivos de instalação do StorageGRID.

Solução de problemas da instalação do hardware

Se você encontrar problemas durante a instalação, talvez seja útil revisar informações de solução de problemas relacionadas a problemas de configuração de hardware e conetividade.

Informações relacionadas

"A configuração do hardware parece travar"

"Solução de problemas de conexão"

A configuração do hardware parece travar

O Instalador de dispositivos StorageGRID pode não estar disponível se falhas de hardware ou erros de cabeamento impedirem que a controladora E5700SG conclua seu processamento de inicialização.

Passos

1. Observe os códigos nos visores de sete segmentos.

   Enquanto o hardware está sendo inicializado durante a inicialização, os dois visores de sete segmentos mostram uma sequência de códigos. Quando o hardware é inicializado com êxito, as telas de sete segmentos mostram códigos diferentes para cada controlador.

2. Reveja os códigos no visor de sete segmentos para o controlador E5700SG.

   > A instalação e o provisionamento demoram. Algumas fases de instalação não relatam atualizações para o instalador do StorageGRID Appliance por vários minutos.

   Se ocorrer um erro, o visor de sete segmentos pisca uma sequência, COMO HE.

3. Para entender o que esses códigos significam, consulte os seguintes recursos:

Controlador	Referência
Controlador E5700SG	• "Indicadores de status no controlador E5700SG" • "HE error: Erro ao sincronizar com o software SANtricity os"
Controlador E2800	*Guia de monitorização do sistema E5700 e E2800* **Nota:** os códigos descritos para o controlador e-Series E5700 não se aplicam ao controlador E5700SG no aparelho.

4. Se isso não resolver o problema, entre em Contato com o suporte técnico.

Informações relacionadas

"Indicadores de status no controlador E5700SG"

"Erro HE: Erro ao sincronizar com o software SANtricity os"

"Site de Documentação de sistemas NetApp e-Series"

Erro HE: Erro ao sincronizar com o software SANtricity os

A exibição de sete segmentos no controlador de computação mostra um código de erro HE se o Instalador de dispositivos StorageGRID não puder sincronizar com o software SANtricity os.

Sobre esta tarefa

Se for apresentado um código de erro HE, efetue esta ação corretiva.

Passos

1. Verifique os dois cabos de interconexão entre os dois controladores e confirme se os cabos e transcetores SFP estão bem conetados.
2. Conforme necessário, substitua um ou ambos os cabos ou transcetores SFP e tente novamente.
3. Se isso não resolver o problema, entre em Contato com o suporte técnico.

Solução de problemas de conexão

Se você encontrar problemas de conexão durante a instalação do StorageGRID Appliance, execute as etapas de ação corretiva listadas.

Não foi possível ligar ao aparelho

Se não conseguir ligar ao dispositivo, poderá haver um problema de rede ou a instalação do hardware poderá não ter sido concluída com êxito.

Passos

1. Se você não conseguir se conetar ao Gerenciador do sistema do SANtricity:
   a. Tente fazer ping no dispositivo usando o endereço IP do controlador E2800 na rede de gerenciamento para o Gerenciador de sistema SANtricity
   ping *E2800_Controller_IP*
   b. Se não receber resposta do ping, confirme que está a utilizar o endereço IP correto.

      Use o endereço IP para a porta de gerenciamento 1 no controlador E2800.

   c. Se o endereço IP estiver correto, verifique o cabeamento do dispositivo e a configuração da rede.

      Se isso não resolver o problema, entre em Contato com o suporte técnico.

   d. Se o ping foi bem-sucedido, abra um navegador da Web.
   e. Digite o URL para o Gerenciador de sistema do SANtricity
   https://*E2800_Controller_IP*

      É apresentada a página de início de sessão do Gestor do sistema SANtricity.

2. Se não conseguir ligar ao controlador E5700SG:
   a. Tente fazer ping no aparelho usando o endereço IP do controlador E5700SG
   ping *E5700SG_Controller_IP*
   b. Se não receber resposta do ping, confirme que está a utilizar o endereço IP correto.

      Pode utilizar o endereço IP do dispositivo na rede de grelha, na rede de administração ou na rede de cliente.

   c. Se o endereço IP estiver correto, verifique o cabeamento do dispositivo, os transcetores SFP e a configuração da rede.

      Se isso não resolver o problema, entre em Contato com o suporte técnico.

   d. Se o ping foi bem-sucedido, abra um navegador da Web.
   e. Digite o URL do instalador do StorageGRID Appliance
   https://*E5700SG_Controller_IP*:8443

      A página inicial é exibida.

Reinicializando o controlador enquanto o Instalador de dispositivos StorageGRID está em execução

Talvez seja necessário reiniciar o controlador de computação enquanto o Instalador de dispositivos StorageGRID estiver em execução. Por exemplo, você pode precisar reiniciar o controlador se a instalação falhar.

Sobre esta tarefa

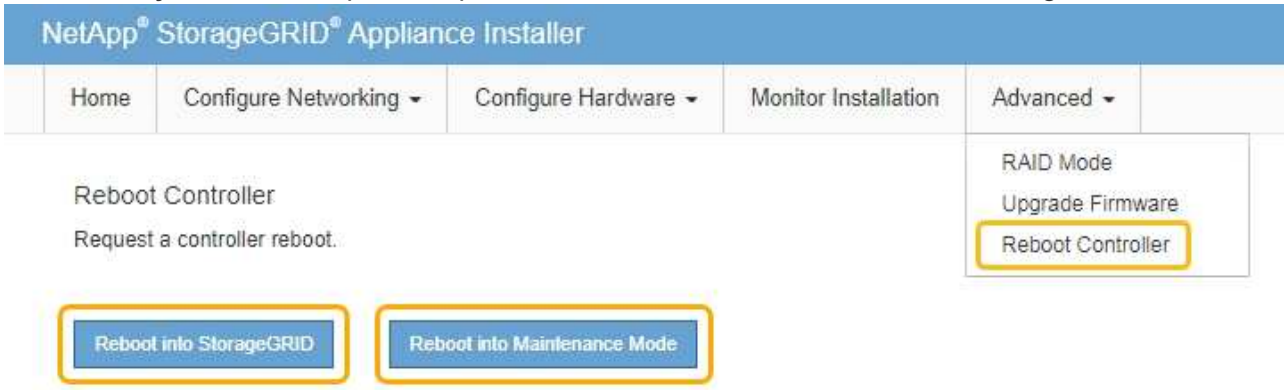
Este procedimento só se aplica quando o controlador de computação está executando o Instalador de dispositivos StorageGRID. Depois que a instalação estiver concluída, esta etapa não funcionará mais porque o Instalador de dispositivos StorageGRID não está mais disponível.

Passos

1. No Instalador do StorageGRID Appliance, clique em **Avançado controlador de reinicialização** e

selecione uma destas opções:

- Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
- Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



O controlador SG6000-CN é reinicializado.

Manutenção do aparelho SG5700

Talvez seja necessário atualizar o software SANtricity os na controladora E2800, alterar a configuração do link Ethernet da controladora E5700SG, substituir a controladora E2800 ou a controladora E5700SG ou substituir componentes específicos. Os procedimentos nesta seção pressupõem que o dispositivo já foi implantado como nó de storage em um sistema StorageGRID.

Passos

- "Colocar um aparelho no modo de manutenção"
- "Atualizando o SANtricity os no controlador de storage"
- "Atualizando o firmware da unidade usando o Gerenciador de sistema do SANtricity"
- "Substituição do controlador E2800"
- "Substituição do controlador E5700SG"
- "Substituição de outros componentes de hardware"
- "Alterar a configuração do link do controlador E5700SG"
- "Alterar a definição MTU"
- "Verificar a configuração do servidor DNS"
- "Monitorização da encriptação do nó no modo de manutenção"

Colocar um aparelho no modo de manutenção

Deve colocar o aparelho no modo de manutenção antes de efetuar procedimentos de

manutenção específicos.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

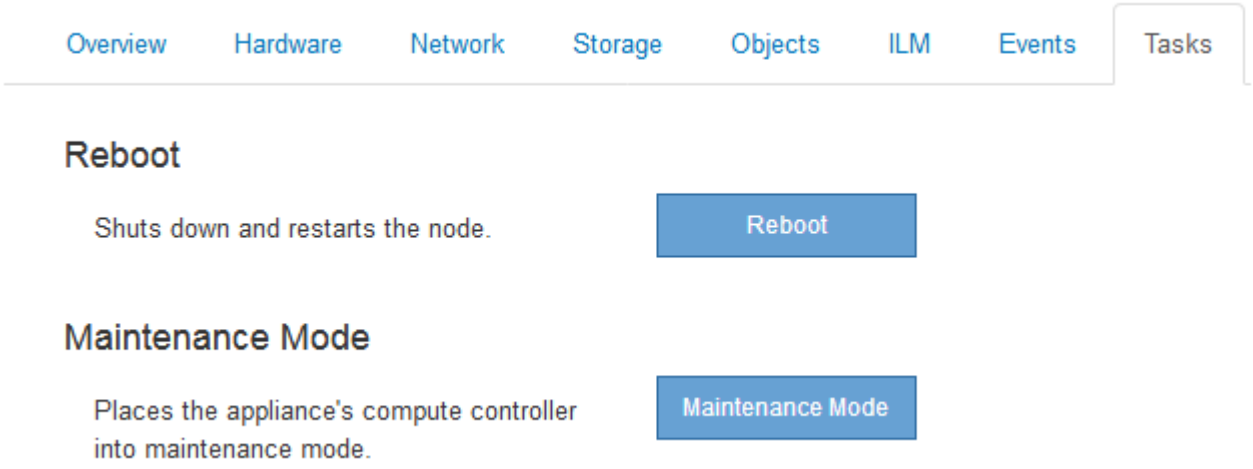
Sobre esta tarefa

Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

> A senha e a chave de host de um dispositivo StorageGRID no modo de manutenção permanecem as mesmas que eram quando o aparelho estava em serviço.

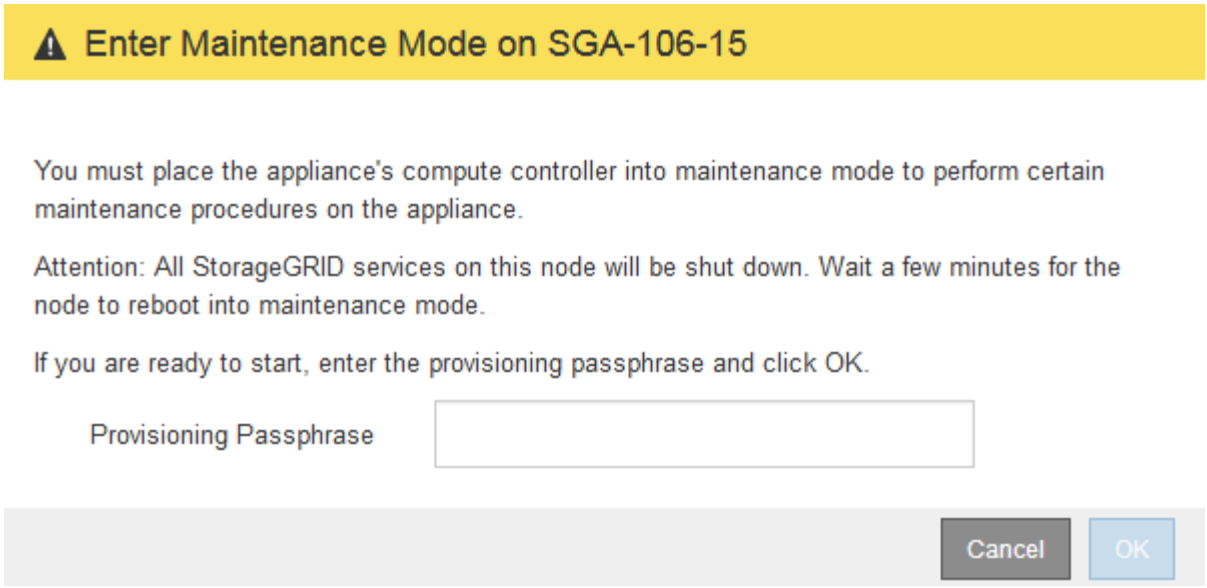
Passos

1. No Gerenciador de Grade, selecione **nós**.
2. Na exibição em árvore da página nós, selecione o nó de storage do dispositivo.
3. Selecione **tarefas**.



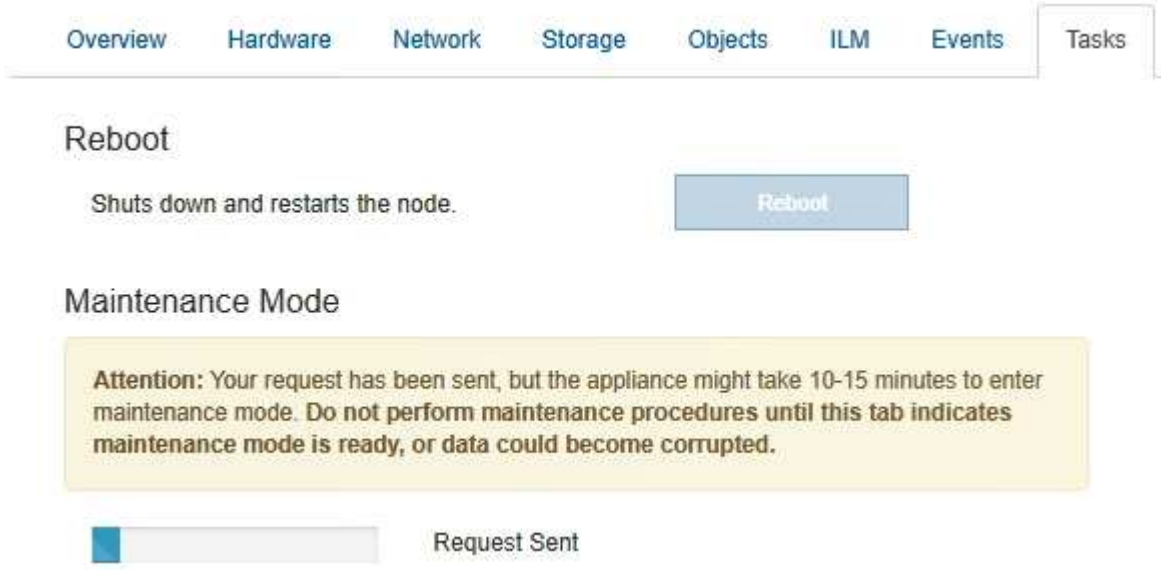
4. Selecione **Maintenance Mode** (modo de manutenção).

   É apresentada uma caixa de diálogo de confirmação.

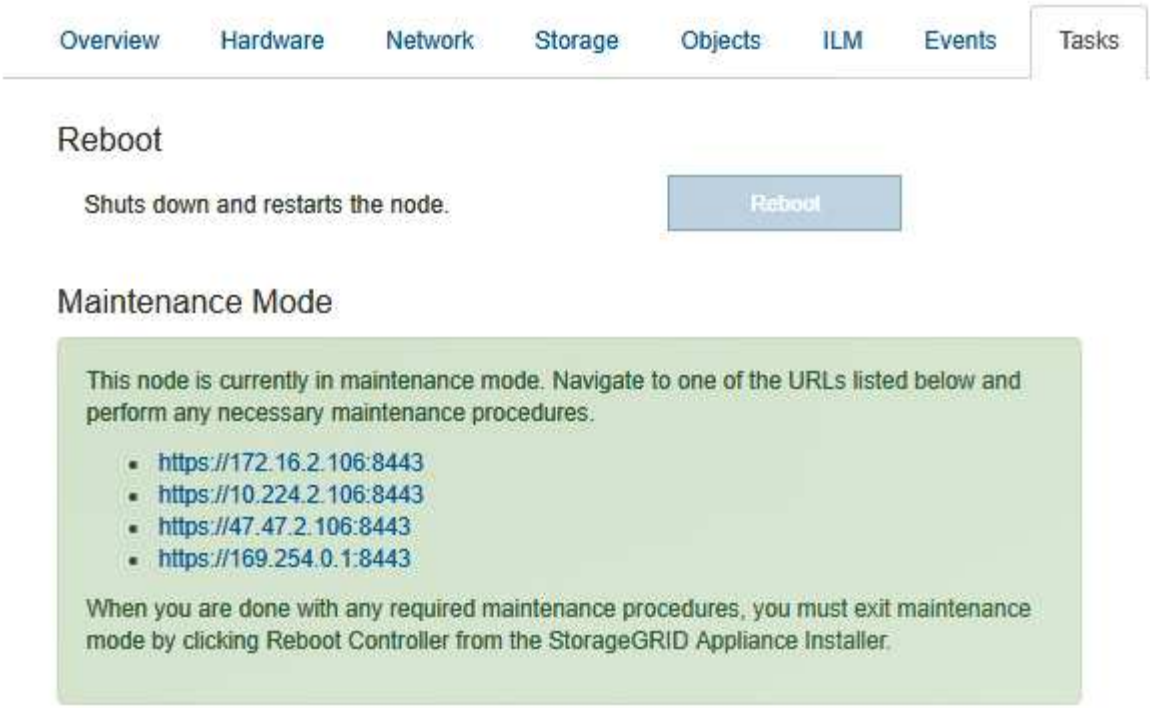


5. Introduza a frase-passe de aprovisionamento e selecione **OK**.

Uma barra de progresso e uma série de mensagens, incluindo "Request Sent" (pedido enviado), "Stop" (Paragem de StorageGRID) e "Reboot" (reinício), indicam que o aparelho está a concluir os passos para entrar no modo de manutenção.



Quando o dispositivo está no modo de manutenção, uma mensagem de confirmação lista os URLs que você pode usar para acessar o Instalador do StorageGRID Appliance.



6. Para acessar o Instalador do StorageGRID Appliance, navegue até qualquer um dos URLs exibidos.

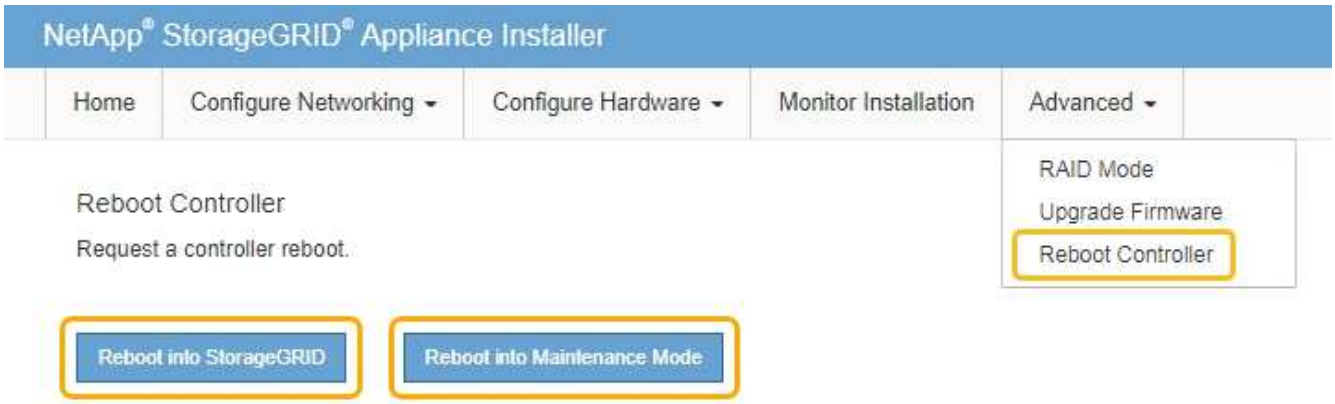
   Se possível, use o URL que contém o endereço IP da porta Admin Network do dispositivo.

   > O acesso `https://169.254.0.1:8443` requer uma conexão direta com a porta de gerenciamento local.

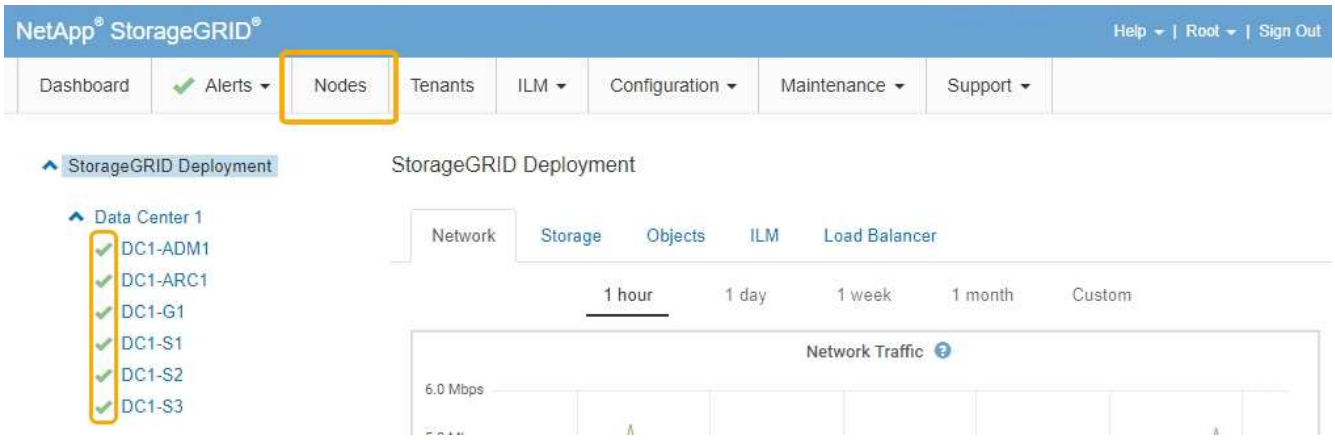
7. A partir do instalador do dispositivo StorageGRID, confirme se o aparelho está no modo de manutenção.

8. Execute todas as tarefas de manutenção necessárias.
9. Depois de concluir as tarefas de manutenção, saia do modo de manutenção e retome a operação normal do nó. No Instalador de dispositivos StorageGRID, selecione **Avançado controlador de reinicialização** e, em seguida, selecione **Reiniciar no StorageGRID**.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Atualizando o SANtricity os no controlador de storage

Para garantir o funcionamento ideal do controlador de storage, é necessário atualizar para a versão de manutenção mais recente do SANtricity os qualificado para o seu dispositivo StorageGRID. Consulte a ferramenta de Matriz de interoperabilidade do NetApp (IMT) para determinar qual versão você deve usar. Se você precisar de assistência, entre em Contato com o suporte técnico.

- Se o controlador de armazenamento estiver usando o SANtricity os 08.42.20.00 (11,42) ou mais recente, use o Gerenciador de Grade para executar a atualização.

  "Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade"

- Se a controladora de storage estiver usando uma versão do SANtricity os anterior a 08.42.20.00 (11,42), use o modo de manutenção para executar a atualização.

  "Atualizando o SANtricity os no controlador E2800 usando o modo de manutenção"

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Downloads do NetApp: SANtricity os"

"Monitorizar Resolução de problemas"

Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade

Para controladores de storage que atualmente usam o SANtricity os 08.42.20.00 (11,42) ou mais recente, você deve usar o Gerenciador de Grade para aplicar uma atualização.

O que você vai precisar

- Você consultou a ferramenta de Matriz de interoperabilidade (IMT) do NetApp para confirmar que a versão do SANtricity os que você está usando para a atualização é compatível com o seu dispositivo.
- Tem de ter a permissão Manutenção.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a senha de provisionamento.
- Você deve ter acesso à página de downloads do NetApp para o SANtricity os.

Sobre esta tarefa

Não é possível executar outras atualizações de software (atualização de software StorageGRID ou hotfix) até concluir o processo de atualização do SANtricity os. Se você tentar iniciar um hotfix ou uma atualização de software StorageGRID antes do processo de atualização do SANtricity os terminar, você será redirecionado para a página de atualização do SANtricity os.

O procedimento não será concluído até que a atualização do SANtricity os tenha sido aplicada com êxito a todos os nós aplicáveis. Pode levar mais de 30 minutos para carregar o SANtricity os em cada nó e até 90 minutos para reinicializar cada dispositivo de storage StorageGRID.

> As etapas a seguir são aplicáveis somente quando você estiver usando o Gerenciador de Grade para executar a atualização. Os controladores de armazenamento no dispositivo da série SG5700 não podem ser atualizados usando o Gerenciador de Grade quando os controladores estão usando o SANtricity os mais antigo que 08.42.20.00 (11,42).

> Este procedimento atualizará automaticamente a NVSRAM para a versão mais recente associada à atualização do sistema operacional SANtricity. Não é necessário aplicar um ficheiro de atualização NVSRAM separado.

Passos

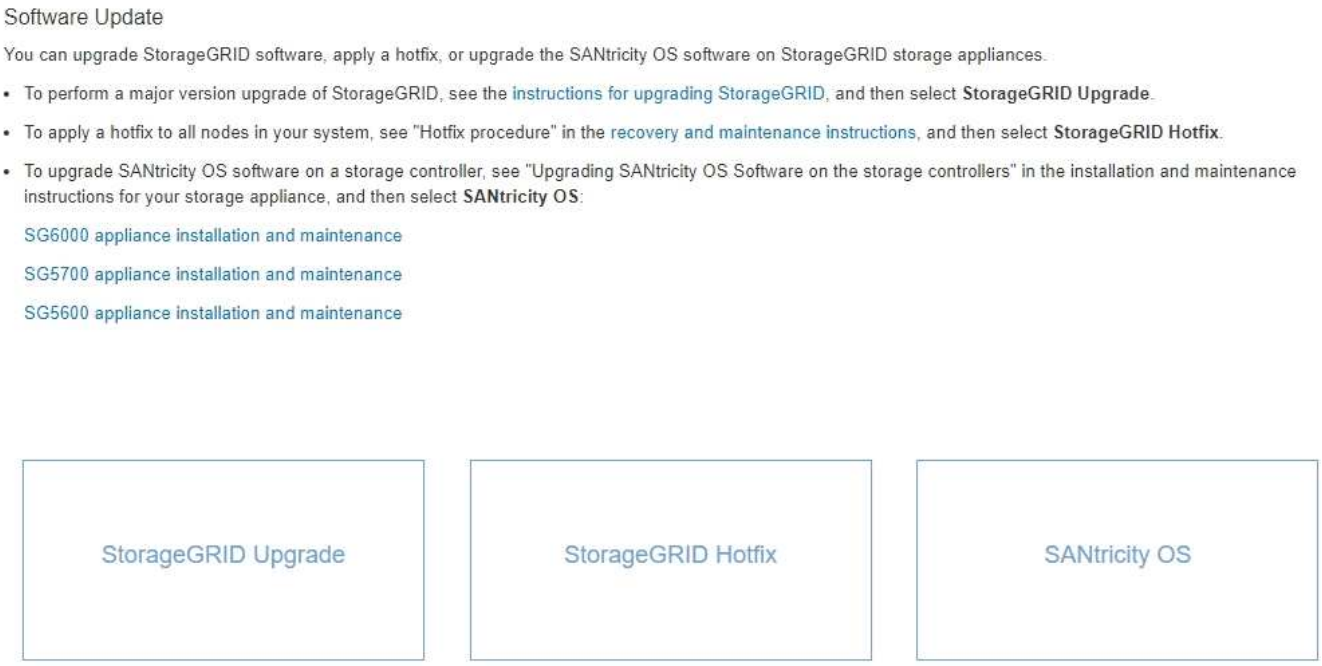
1. A partir de um portátil de serviço, transfira o novo ficheiro de software SANtricity os a partir do site de suporte da NetApp.

   Certifique-se de escolher a versão do SANtricity os para os controladores de storage E2800.

   "Downloads do NetApp: SANtricity os"

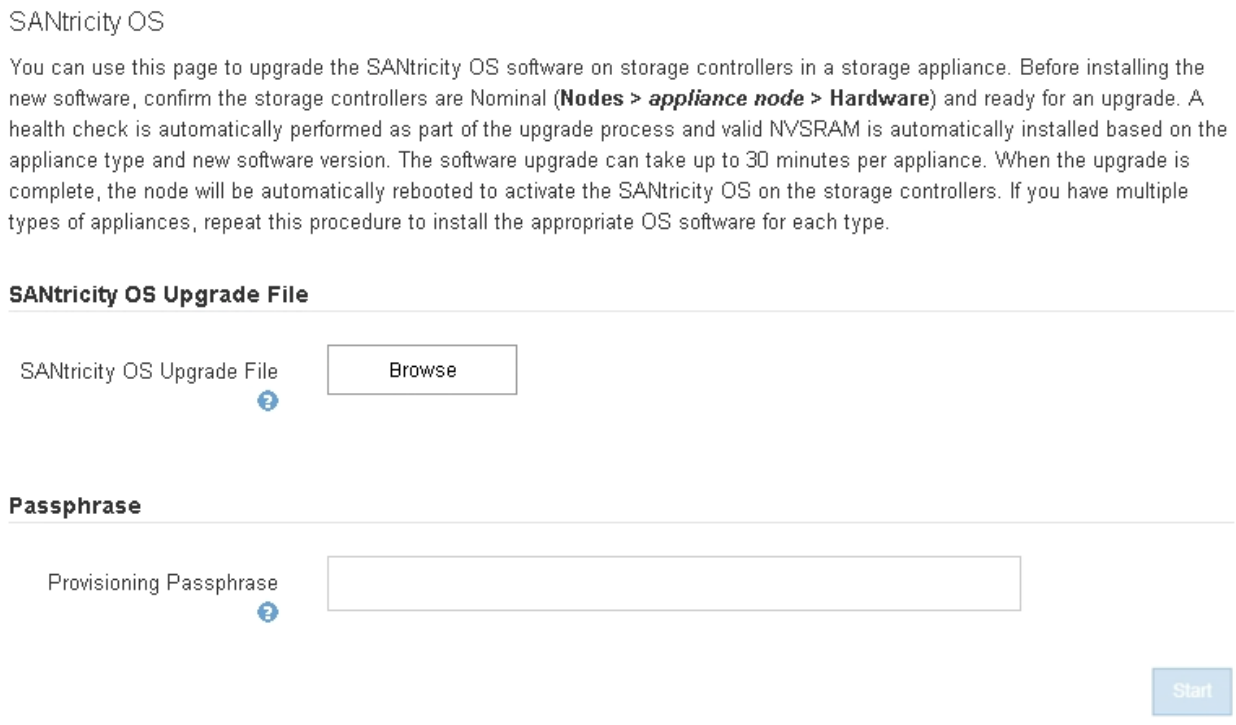
2. Faça login no Gerenciador de Grade usando um navegador compatível.
3. Selecione **Manutenção**. Em seguida, na seção sistema do menu, selecione **Atualização de software**.

   A página Atualização de software é exibida.



4. Clique em **SANtricity os**.

   A página do SANtricity os é exibida.



5. Selecione o arquivo de atualização do SANtricity os que você baixou no site de suporte do NetApp.

   a. Clique em **Procurar**.

   b. Localize e selecione o ficheiro.

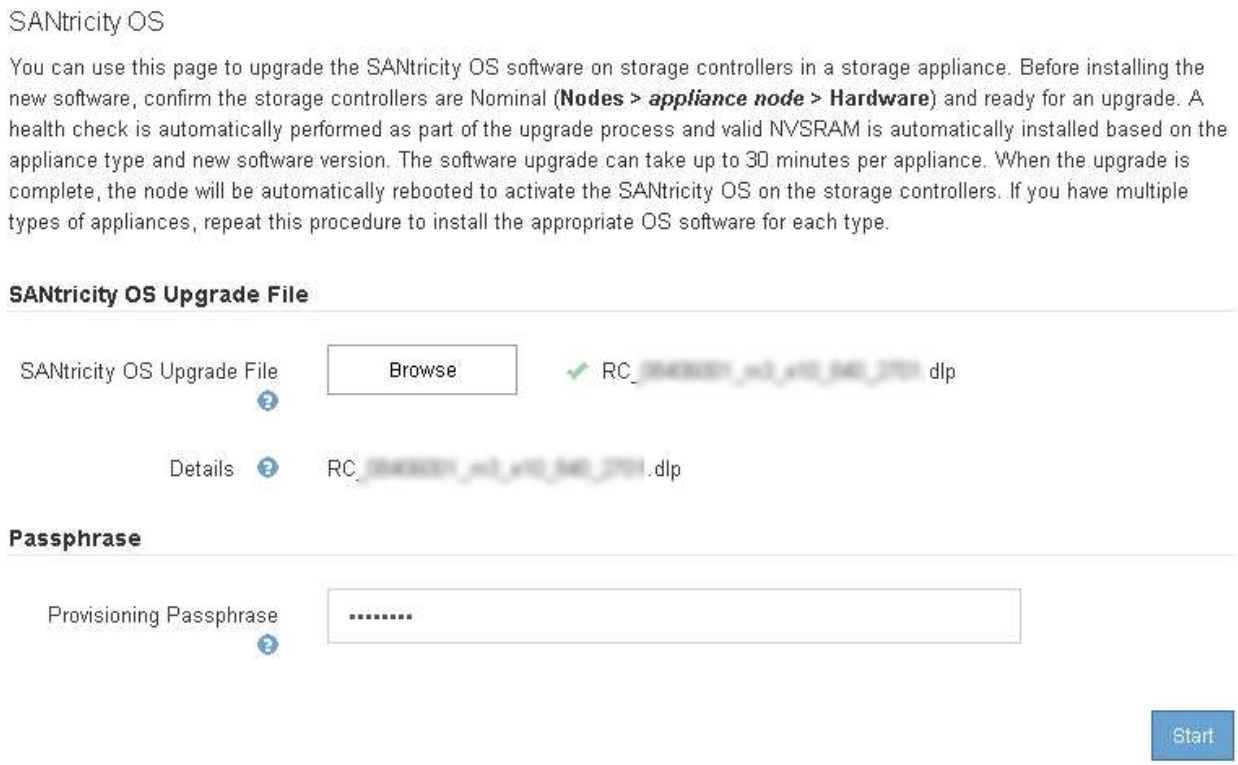
c. Clique em **abrir**.

O arquivo é carregado e validado. Quando o processo de validação é concluído, o nome do arquivo é mostrado no campo Detalhes.

Não altere o nome do arquivo, pois ele faz parte do processo de verificação.

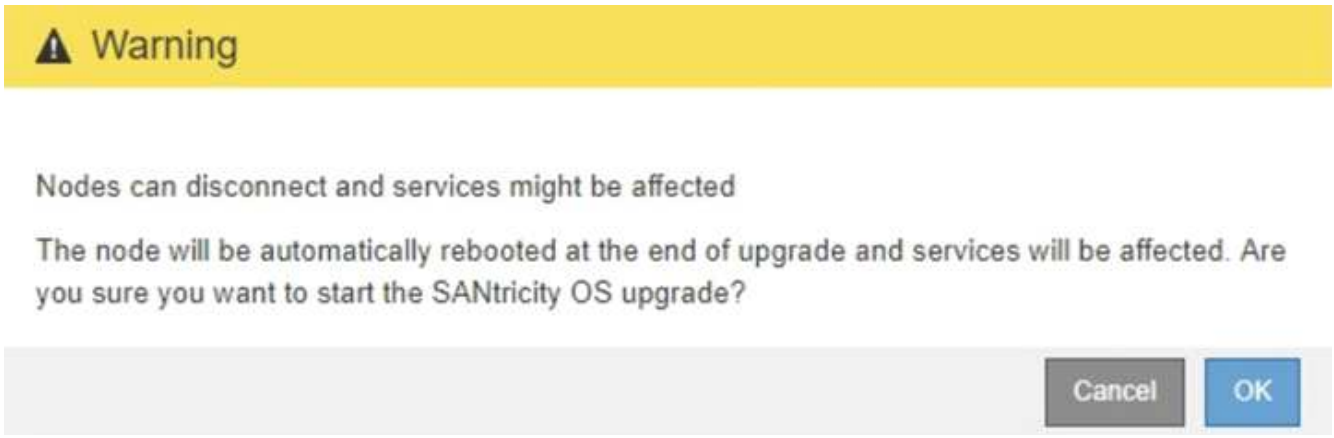
6. Introduza a frase-passe de aprovisionamento.

O botão **Start** está ativado.



7. Clique em **Iniciar**.

   Uma caixa de aviso aparece informando que a conexão do seu navegador pode ser perdida temporariamente à medida que os serviços nos nós atualizados são reiniciados.



8. Clique em **OK** para colocar o arquivo de atualização do SANtricity os no nó de administração principal.

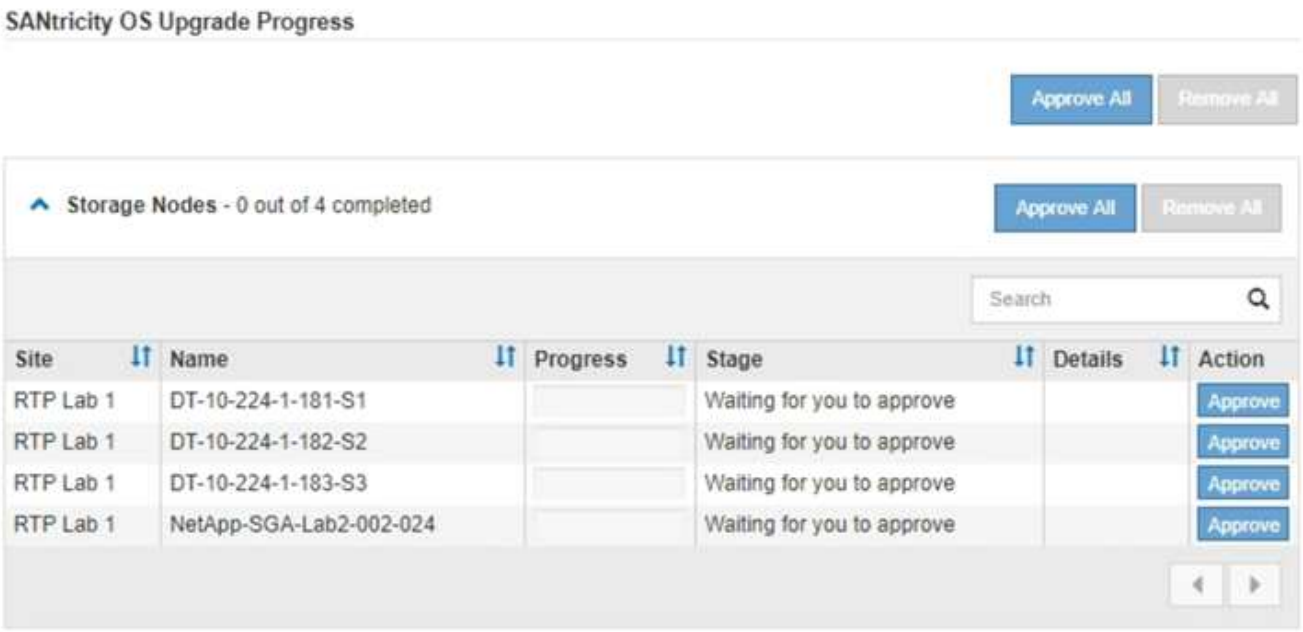
   Quando a atualização do SANtricity os é iniciada:

   a. A verificação de integridade é executada. Esse processo verifica se nenhum nó tem o status de precisa de atenção.

      Se algum erro for relatado, resolva-os e clique em **Start** novamente.

   b. A tabela de progresso da atualização do SANtricity os é exibida. Esta tabela mostra todos os nós de storage na grade e a etapa atual da atualização para cada nó.

A tabela mostra todos os nós de storage, incluindo nós de storage baseados em software. Você precisa aprovar a atualização para todos os nós de storage, mesmo que uma atualização do SANtricity os não afete os nós de storage baseados em software. A mensagem de atualização retornada para nós de storage baseados em software é "a atualização do SANtricity os não se aplica a este nó."



9. Opcionalmente, classifique a lista de nós em ordem crescente ou decrescente por **Site**, **Nome**, **progresso**, **Estágio** ou **Detalhes**. Ou insira um termo na caixa **pesquisar** para pesquisar nós específicos.

   Você pode rolar pela lista de nós usando as setas esquerda e direita no canto inferior direito da seção.

10. Aprove os nós de grade que você está pronto para adicionar à fila de atualização. Nós aprovados do mesmo tipo são atualizados um de cada vez.

    Não aprove a atualização do SANtricity os para um nó de armazenamento de dispositivo, a menos que você tenha certeza de que o nó está pronto para ser interrompido e reinicializado.quando a atualização do SANtricity os for aprovada em um nó, os serviços nesse nó são interrompidos. Mais tarde, quando o nó é atualizado, o nó do appliance é reinicializado. Essas operações podem causar interrupções de serviço para clientes que estão se comunicando com o nó.

    - Clique em um dos botões **Approve All** para adicionar todos os nós de armazenamento à fila de atualização do SANtricity os.

      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).

    - Clique em um ou mais botões **Approve** para adicionar um ou mais nós à fila de atualização do SANtricity os.

Você pode atrasar a aplicação de uma atualização do SANtricity os a um nó, mas o processo de atualização do SANtricity os não será concluído até que você aprove a atualização do SANtricity os em todos os nós de armazenamento listados.

Depois de clicar em **Approve**, o processo de atualização determina se o nó pode ser atualizado. Se um nó puder ser atualizado, ele será adicionado à fila de atualização. E

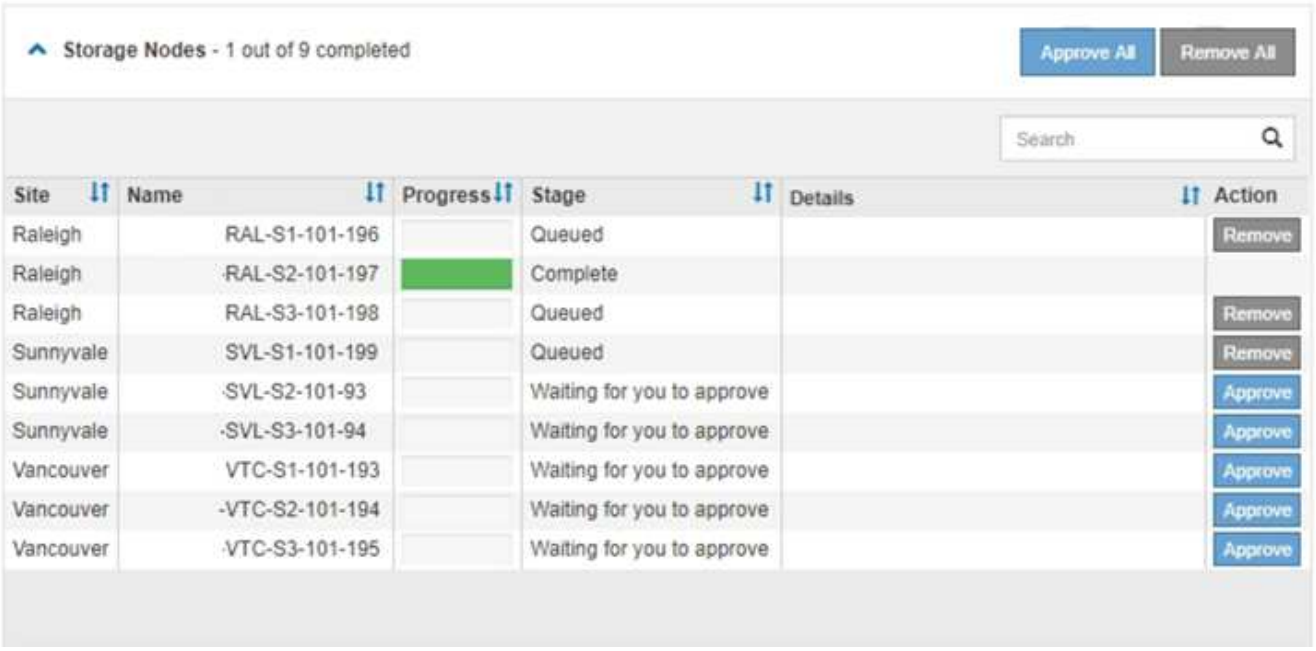
Para alguns nós, o arquivo de atualização selecionado não é aplicado intencionalmente e você pode concluir o processo de atualização sem atualizar esses nós específicos. Para nós intencionalmente não atualizados, o processo mostrará o estágio completo com uma das seguintes mensagens na coluna Detalhes:

- O nó de storage já foi atualizado.
- A atualização do SANtricity os não é aplicável a este nó.
- O ficheiro SANtricity os não é compatível com este nó.

A mensagem "'SANtricity os upgrade não é aplicável a este nó'" indica que o nó não tem um controlador de armazenamento que pode ser gerenciado pelo sistema StorageGRID. Essa mensagem será exibida para nós de storage que não sejam do dispositivo. Você pode concluir o processo de atualização do SANtricity os sem atualizar o nó exibindo esta mensagem. A mensagem "'arquivo SANtricity os não é compatível com este nó'" indica que o nó requer um arquivo SANtricity os diferente daquele que o processo está tentando instalar. Depois de concluir a atualização atual do SANtricity os, baixe o SANtricity os apropriado para o nó e repita o processo de atualização.

11. Se você precisar remover um nó ou todos os nós da fila de atualização do SANtricity os, clique em **Remover** ou **Remover tudo**.

    Como mostrado no exemplo, quando o estágio avança além da fila, o botão **Remover** fica oculto e você não pode mais remover o nó do processo de atualização do SANtricity os.



12. Aguarde enquanto a atualização do SANtricity os é aplicada a cada nó de grade aprovado.

Se algum nó mostrar um estágio de erro enquanto a atualização do SANtricity os está sendo aplicada, a atualização falhou para esse nó. Pode ser necessário colocar o aparelho no modo de manutenção para recuperar da falha. Contacte o suporte técnico antes de continuar.

Se o firmware no nó é muito antigo para ser atualizado com o Gerenciador de Grade, o nó mostra um estágio de erro com os detalhes: "'você deve usar o modo de manutenção para atualizar o SANtricity os neste nó. Consulte as instruções de instalação e manutenção do seu aparelho. Após a atualização, você pode usar este utilitário para futuras atualizações." para resolver o erro, faça o seguinte:

a. Use o modo de manutenção para atualizar o SANtricity os no nó que mostra um estágio de erro.
b. Use o Gerenciador de Grade para reiniciar e concluir a atualização do SANtricity os.

   Quando a atualização do SANtricity os é concluída em todos os nós aprovados, a tabela de progresso da atualização do SANtricity os fecha e um banner verde mostra a data e a hora em que a atualização do SANtricity os foi concluída.

13. Repita este procedimento de atualização para todos os nós com um estágio de conclusão que exigem um arquivo de atualização diferente do SANtricity os.

Para todos os nós com um status de precisa de atenção, use o modo de manutenção para executar a atualização.

Informações relacionadas

"Atualizando o SANtricity os no controlador E2800 usando o modo de manutenção"

Atualizando o SANtricity os no controlador E2800 usando o modo de manutenção

Para controladores de storage que atualmente usam o SANtricity os com mais de 08.42.20.00 GB (11,42 GB), você deve usar o procedimento de modo de manutenção para aplicar uma atualização.

O que você vai precisar

- Você consultou a ferramenta de Matriz de interoperabilidade (IMT) do NetApp para confirmar que a versão do SANtricity os que você está usando para a atualização é compatível com o seu dispositivo.
- Você deve colocar o controlador E5700SG no modo de manutenção, o que interrompe a conexão com o controlador E2800. Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

"Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Não atualize o SANtricity os ou a NVSRAM na controladora e-Series em mais de um dispositivo StorageGRID de cada vez.

> A atualização de mais de um dispositivo StorageGRID por vez pode causar indisponibilidade de dados, dependendo do modelo de implantação e das políticas de ILM.

Passos

1. A partir de um portátil de serviço, aceda ao Gestor de sistema SANtricity e inicie sessão.
2. Transfira o novo ficheiro de software SANtricity os e o ficheiro NVSRAM para o cliente de gestão.

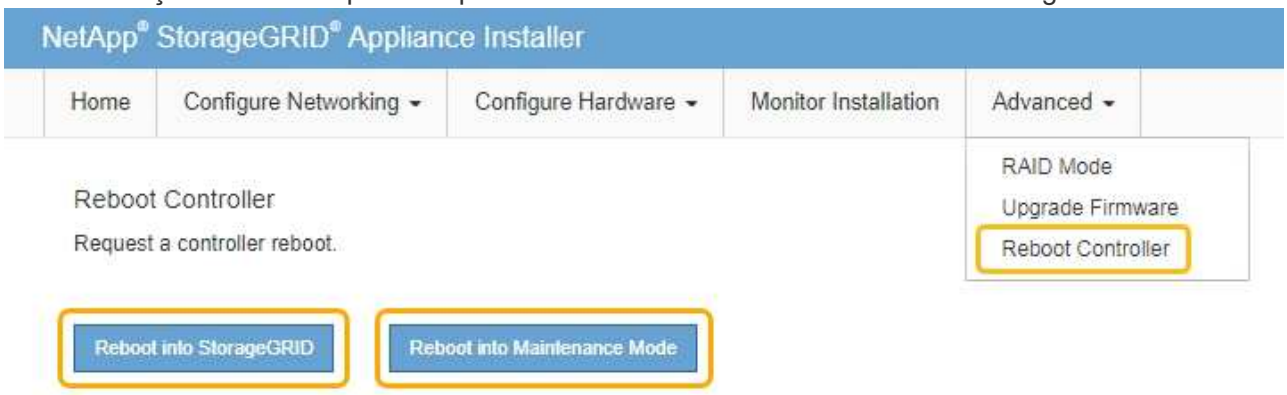
   > A NVSRAM é específica do dispositivo StorageGRID. Não utilize a transferência NVSRAM padrão.

3. Siga as instruções no Guia de atualização de software e firmware do SANtricity *E2800 e E5700* ou na ajuda on-line do Gerenciador de sistema do SANtricity para atualizar o firmware e a NVSRAM da controladora E2800.

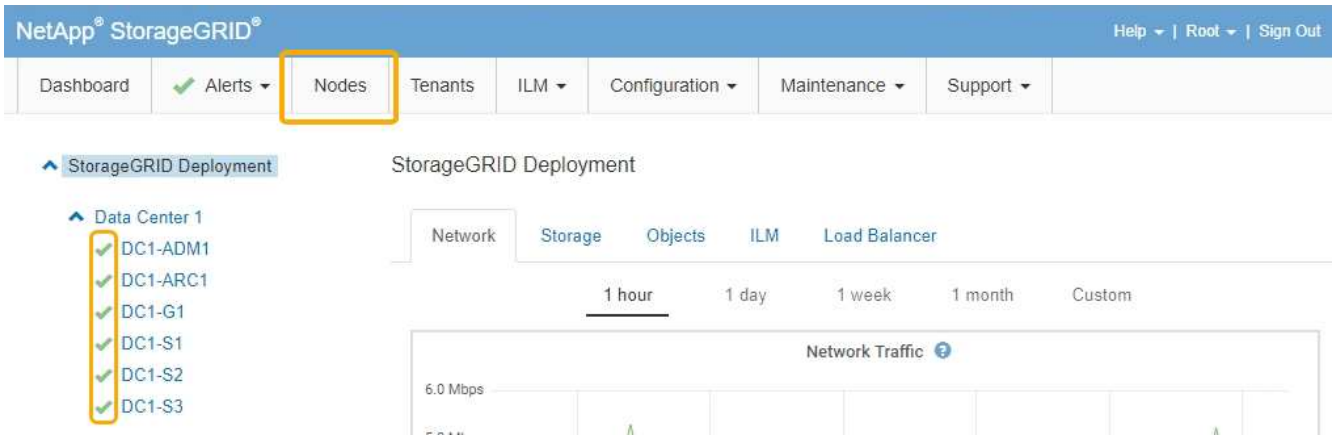
   > Ative os arquivos de atualização imediatamente. Não adiar a ativação.

4. Uma vez concluída a operação de atualização, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



   Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade"

Atualizando o firmware da unidade usando o Gerenciador de sistema do SANtricity

Você atualiza o firmware da sua unidade para garantir que você tenha todos os recursos mais recentes e correções de bugs.

O que você vai precisar

- O dispositivo de armazenamento tem um status ideal.
- Todas as unidades têm um status ideal.
- Você tem a versão mais recente do Gerenciador de sistema do SANtricity instalada que é compatível com sua versão do StorageGRID.
- Colocou o aparelho StorageGRID no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

> O modo de manutenção interrompe a conexão com o controlador de storage, interrompendo todas as atividades de e/S e colocando todas as unidades offline.

> Não atualize o firmware da unidade em mais de um dispositivo StorageGRID de cada vez. Isso pode causar indisponibilidade de dados, dependendo do modelo de implantação e das políticas de ILM.

Passos

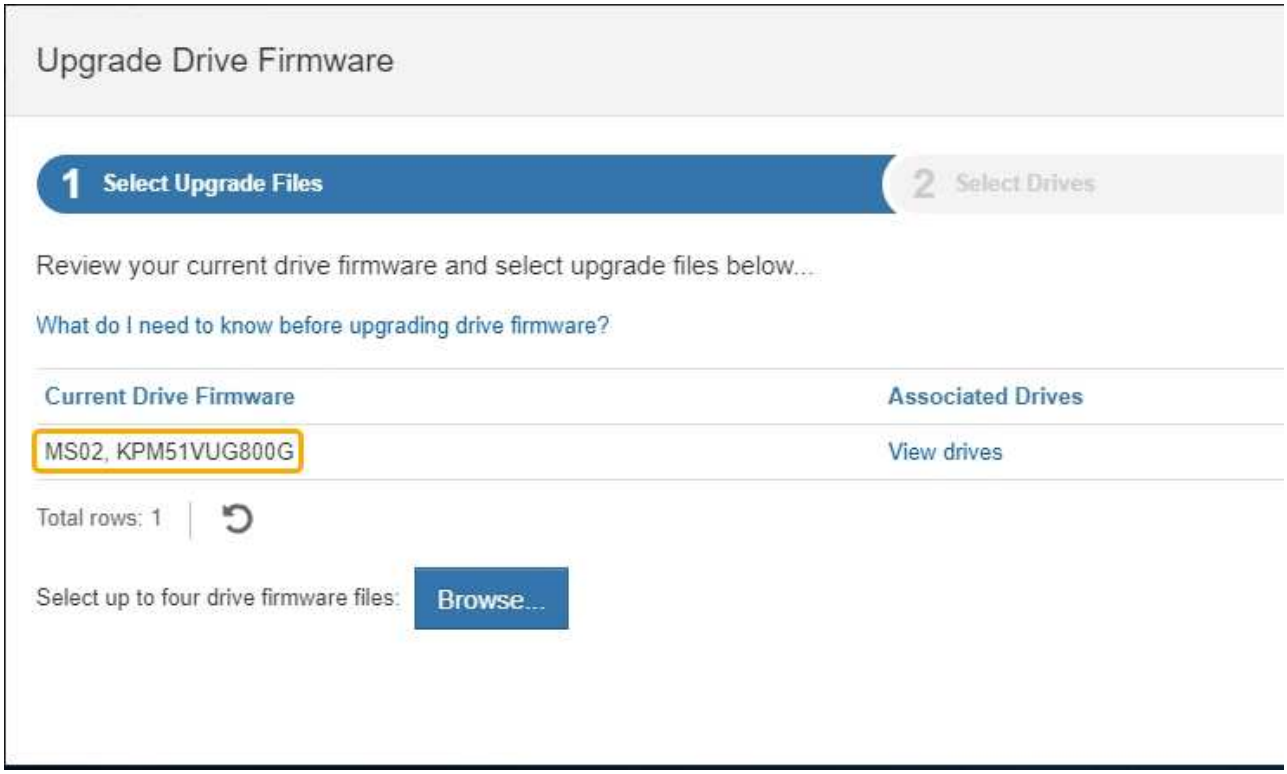
1. Acesse o Gerenciador de sistemas do SANtricity usando um destes métodos:
   - Use o Instalador do StorageGRID Appliance e selecione **Avançado Gerenciador do sistema SANtricity**
   - Use o Gerenciador de Grade e selecione **nós** * `***appliance Storage Node***`Gerenciador de sistema SANtricity*

> Se estas opções não estiverem disponíveis ou a página de início de sessão do Gestor do sistema SANtricity não for apresentada, aceda ao Gestor do sistema SANtricity navegando para o IP do controlador de armazenamento
> `https://Storage_Controller_IP`

2. Introduza o nome de utilizador e a palavra-passe do administrador do Gestor do sistema SANtricity, se necessário.
3. Verifique a versão do firmware da unidade atualmente instalada no dispositivo de armazenamento:
   a. No Gerenciador do sistema SANtricity, selecione **suporte Centro de Atualização**.
   b. Em Drive firmware upgrade, selecione **Begin Upgrade** (Iniciar atualização).

      O firmware da unidade de atualização exibe os arquivos de firmware da unidade atualmente instalados.

   c. Observe as revisões atuais do firmware da unidade e os identificadores da unidade na coluna firmware da unidade atual.



      Neste exemplo:

      - A revisão do firmware da unidade é **MS02**.
      - O identificador da unidade é **KPM51VUG800G**.

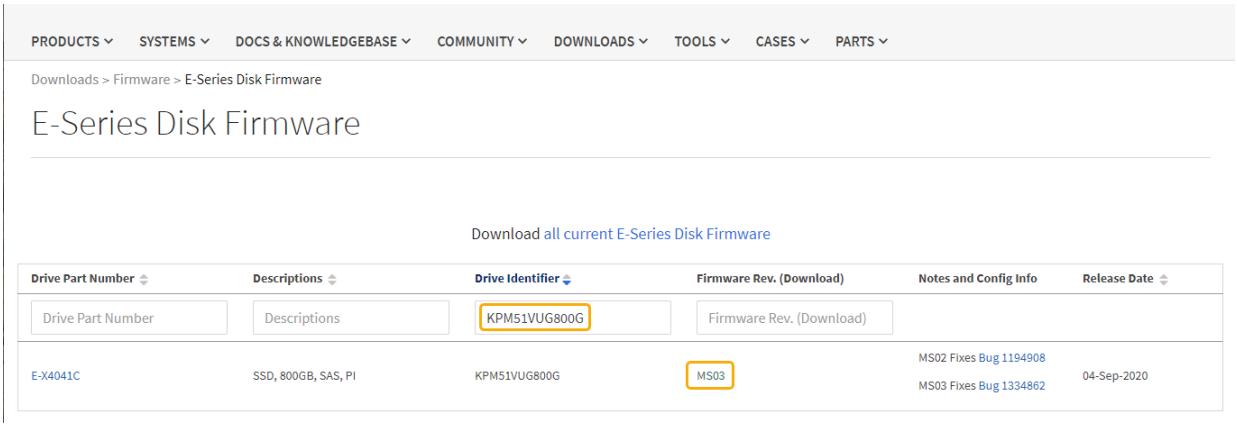
   Selecione **Exibir unidades** na coluna unidades associadas para exibir onde essas unidades estão instaladas no seu dispositivo de armazenamento.

   a. Feche a janela Upgrade Drive firmware (Atualizar firmware da unidade).
4. Transfira e prepare a atualização de firmware da unidade disponível:
   a. Em Atualização do firmware da unidade, selecione **suporte NetApp**.
   b. No site de suporte da NetApp, selecione a guia **Downloads** e, em seguida, selecione **firmware da unidade de disco da série e**.

      É apresentada a página firmware do disco e-Series.

c. Procure cada **Drive Identifier** instalado no seu dispositivo de armazenamento e verifique se cada identificador de unidade tem a revisão de firmware mais recente.

   - Se a revisão do firmware não for um link, esse identificador de unidade terá a revisão de firmware mais recente.
   - Se um ou mais números de peça de unidade forem listados para um identificador de unidade, uma atualização de firmware estará disponível para essas unidades. Pode selecionar qualquer ligação para transferir o ficheiro de firmware.



d. Se estiver listada uma revisão de firmware posterior, selecione o link na coluna firmware Rev. (Download) para baixar um `.zip` arquivo contendo o arquivo de firmware.

e. Extraia (descompacte) os arquivos de arquivo de firmware da unidade que você baixou do site de suporte.

5. Instale a atualização do firmware da unidade:

a. No Gerenciador de sistema do SANtricity, em Atualização do firmware da unidade, selecione **Begin Upgrade**.

b. Selecione **Procurar** e selecione os novos arquivos de firmware da unidade que você baixou no site de suporte.

   Os arquivos de firmware da unidade têm um nome de arquivo semelhante a `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`

   Você pode selecionar até quatro arquivos de firmware da unidade, um de cada vez. Se mais de um arquivo de firmware de unidade for compatível com a mesma unidade, você receberá um erro de conflito de arquivo. Decida qual arquivo de firmware da unidade você deseja usar para a atualização e remova o outro.

c. Selecione **seguinte**.

   Selecionar unidades lista as unidades que você pode atualizar com os arquivos de firmware selecionados.

   Apenas as unidades compatíveis aparecem.

   O firmware selecionado para a unidade aparece em **firmware proposto**. Se tiver de alterar este firmware, selecione **voltar**.

d. Selecione **Offline (paralelo)** upgrade.

   Você pode usar o método de atualização off-line porque o dispositivo está no modo de manutenção, onde a atividade de e/S é interrompida para todas as unidades e todos os volumes.

e. Na primeira coluna da tabela, selecione a unidade ou unidades que deseja atualizar.

   A prática recomendada é atualizar todas as unidades do mesmo modelo para a mesma revisão de firmware.

f. Selecione **Iniciar** e confirme que deseja executar a atualização.

   Se você precisar parar a atualização, selecione **Stop**. Todas as transferências de firmware atualmente em curso são concluídas. Quaisquer downloads de firmware que não tenham sido iniciados são cancelados.

   > Parar a atualização do firmware da unidade pode resultar em perda de dados ou unidades indisponíveis.

g. (Opcional) para ver uma lista do que foi atualizado, selecione **Save Log**.

   O arquivo de log é salvo na pasta de downloads do navegador com o `latest-upgrade-log-timestamp.txt` nome .

   Se ocorrer algum dos seguintes erros durante o procedimento de atualização, tome a ação recomendada apropriada.

   - **Unidades atribuídas com falha**

     Um motivo para a falha pode ser que a unidade não tenha a assinatura apropriada. Certifique-se de que a unidade afetada é uma unidade autorizada. Entre em Contato com o suporte técnico para obter mais informações.

   Ao substituir uma unidade, certifique-se de que a unidade de substituição tem uma capacidade igual ou superior à unidade com falha que está a substituir.

Você pode substituir a unidade com falha enquanto a matriz de armazenamento está recebendo e/S

- **Verifique a matriz de armazenamento**
  - Certifique-se de que foi atribuído um endereço IP a cada controlador.
  - Certifique-se de que todos os cabos ligados ao controlador não estão danificados.
  - Certifique-se de que todos os cabos estão bem ligados.
- **Unidades hot spare integradas**

  Esta condição de erro tem de ser corrigida antes de poder atualizar o firmware.

- **Grupos de volumes incompletos**

  Se um ou mais grupos de volumes ou pools de discos estiverem incompletos, você deverá corrigir essa condição de erro antes de atualizar o firmware.

- * Operações exclusivas (exceto Mídia em segundo plano/varredura de paridade) atualmente em execução em qualquer grupo de volume*

  Se uma ou mais operações exclusivas estiverem em andamento, as operações devem ser concluídas antes que o firmware possa ser atualizado. Use o System Manager para monitorar o andamento das operações.

- **Volumes em falta**

  Você deve corrigir a condição de volume ausente antes que o firmware possa ser atualizado.

- * Qualquer controlador em um estado diferente do ideal*

  Um dos controladores de storage array precisa de atenção. Esta condição deve ser corrigida antes que o firmware possa ser atualizado.

- **Informações de partição de armazenamento incompatíveis entre gráficos de objetos do controlador**

  Ocorreu um erro ao validar os dados nos controladores. Contacte o suporte técnico para resolver este problema.

- **SPM verificar falha na verificação do controlador de banco de dados**

  Ocorreu um erro de banco de dados de mapeamento de partições de armazenamento em um controlador. Contacte o suporte técnico para resolver este problema.

- **Validação da base de dados de configuração (se suportada pela versão do controlador da matriz de armazenamento)**

  Ocorreu um erro de banco de dados de configuração em um controlador. Contacte o suporte técnico para resolver este problema.

- **Verificações relacionadas ao mel**

  Contacte o suporte técnico para resolver este problema.

- **Mais de 10 eventos informativos ou críticos de mel foram relatados nos últimos 7 dias**

  Contacte o suporte técnico para resolver este problema.

- **Mais de 2 Página 2C Eventos críticos de mel foram relatados nos últimos 7 dias**

  Contacte o suporte técnico para resolver este problema.

- **Mais de 2 eventos de mel críticos de canal de unidade degradada foram relatados nos últimos 7 dias**

  Contacte o suporte técnico para resolver este problema.

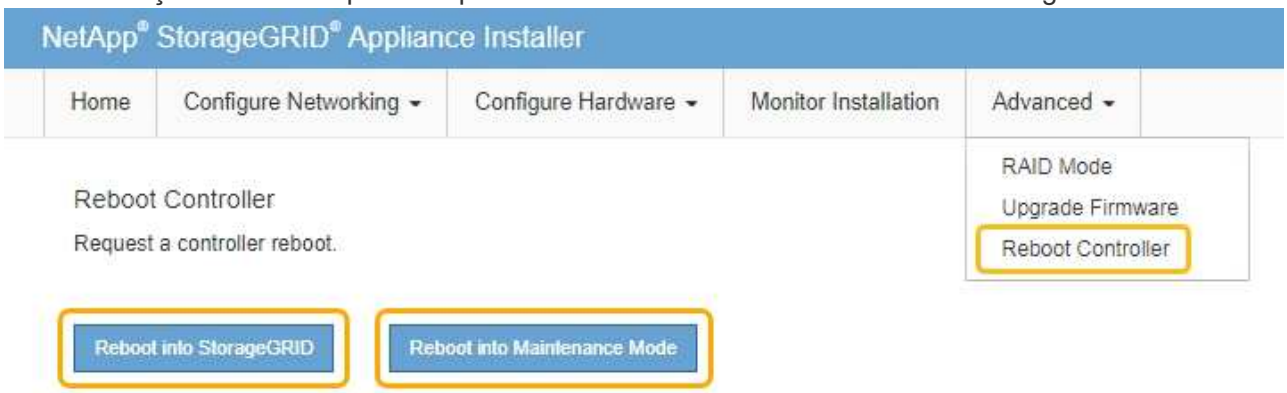
- **Mais de 4 entradas críticas de mel nos últimos 7 dias**

  Contacte o suporte técnico para resolver este problema.

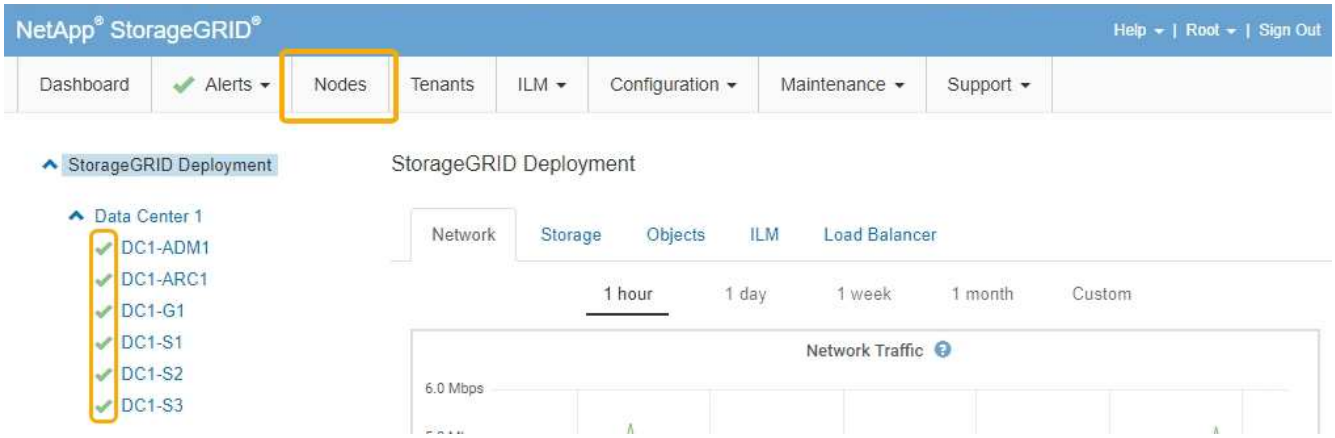
6. Quando a operação de atualização estiver concluída, reinicie o aparelho. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o

controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Atualizando o SANtricity os no controlador de storage"

Substituição do controlador E2800

Talvez seja necessário substituir o controlador E2800 se ele não estiver funcionando de forma ideal ou se ele tiver falhado.

Sobre esta tarefa

- Você tem um controlador de substituição com o mesmo número de peça do controlador que está substituindo.
- Você baixou as instruções para substituir a configuração simplex de um recipiente de controlador E2800 com falha.

Consulte as instruções da Série e apenas quando for direcionado ou se precisar de mais detalhes para executar uma etapa específica. Não confie nas instruções do e-Series para substituir um controlador no dispositivo StorageGRID, porque os procedimentos não são os mesmos.

- Você tem etiquetas para identificar cada cabo conetado ao controlador.
- Se todas as unidades estiverem protegidas, você revisou as etapas do procedimento de substituição do controlador simplex E2800, que incluem o download e a instalação do e-Series SANtricity Storage Manager do site de suporte da NetApp e, em seguida, usando a janela de gerenciamento empresarial (EMW) para desbloquear as unidades protegidas depois de ter substituído o controlador.

  Não poderá utilizar o aparelho até desbloquear as unidades com a chave guardada.

- Você deve ter permissões de acesso específicas.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Você pode determinar se você tem um recipiente de controlador com falha de duas maneiras:

- O Guru de recuperação no Gerenciador de sistema do SANtricity direciona você para substituir o controlador.
- O LED âmbar de atenção no controlador está aceso, indicando que o controlador tem uma avaria.

O nó de storage do dispositivo não estará acessível quando você substituir o controlador. Se o controlador E2800 estiver a funcionar o suficiente, pode colocar o controlador E5700SG no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Quando substituir um controlador, tem de remover a bateria do controlador original e instalá-la no controlador de substituição.

O controlador E2800 no dispositivo não inclui uma placa de interface de host (HIC).

Passos

1. Siga as instruções no procedimento de substituição do controlador E2800 para preparar a remoção do controlador.

   Use o Gerenciador de sistema do SANtricity para executar estas etapas.

   a. Anote qual versão do software SANtricity os está atualmente instalada no controlador.
   b. Anote qual versão do NVSRAM está instalada atualmente.
   c. Se o recurso Segurança da unidade estiver ativado, verifique se existe uma chave salva e se você sabe a frase-passe necessária para instalá-la.

      Possível perda de acesso a dados -- se todas as unidades do dispositivo estiverem habilitadas para segurança, o novo controlador não poderá acessar o dispositivo até que você desbloqueie as unidades protegidas usando a janela Gerenciamento Empresarial no SANtricity Storage Manager.

   d. Faça uma cópia de segurança da base de dados de configuração.

Se ocorrer um problema ao remover um controlador, pode utilizar o ficheiro guardado para restaurar a configuração.

e. Colete dados de suporte para o dispositivo.

> A coleta de dados de suporte antes e depois da substituição de um componente garante que você possa enviar um conjunto completo de logs para o suporte técnico caso a substituição não resolva o problema.

2. Se o dispositivo StorageGRID estiver a funcionar num sistema StorageGRID, coloque o controlador E5700SG no modo de manutenção.

   "Colocar um aparelho no modo de manutenção"

3. Se o controlador E2800 estiver a funcionar o suficiente para permitir um encerramento controlado, confirme que todas as operações foram concluídas.
   a. Na página inicial do Gerenciador do sistema do SANtricity, selecione **Exibir operações em andamento**.
   b. Confirme se todas as operações foram concluídas.
4. Retire o controlador do aparelho:
   a. Coloque uma pulseira antiestática ou tome outras precauções antiestáticas.
   b. Identifique os cabos e, em seguida, desligue os cabos e SFPs.

      > Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos.

   c. Solte o controlador do aparelho apertando o trinco na pega do came até soltar e, em seguida, abra a pega do came para a direita.
   d. Utilizando as duas mãos e a pega do came, deslize o controlador para fora do aparelho.

      > Utilize sempre duas mãos para suportar o peso do controlador.

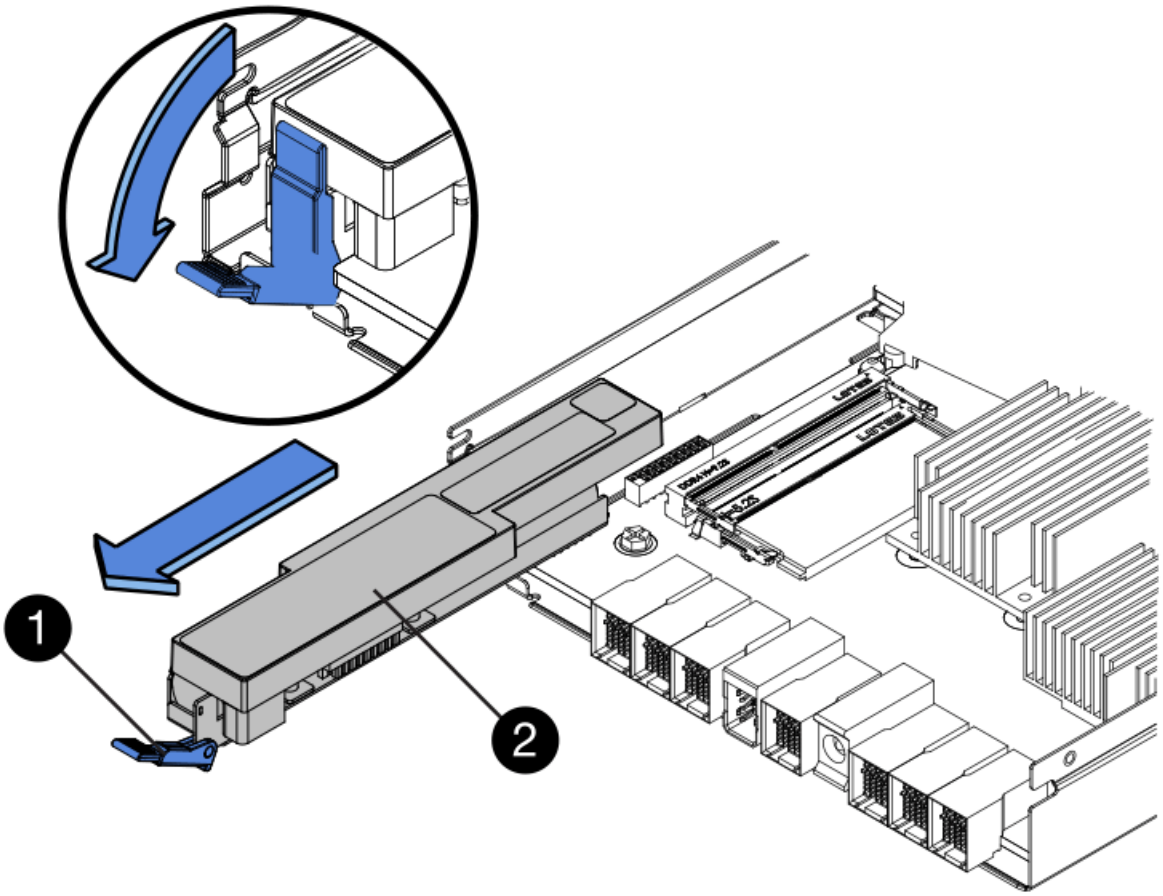
   e. Coloque o controlador numa superfície plana e sem estática com a tampa amovível virada para cima.
   f. Remova a tampa pressionando o botão e deslizando a tampa para fora.
5. Remova a bateria do controlador com falha e instale-a no controlador de substituição:
   a. Confirme se o LED verde dentro do controlador (entre a bateria e os DIMMs) está desligado.

      Se este LED verde estiver ligado, o controlador ainda está a utilizar a bateria. Deve aguardar que este LED se apague antes de remover quaisquer componentes.

Item	Descrição
1	LED Ativo Cache Interno
2	Bateria

b. Localize a trava de liberação azul da bateria.

c. Desengate a bateria empurrando a trava de liberação para baixo e afastando-a do controlador.



Item	Descrição
	Trinco de desbloqueio da bateria
	Bateria

d. Levante a bateria e deslize-a para fora do controlador.

e. Retire a tampa do controlador de substituição.

f. Oriente o controlador de substituição para que a ranhura da bateria fique voltada para si.

g. Introduza a bateria no controlador a um ligeiro ângulo descendente.

   Deve inserir a flange metálica na parte frontal da bateria na ranhura na parte inferior do controlador e deslizar a parte superior da bateria por baixo do pequeno pino de alinhamento no lado esquerdo do controlador.

h. Desloque o trinco da bateria para cima para fixar a bateria.

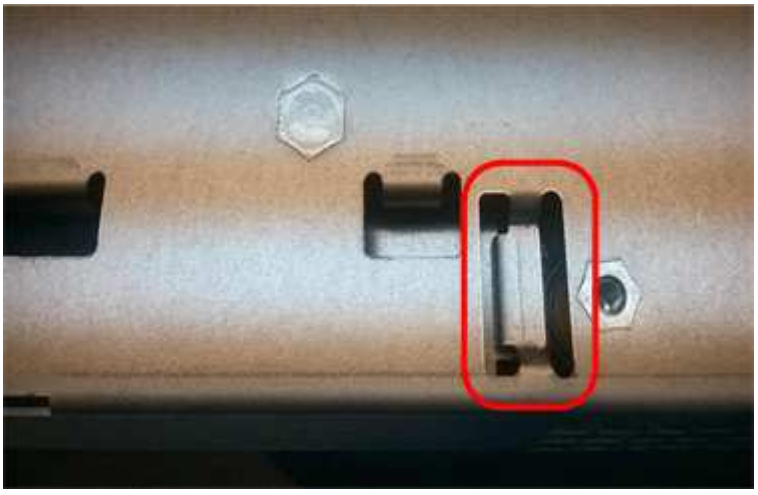
   Quando a trava se encaixa no lugar, a parte inferior da trava se encaixa em uma ranhura metálica no chassi.

i. Vire o controlador para confirmar que a bateria está instalada corretamente.

> **Possíveis danos ao hardware** — a flange metálica na parte frontal da bateria deve ser completamente inserida na ranhura do controlador (como mostrado na primeira figura). Se a bateria não estiver instalada corretamente (como mostrado na segunda figura), a flange metálica pode entrar em Contato com a placa controladora, causando danos.

- **Correto — a flange de metal da bateria está completamente inserida na ranhura do controlador:**

- **Incorreto — a flange metálica da bateria não está inserida na ranhura do controlador:**



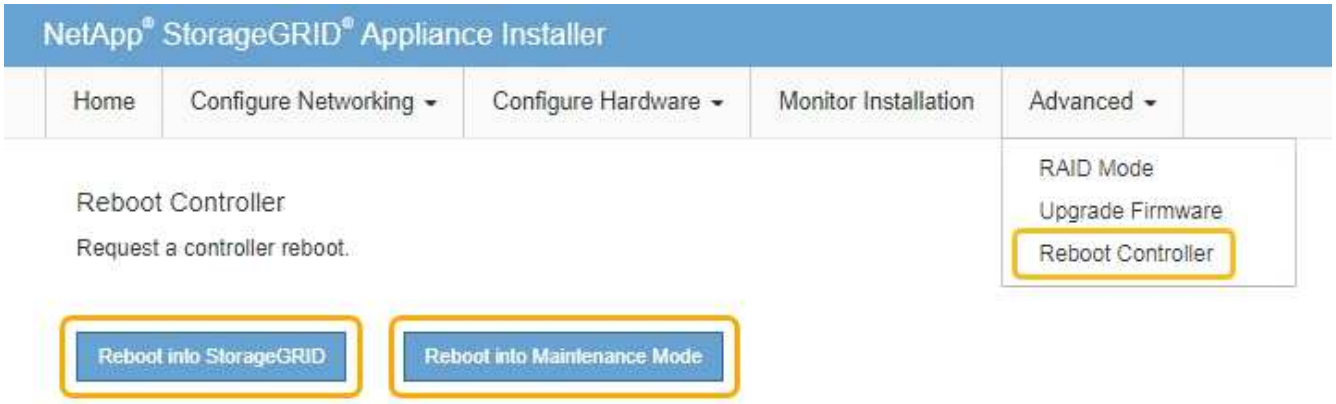
j. Volte a colocar a tampa do controlador.

6. Instale o controlador de substituição no aparelho.
   a. Vire o controlador ao contrário, de modo a que a tampa amovível fique virada para baixo.
   b. Com a pega do came na posição aberta, deslize o controlador até ao aparelho.
   c. Mova a alavanca do came para a esquerda para bloquear o controlador no lugar.
   d. Substitua os cabos e SFPs.
   e. Aguarde até que o controlador E2800 seja reiniciado. Verifique se o visor de sete segmentos mostra um estado `99` de .
   f. Determine como você atribuirá um endereço IP ao controlador de substituição.

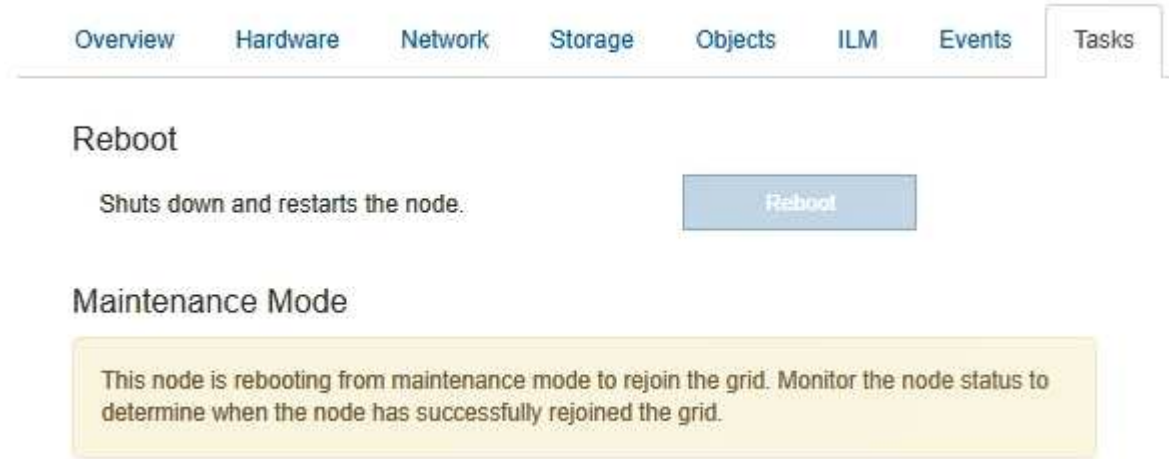
As etapas para atribuir um endereço IP ao controlador de substituição dependem se você conetou a porta de gerenciamento 1 a uma rede com um servidor DHCP e se todas as unidades estão protegidas.

- Se a porta de gerenciamento 1 estiver conetada a uma rede com um servidor DHCP, o novo controlador obterá seu endereço IP do servidor DHCP. Este valor pode ser diferente do endereço IP do controlador original.
- Se todas as unidades estiverem protegidas, você deverá usar a janela Gerenciamento Empresarial (EMW) no SANtricity Storage Manager para desbloquear as unidades protegidas. Não é possível aceder ao novo controlador até desbloquear as unidades com a chave guardada. Consulte as instruções da e-Series para substituir um controlador simplex E2800.

7. Se o aparelho usar unidades seguras, siga as instruções no procedimento de substituição do controlador E2800 para importar a chave de segurança da unidade.
8. Volte a colocar o aparelho no modo de funcionamento normal. No Instalador de dispositivos StorageGRID, selecione **Avançado controlador de reinicialização** e, em seguida, selecione **Reiniciar no StorageGRID**.

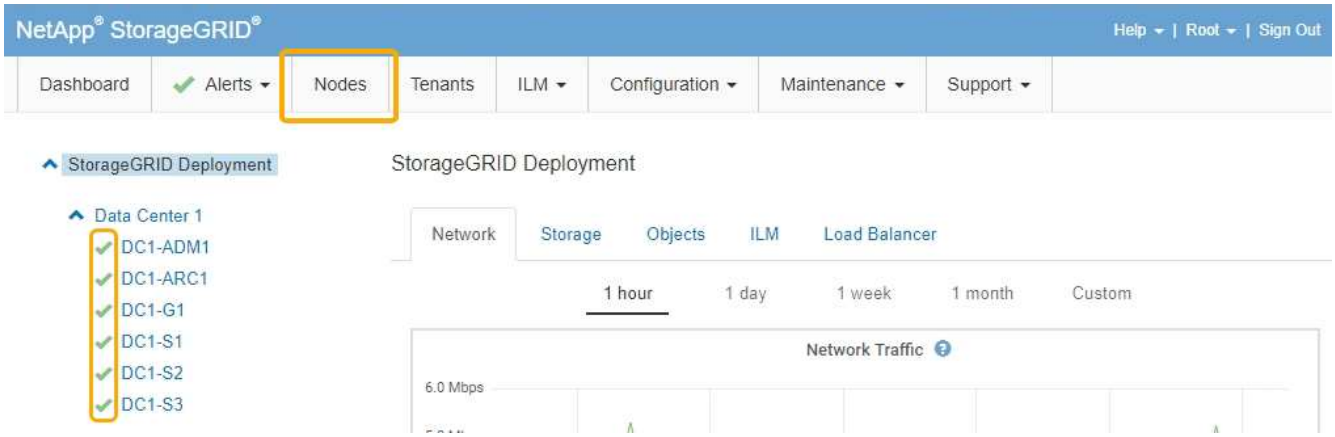


Durante a reinicialização, é apresentado o seguinte ecrã:



O aparelho reinicia e regozija-se com a grelha. Este processo pode demorar até 20 minutos.

9. Confirme se a reinicialização está concluída e se o nó voltou a ingressar na grade. No Gerenciador de Grade, verifique se a guia **nós** exibe um status normal ✔para o nó do dispositivo, indicando que nenhum alerta está ativo e o nó está conetado à grade.



10. No Gerenciador de sistemas do SANtricity, confirme se o novo controlador é ideal e colete dados de suporte.

Informações relacionadas

"Site de Documentação de sistemas NetApp e-Series"

Substituição do controlador E5700SG

Talvez seja necessário substituir o controlador E5700SG se ele não estiver funcionando de forma ideal ou se ele tiver falhado.

O que você vai precisar

- Você tem um controlador de substituição com o mesmo número de peça do controlador que está substituindo.
- Você baixou as instruções do e-Series para substituir um controlador E5700 com falha.

> ⓘ Use as instruções do e-Series para referência somente se você precisar de mais detalhes para executar uma etapa específica. Não confie nas instruções do e-Series para substituir um controlador no dispositivo StorageGRID, porque os procedimentos não são os mesmos. Por exemplo, as instruções do e-Series para o controlador E5700 descrevem como remover a bateria e a placa de interface do host (HIC) de um controlador com falha e instalá-los em um controlador de substituição. Estas etapas não se aplicam ao controlador E5700SG.

- Você tem etiquetas para identificar cada cabo conetado ao controlador.
- O aparelho foi colocado no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

O nó de storage do dispositivo não estará acessível quando você substituir o controlador. Se o controlador E5700SG estiver a funcionar o suficiente, pode efetuar um encerramento controlado no início deste procedimento.

Se você estiver substituindo o controlador antes de instalar o software StorageGRID, talvez você não consiga acessar o instalador do StorageGRID Appliance imediatamente após concluir este procedimento. Embora você possa acessar o Instalador de dispositivos StorageGRID de outros hosts na mesma sub-rede que o appliance, você não pode acessá-lo de hosts em outras sub-redes. Esta condição deve resolver-se dentro de 15 minutos (quando qualquer entrada de cache ARP para o tempo limite do controlador original), ou você pode limpar a condição imediatamente, limpando quaisquer entradas de cache ARP antigas manualmente do roteador ou gateway local.

Passos

1. Quando o aparelho tiver sido colocado no modo de manutenção, desligue o controlador E5700SG.
   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. Desligue o controlador E5700SG
      `shutdown -h now`
   c. Aguarde até que quaisquer dados na memória cache sejam gravados nas unidades.

      O LED verde Cache ative na parte de trás do controlador E2800 fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue.

2. Desligue a alimentação.
   a. Na página inicial do Gerenciador do sistema do SANtricity, selecione **Exibir operações em andamento**.
   b. Confirme se todas as operações foram concluídas.
   c. Desligue ambos os interrutores de alimentação do aparelho.
   d. Aguarde que todos os LEDs se desliguem.
3. Se as redes StorageGRID conetadas ao controlador usarem servidores DHCP:
   a. Observe os endereços MAC das portas no controlador de substituição (localizados em etiquetas no controlador).
   b. Peça ao administrador da rede que atualize as definições de endereço IP do controlador original para refletir os endereços MAC do controlador de substituição.

      Você deve garantir que os endereços IP do controlador original foram atualizados antes de aplicar energia ao controlador de substituição. Caso contrário, o controlador obterá novos endereços IP DHCP quando iniciar e poderá não conseguir reconetar-se ao StorageGRID. Esta etapa se aplica a todas as redes StorageGRID conetadas ao controlador.

4. Retire o controlador do aparelho:
   a. Coloque uma pulseira antiestática ou tome outras precauções antiestáticas.

b. Identifique os cabos e, em seguida, desligue os cabos e SFPs.

> Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos.

c. Solte o controlador do aparelho apertando o trinco na pega do came até soltar e, em seguida, abra a pega do came para a direita.

d. Utilizando as duas mãos e a pega do came, deslize o controlador para fora do aparelho.

> Utilize sempre duas mãos para suportar o peso do controlador.

5. Instale o controlador de substituição no aparelho.
   a. Vire o controlador ao contrário, de modo a que a tampa amovível fique virada para baixo.
   b. Com a pega do came na posição aberta, deslize o controlador até ao aparelho.
   c. Mova a alavanca do came para a esquerda para bloquear o controlador no lugar.
   d. Substitua os cabos e SFPs.
6. Ligue o aparelho e monitorize os LEDs do controlador e os ecrãs de sete segmentos.

   Depois que os controladores iniciarem com êxito, os visores de sete segmentos devem mostrar o seguinte:

   - Controlador E2800:

     O estado final é `99`.

   - Controlador E5700SG:

     O estado final é `HA`.
7. Confirme se o nó de armazenamento do dispositivo é exibido no Gerenciador de Grade e se nenhum alarme é exibido.

Informações relacionadas

"Site de Documentação de sistemas NetApp e-Series"

Substituição de outros componentes de hardware

Talvez seja necessário substituir uma bateria, unidade, ventilador ou fonte de alimentação do controlador no aparelho StorageGRID.

O que você vai precisar

- Você tem o procedimento de substituição de hardware do e-Series.
- O aparelho foi colocado no modo de manutenção se o procedimento de substituição de componentes exigir que desligue o aparelho.

  "Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Para substituir a bateria no controlador E2800, consulte as instruções nestas instruções para substituir o controlador E2800. Essas instruções descrevem como remover o controlador do aparelho, remover a bateria

do controlador, instalar a bateria e substituir o controlador.

Para substituir uma unidade, um recipiente do ventilador, um recipiente do ventilador, um recipiente de alimentação ou uma gaveta de unidade no aparelho, acesse os procedimentos do e-Series para manter o hardware do E2800.

SG5712 instruções de substituição de componentes

FRU	Consulte as instruções do e-Series para
Condução	Substituição de uma unidade nas gavetas de E2800 12 ou 24 unidades
Depósito da ventoinha de alimentação	Substituição de um recipiente do ventilador elétrico em E2800 prateleiras

SG5760 instruções de substituição de componentes

FRU	Consulte as instruções do e-Series para
Condução	Substituição de uma unidade em E2860 gavetas
Depósito de alimentação	Substituição de um recipiente de alimentação em E2860 prateleiras
Recipiente da ventoinha	Substituição de um recipiente do ventilador em E2860 prateleiras
Gaveta da unidade	Substituição de uma gaveta de unidades em E2860 gavetas

Informações relacionadas

"Substituição do controlador E2800"

"Site de Documentação de sistemas NetApp e-Series"

Alterar a configuração do link do controlador E5700SG

Pode alterar a configuração da ligação Ethernet do controlador E5700SG. Pode alterar o modo de ligação de porta, o modo de ligação de rede e a velocidade de ligação.

O que você vai precisar

Tem de colocar o controlador E5700SG no modo de manutenção. Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

"Colocar um aparelho no modo de manutenção"

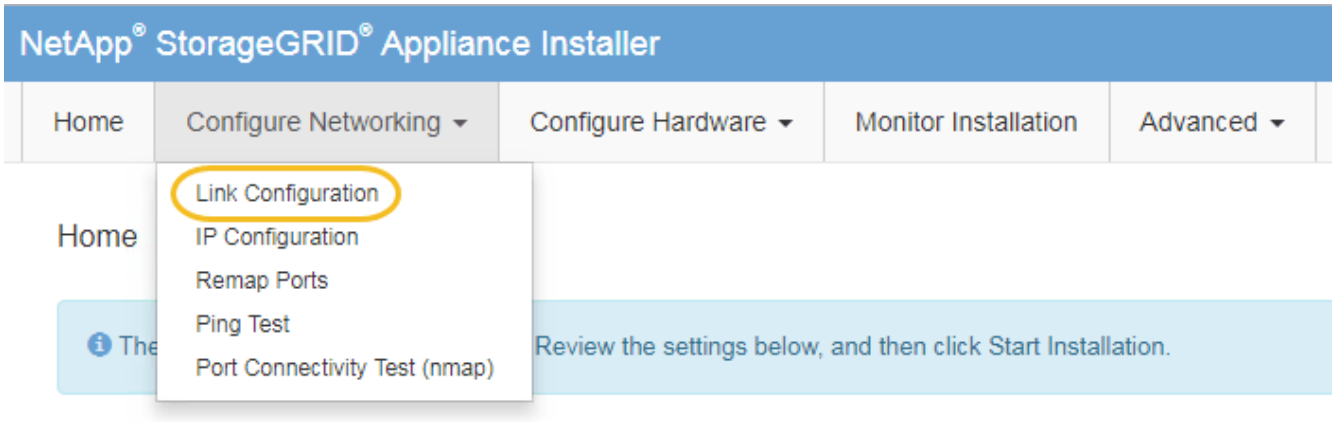
Sobre esta tarefa

As opções para alterar a configuração do link Ethernet do controlador E5700SG incluem:

- Alterar o modo **Port bond** de fixo para agregado, ou de agregado para fixo
- Alteração do **modo de ligação de rede** de ative-Backup para LACP ou de LACP para ative-Backup
- Ativar ou desativar a marcação de VLAN ou alterar o valor de uma tag VLAN
- Alteração da velocidade do link de 10 GbE para 25 GbE ou de 25 GbE para 10 GbE

Passos

1. Selecione **Configurar rede Configuração de ligação** no menu.



1. Faça as alterações desejadas na configuração do link.

   Para obter mais informações sobre as opções, consulte ""Configurando links de rede".

2. Quando estiver satisfeito com suas seleções, clique em **Salvar**.

   > Poderá perder a ligação se tiver efetuado alterações à rede ou à ligação através da qual está ligado. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do Instalador de appliance StorageGRID usando um dos outros endereços IP atribuídos ao appliance
   > **`https://E5700SG_Controller_IP:8443`**

   Se você fez alterações nas configurações de VLAN, a sub-rede do dispositivo pode ter sido alterada. Se você precisar alterar os endereços IP do dispositivo, siga as instruções para configurar endereços IP.

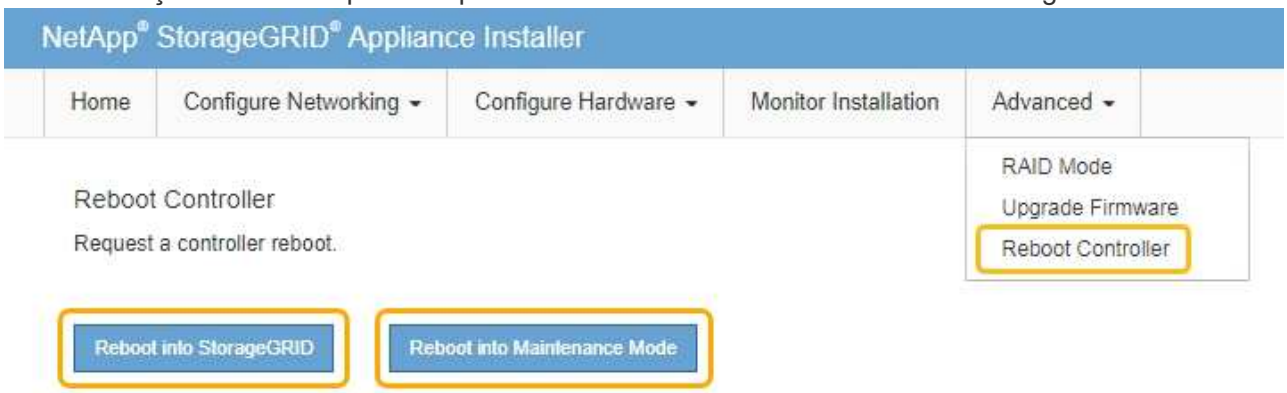
   "Definir a configuração IP"

3. No Instalador do StorageGRID Appliance, selecione **Configurar rede Teste de ping**.
4. Use a ferramenta Teste de ping para verificar a conetividade com endereços IP em qualquer rede que possa ter sido afetada pelas alterações de configuração de link feitas na Alterar a configuração do link etapa.

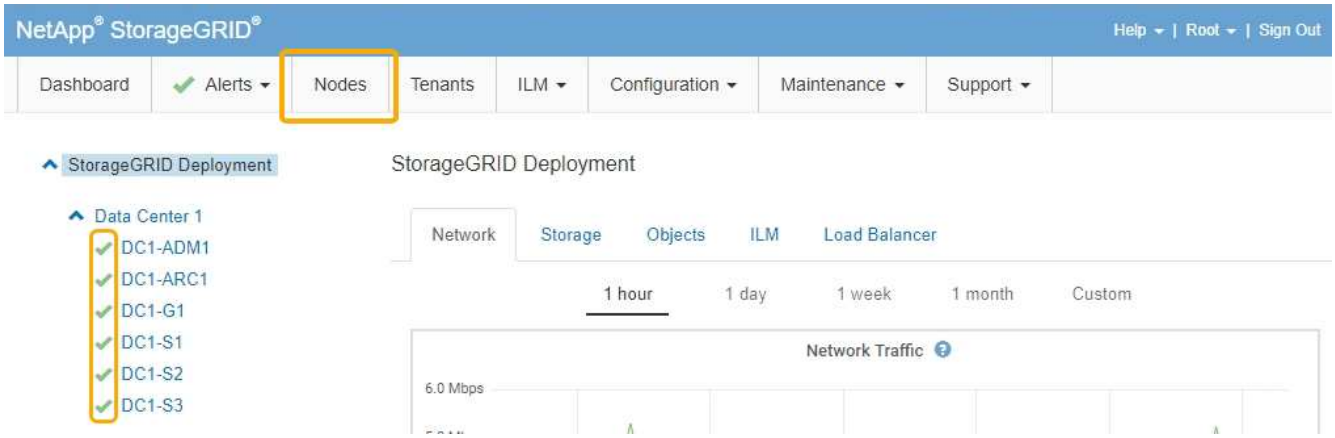
   Além de quaisquer outros testes que você escolher executar, confirme que você pode fazer ping no endereço IP da grade do nó Admin principal e no endereço IP da grade de pelo menos um outro nó de armazenamento. Se necessário, corrija quaisquer problemas de configuração do link.

5. Uma vez que você estiver satisfeito que as alterações de configuração do link estão funcionando, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

- Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
- Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Configurando links de rede (SG5700)"

Alterar a definição MTU

Você pode alterar a configuração MTU atribuída quando configurou endereços IP para o nó do dispositivo.

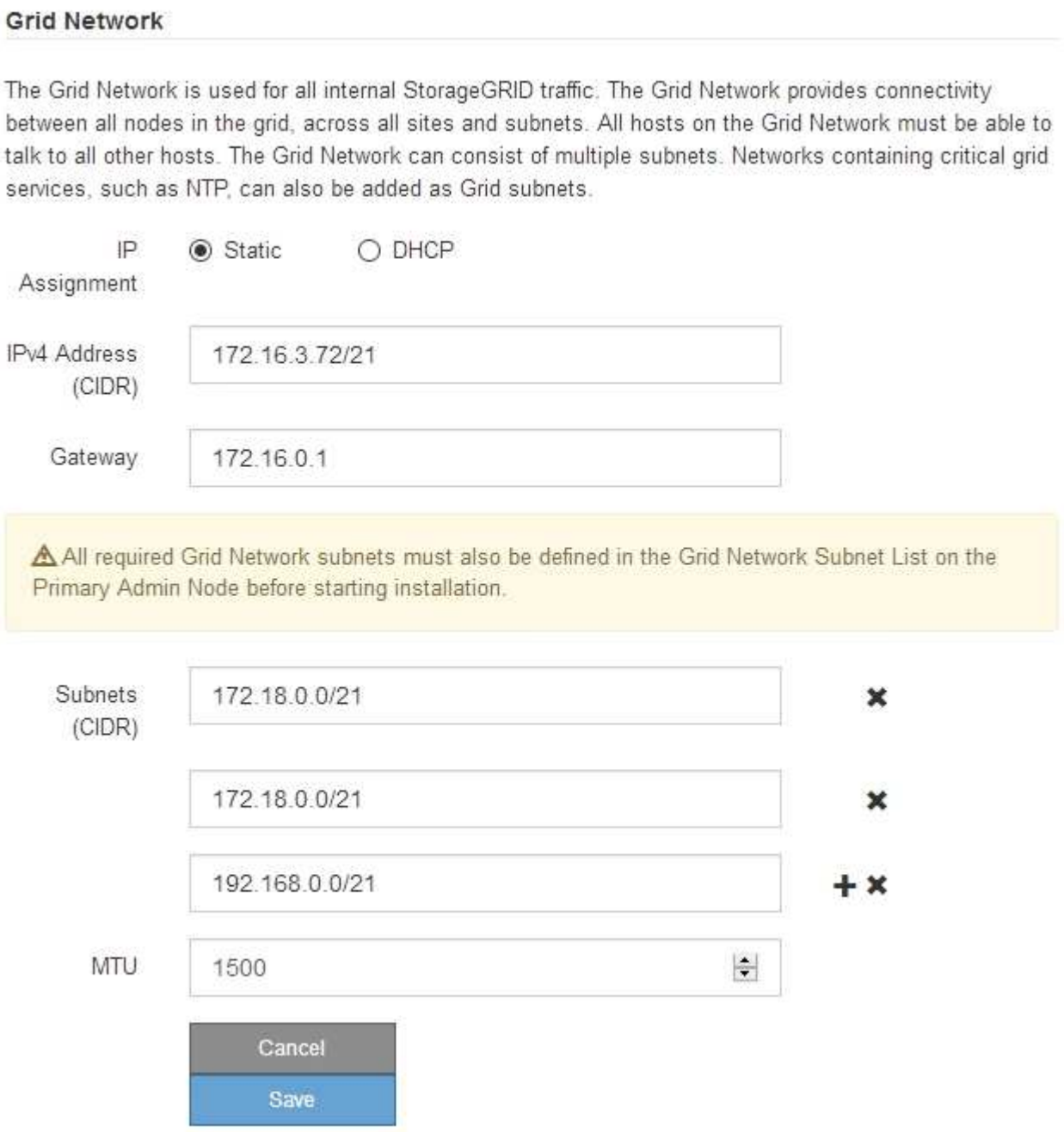
O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Passos

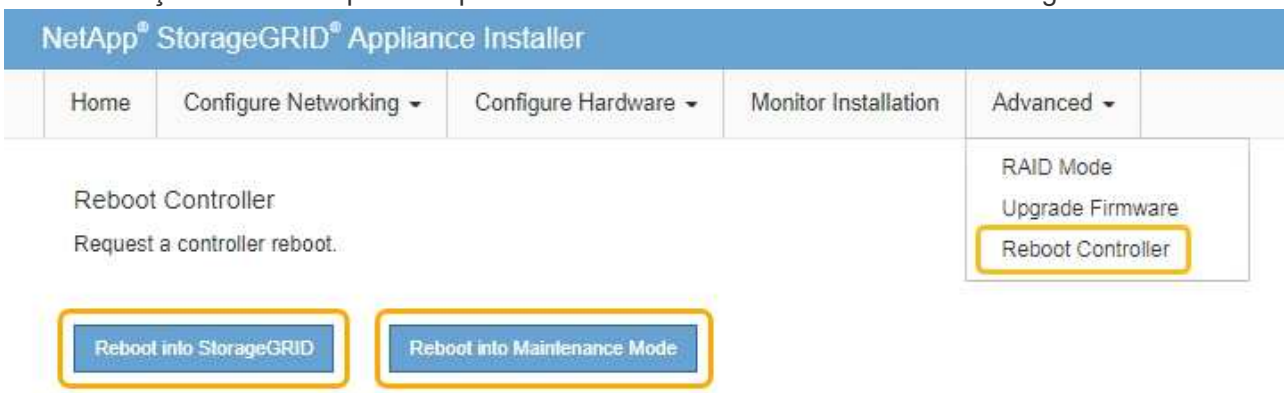
1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração IP**.
2. Faça as alterações desejadas nas configurações de MTU para rede de Grade, rede de Admin e rede de cliente.



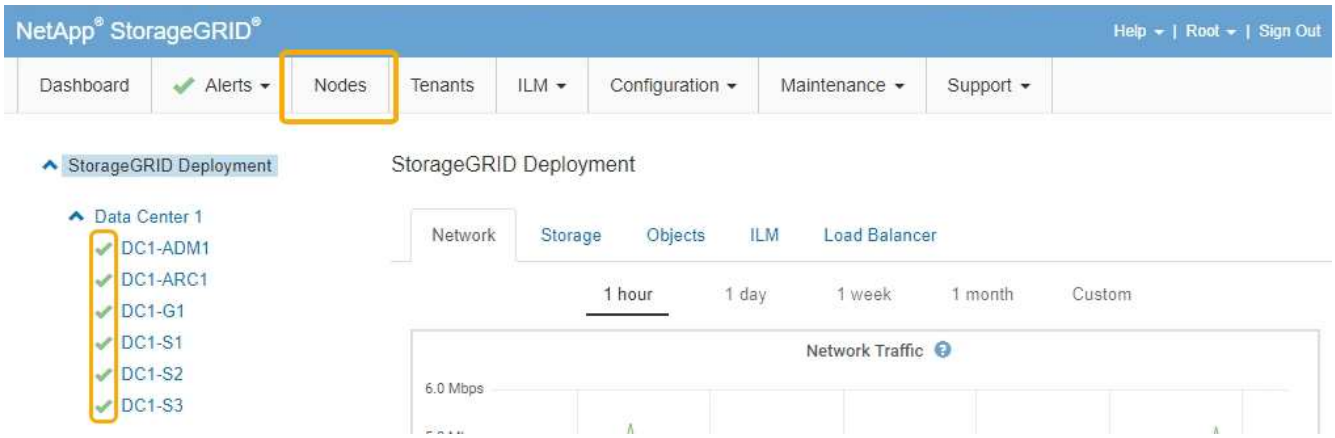
O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

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.

3. Quando estiver satisfeito com as definições, selecione **Guardar**.
4. Reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:
   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Administrar o StorageGRID"

Verificar a configuração do servidor DNS

Você pode verificar e alterar temporariamente os servidores DNS (sistema de nomes de domínio) que estão atualmente em uso por este nó de appliance.

O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Talvez seja necessário alterar as configurações do servidor DNS se um dispositivo criptografado não puder se conetar ao servidor de gerenciamento de chaves (KMS) ou ao cluster KMS porque o nome do host para o KMS foi especificado como um nome de domínio em vez de um endereço IP. Quaisquer alterações efetuadas nas definições de DNS do dispositivo são temporárias e perdem-se quando sai do modo de manutenção. Para tornar essas alterações permanentes, especifique os servidores DNS no Gerenciador de Grade (**Manutenção rede servidores DNS**).

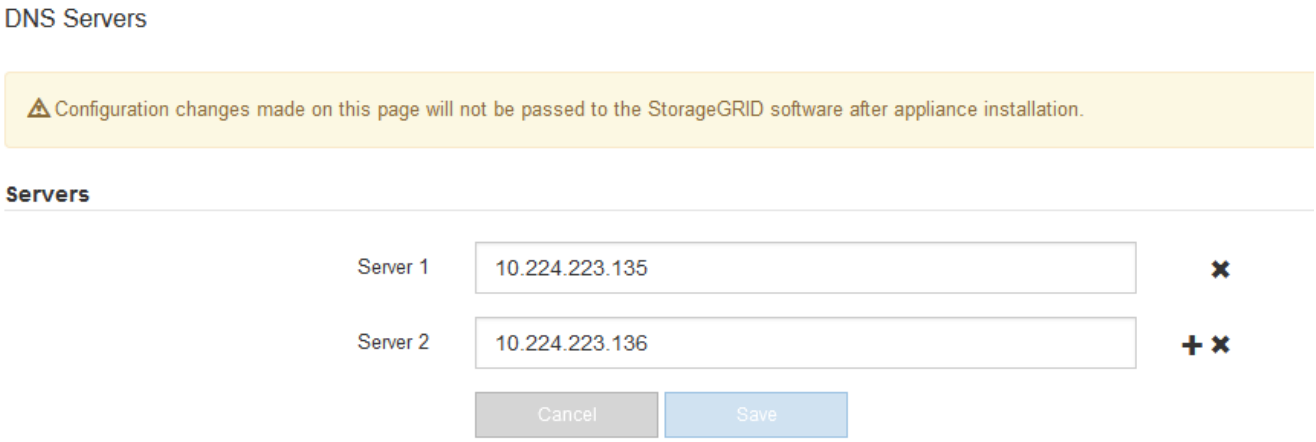
- As alterações temporárias na configuração DNS são necessárias apenas para dispositivos encriptados por nó onde o servidor KMS é definido utilizando um nome de domínio totalmente qualificado, em vez de um endereço IP, para o nome de anfitrião.
- Quando um dispositivo criptografado por nó se coneta a um KMS usando um nome de domínio, ele deve se conetar a um dos servidores DNS definidos para a grade. Um desses servidores DNS converte o nome de domínio em um endereço IP.
- Se o nó não conseguir alcançar um servidor DNS para a grade, ou se você alterou as configurações de DNS em toda a grade quando um nó de dispositivo criptografado por nó estava off-line, o nó não consegue se conetar ao KMS. Os dados criptografados no dispositivo não podem ser descriptografados até que o problema de DNS seja resolvido.

Para resolver um problema de DNS que impede a ligação KMS, especifique o endereço IP de um ou mais servidores DNS no Instalador de aplicações StorageGRID. Essas configurações de DNS temporárias permitem que o dispositivo se conete ao KMS e descriptografar dados no nó.

Por exemplo, se o servidor DNS para a grade mudar enquanto um nó criptografado estava off-line, o nó não será capaz de alcançar o KMS quando ele voltar on-line, uma vez que ainda está usando os valores DNS anteriores. A introdução do novo endereço IP do servidor DNS no Instalador de aplicações StorageGRID permite que uma ligação KMS temporária desencripte os dados do nó.

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração de DNS**.
2. Verifique se os servidores DNS especificados estão corretos.



3. Se necessário, altere os servidores DNS.

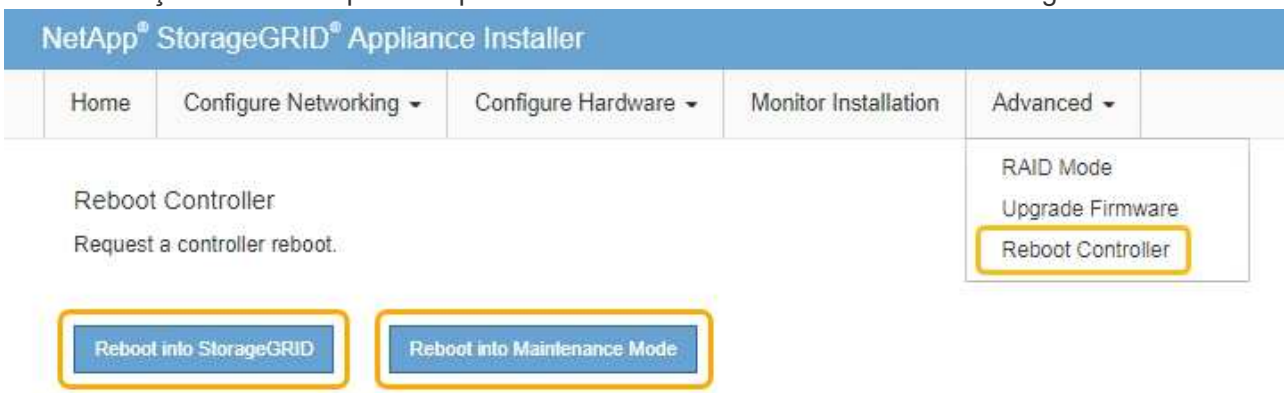
> As alterações efetuadas nas definições de DNS são temporárias e perdem-se quando sai do modo de manutenção.

4. Quando estiver satisfeito com as definições de DNS temporárias, selecione **Guardar**.

   O nó usa as configurações do servidor DNS especificadas nesta página para se reconetar ao KMS, permitindo que os dados no nó sejam descriptografados.

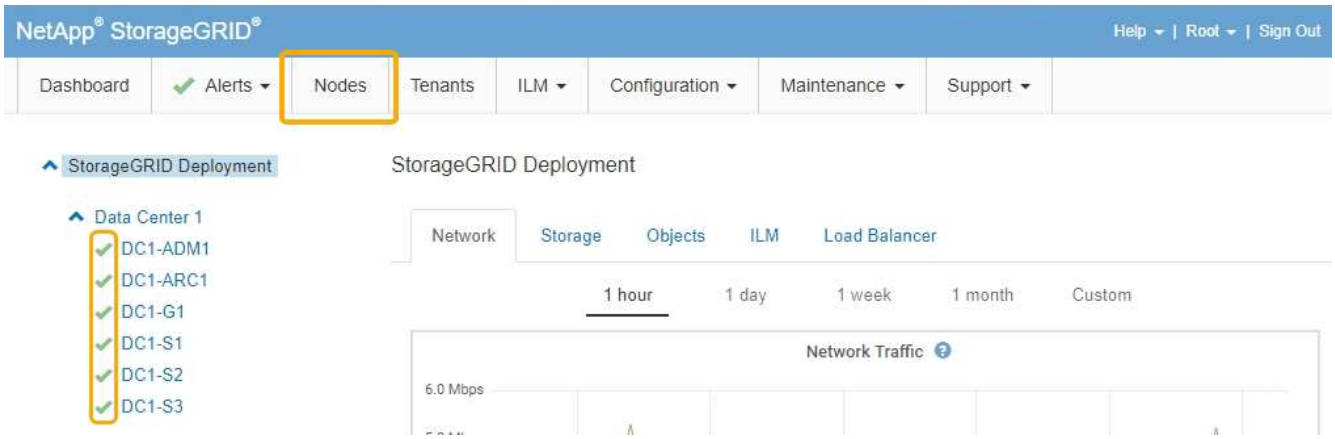
5. Depois que os dados do nó forem descriptografados, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Quando o nó reinicializa e realegra a grade, ele usa os servidores DNS de todo o sistema listados no Gerenciador de Grade. Depois de reingressar na grade, o dispositivo não usará mais os servidores DNS temporários especificados no Instalador de dispositivos StorageGRID enquanto o dispositivo estava no modo de manutenção.

Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔ para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Monitorização da encriptação do nó no modo de manutenção

Se você ativou a criptografia de nó para o dispositivo durante a instalação, poderá monitorar o status de criptografia de nó de cada nó do dispositivo, incluindo os detalhes do estado de criptografia de nó e do servidor de gerenciamento de chaves (KMS).

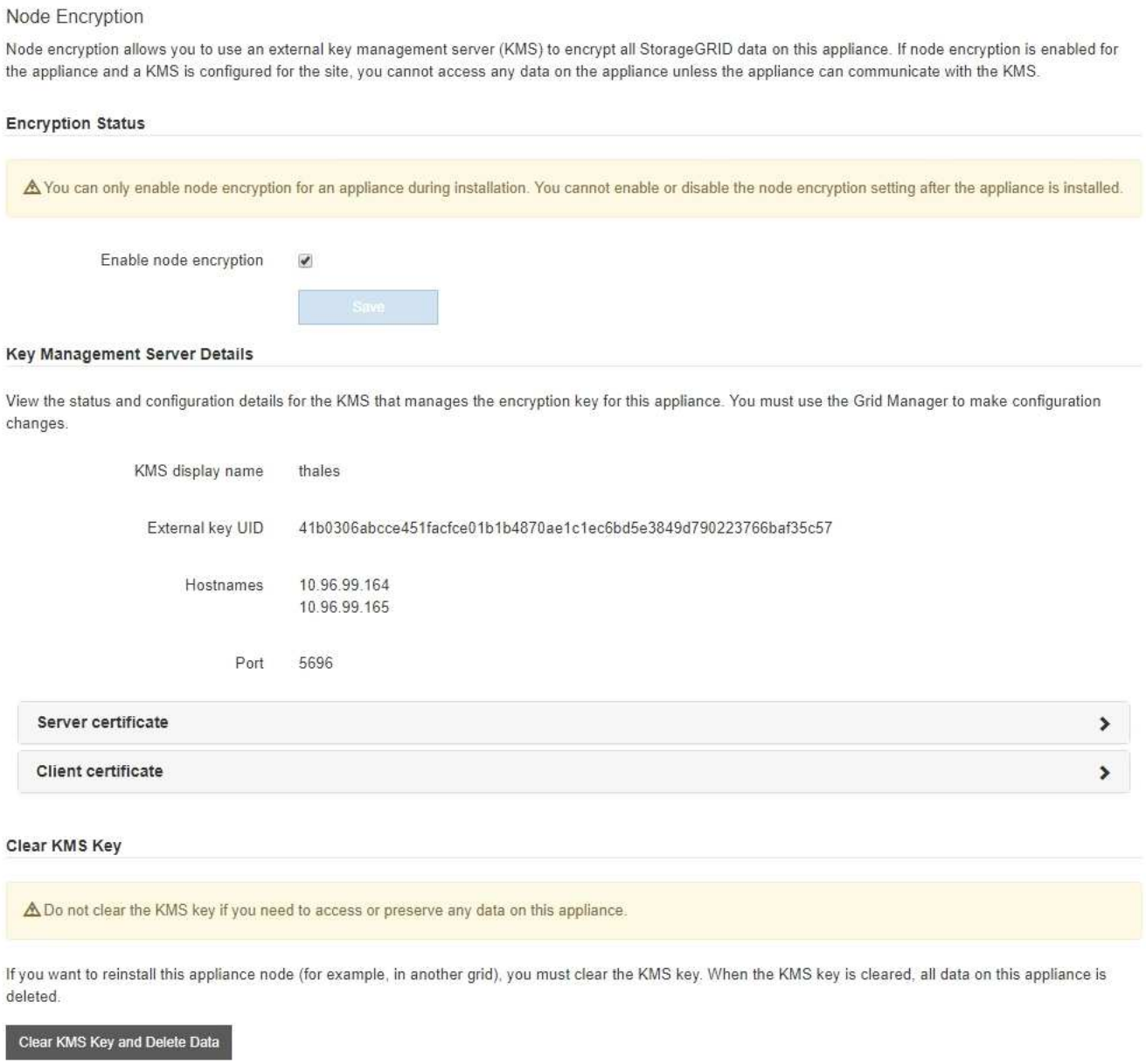
O que você vai precisar

- A criptografia do nó deve ter sido ativada para o dispositivo durante a instalação. Não é possível ativar a criptografia de nó depois que o dispositivo estiver instalado.
- O aparelho foi colocado no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Configurar hardware criptografia de nó**.



A página criptografia do nó inclui estas três seções:

- O estado de encriptação mostra se a encriptação do nó está ativada ou desativada para o dispositivo.
- Detalhes do servidor de gerenciamento de chaves mostra informações sobre o KMS sendo usado para criptografar o dispositivo. Você pode expandir as seções de certificado de servidor e cliente para exibir detalhes e status do certificado.
  - Para resolver problemas com os próprios certificados, como a renovação de certificados expirados, consulte as informações sobre o KMS nas instruções de administração do StorageGRID.
  - Se houver problemas inesperados ao se conetar aos hosts KMS, verifique se os servidores DNS (sistema de nomes de domínio) estão corretos e se a rede do appliance está configurada corretamente.

    "Verificar a configuração do servidor DNS"

  - Se você não conseguir resolver os problemas do certificado, entre em Contato com o suporte técnico.

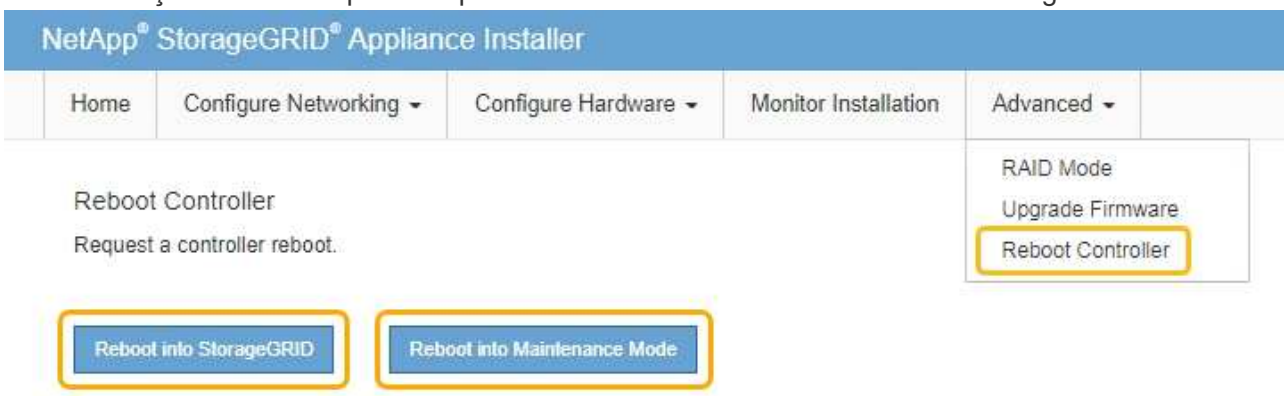
- Limpar chave KMS desativa a criptografia de nó para o dispositivo, remove a associação entre o dispositivo e o servidor de gerenciamento de chaves que foi configurado para o site StorageGRID e exclui todos os dados do dispositivo. Tem de limpar a chave KMS antes de poder instalar o aparelho noutro sistema StorageGRID.

  "Limpando a configuração do servidor de gerenciamento de chaves"

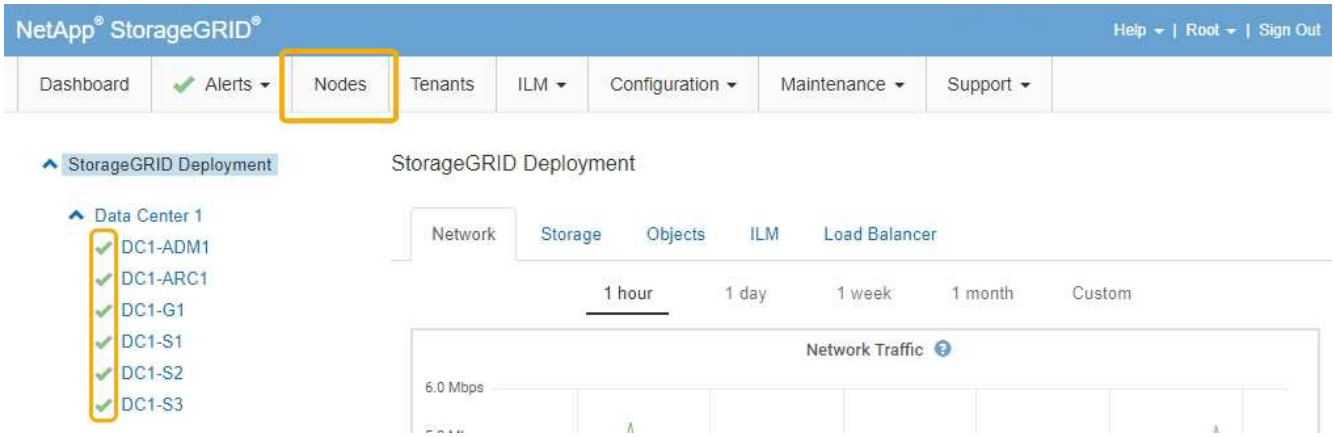
  Limpar a configuração do KMS exclui os dados do dispositivo, tornando-os permanentemente inacessíveis. Estes dados não são recuperáveis.

2. Quando terminar de verificar o estado da encriptação do nó, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Administrar o StorageGRID"

Limpando a configuração do servidor de gerenciamento de chaves

Limpar a configuração do servidor de gerenciamento de chaves (KMS) desativa a criptografia de nó no seu dispositivo. Depois de limpar a configuração do KMS, os dados do seu aparelho são excluídos permanentemente e não são mais acessíveis. Estes dados não são recuperáveis.

O que você vai precisar

Se você precisar preservar dados no dispositivo, você deve executar um procedimento de desativação de nós antes de limpar a configuração do KMS.

> Quando o KMS é eliminado, os dados no aparelho serão eliminados permanentemente e deixarão de estar acessíveis. Estes dados não são recuperáveis.

Desative o nó para mover quaisquer dados que ele contenha para outros nós no StorageGRID. Consulte as instruções de recuperação e manutenção para a desativação do nó da grade.

Sobre esta tarefa

A limpeza da configuração do KMS do appliance desativa a criptografia do nó, removendo a associação entre o nó do appliance e a configuração do KMS para o site do StorageGRID. Os dados no dispositivo são então excluídos e o dispositivo é deixado em um estado de pré-instalação. Este processo não pode ser revertido.

Você deve limpar a configuração do KMS:

- Antes de instalar o aparelho em outro sistema StorageGRID, isso não usa um KMS ou que usa um KMS diferente.

  > Não limpe a configuração do KMS se você planeja reinstalar um nó de dispositivo em um sistema StorageGRID que usa a mesma chave KMS.

- Antes de poder recuperar e reinstalar um nó onde a configuração do KMS foi perdida e a chave KMS não é recuperável.
- Antes de devolver qualquer aparelho que estava anteriormente em uso em seu site.
- Após a desativação de um dispositivo que tinha a criptografia de nó ativada.

> Desative o dispositivo antes de limpar o KMS para mover seus dados para outros nós em seu sistema StorageGRID. Limpar o KMS antes de desativar o aparelho resultará em perda de dados e pode tornar o aparelho inoperável.

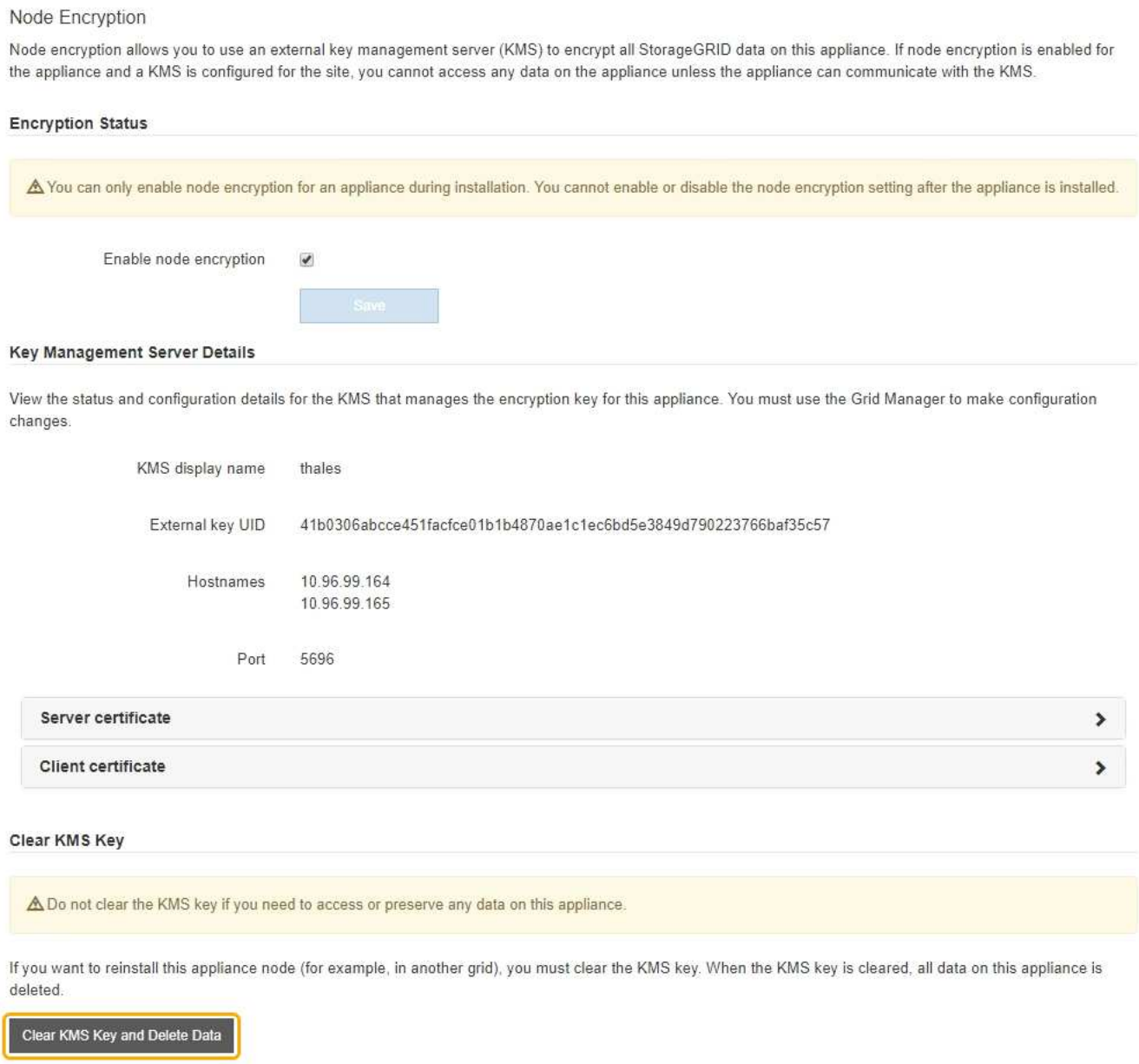
Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

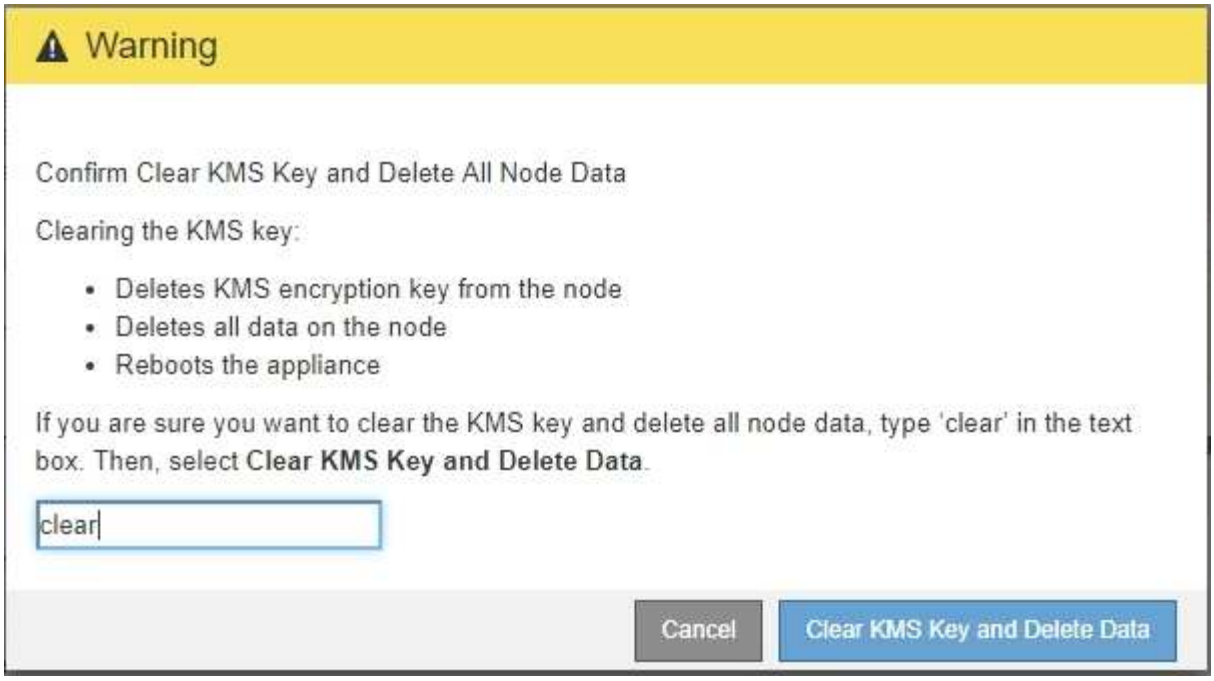
   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configure hardware Node Encryption**.



> Se a configuração do KMS for limpa, os dados no dispositivo serão excluídos permanentemente. Estes dados não são recuperáveis.

3. Na parte inferior da janela, selecione **Limpar chave KMS e Excluir dados**.
4. Se você tem certeza de que deseja limpar a configuração do KMS, digite `clear` e selecione **Limpar chave KMS e Excluir dados**.



A chave de criptografia KMS e todos os dados são excluídos do nó e o dispositivo é reinicializado. Isso pode levar até 20 minutos.

5. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E **`https://Controller_IP:8443`**

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

6. Selecione **Configure hardware Node Encryption**.
7. Verifique se a criptografia do nó está desativada e se as informações de chave e certificado em **Key Management Server Details** e **Clear KMS Key e Delete Data** control são removidas da janela.

   A criptografia do nó não pode ser reativada no dispositivo até que seja reinstalada em uma grade.

Depois de terminar

Depois de o aparelho reiniciar e verificar se o KMS foi limpo e se o aparelho está num estado de pré-instalação, pode remover fisicamente o aparelho do sistema StorageGRID. Consulte as instruções de recuperação e manutenção para obter informações sobre como preparar um aparelho para reinstalação.

Informações relacionadas

"Administrar o StorageGRID"

"Manter recuperar"

SG5600 dispositivos de armazenamento

Saiba como instalar e manter dispositivos StorageGRID SG5612 e SG5660.

- "Visão geral do dispositivo StorageGRID"

- "Visão geral da instalação e implantação"
- "Preparando-se para a instalação"
- "Instalar o hardware"
- "Configurar o hardware"
- "Implantando um nó de storage de dispositivos"
- "Monitorização da instalação do dispositivo de armazenamento"
- "Automatizando a instalação e a configuração do dispositivo"
- "Visão geral das APIs REST de instalação"
- "Solução de problemas da instalação do hardware"
- "Manutenção do aparelho SG5600"

Visão geral do dispositivo StorageGRID

O dispositivo StorageGRID SG5600 é uma plataforma de storage e computação integrada que opera como nó de storage em uma grade StorageGRID.

O dispositivo StorageGRID SG5600 inclui os seguintes componentes:

Componente	Descrição
Controlador E5600SG	Servidor de computaçãoO controlador E5600SG executa o sistema operacional Linux e o software StorageGRID. Este controlador liga-se ao seguinte: • As redes Admin, Grid e Client para o sistema StorageGRID • A controladora E2700, usando caminhos SAS duplos (ativo/ativo) com a controladora E5600SG operando como iniciador
Controlador E2700	Controlador de armazenamento o controlador E2700 funciona como um storage padrão da série e no modo simplex e executa o sistema operacional SANtricity (firmware do controlador). Este controlador liga-se ao seguinte: • A rede de gerenciamento onde o SANtricity Storage Manager está instalado • A controladora E5600SG, usando caminhos SAS duplos (ativo/ativo) com a controladora E2700 operando como destino

O aparelho SG5600 também inclui os seguintes componentes, dependendo do modelo:

Componente	Modelo SG5612	Modelo SG5660
Unidades	Unidades NL-SAS de 12 TB	Unidades NL-SAS de 60 TB
Compartimento	Compartimento DE1600U, um chassi de duas unidades de rack (2UU) que aloja as unidades e as controladoras	Compartimento DE6600U, um chassi de quatro unidades de rack (4UU) que aloja as unidades e as controladoras
Fontes de alimentação e ventiladores	Dois coletores de ventilador de potência	Duas fontes de alimentação e duas ventoinhas

O controlador E5600SG é altamente personalizado para uso no dispositivo StorageGRID. Todos os outros componentes funcionam conforme descrito na documentação da Série e, exceto conforme indicado nestas instruções.

O storage bruto máximo disponível em cada nó de storage do dispositivo StorageGRID é fixo, baseado no modelo e na configuração do dispositivo. Não é possível expandir o storage disponível adicionando uma gaveta com unidades adicionais.

Recursos do dispositivo StorageGRID

O dispositivo StorageGRID SG5600 fornece uma solução de storage integrada para a criação de um novo sistema StorageGRID ou para a expansão da capacidade de um sistema existente.

O dispositivo StorageGRID fornece os seguintes recursos:

- Combina a computação do nó de storage da StorageGRID e elementos de storage em uma solução única, eficiente e integrada
- Simplifica a instalação e configuração de um nó de storage, automatizando a maior parte do processo necessário
- Fornece uma solução de storage de alta densidade com duas opções de compartimento: Uma 2U e uma 4U
- Usa interfaces IP de 10 GbE diretamente no nó de storage, sem a necessidade de interfaces de storage intermediárias, como FC ou iSCSI
- Pode ser usado em um ambiente de grade híbrida que usa dispositivos StorageGRID e nós de storage virtuais (baseados em software)
- Inclui armazenamento pré-configurado e vem pré-carregado com o Instalador de dispositivos StorageGRID (no controlador E5600SG) para implementação e integração de software prontos para o campo

Diagramas de hardware

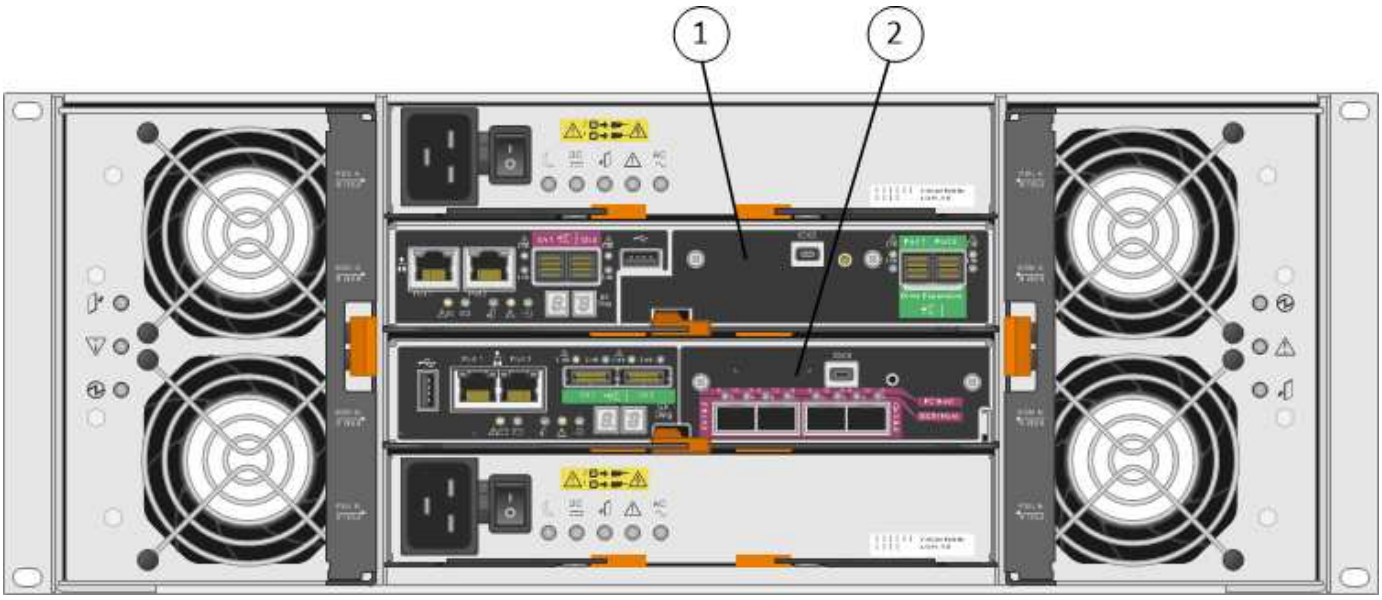
Os modelos SG5612 e SG5660 do dispositivo StorageGRID incluem um controlador E2700 e um controlador E5600SG. Você deve rever os diagramas para aprender as diferenças entre os modelos e os controladores.

Modelo SG5612 2U: Vista traseira do controlador E2700 e do controlador E5600SG

	Descrição
1	Controlador E2700
2	Controlador E5600SG

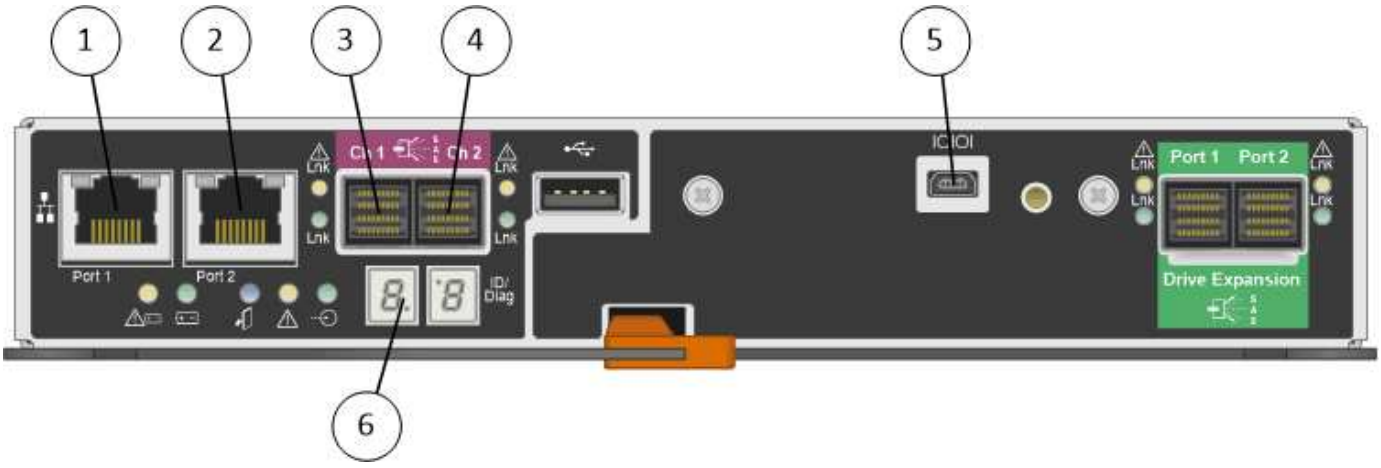
Modelo SG5660 4U: Vista traseira do controlador E2700 e do controlador E5600SG

O controlador E2700 está acima do controlador E5600SG.



	Descrição
1	Controlador E2700
2	Controlador E5600SG

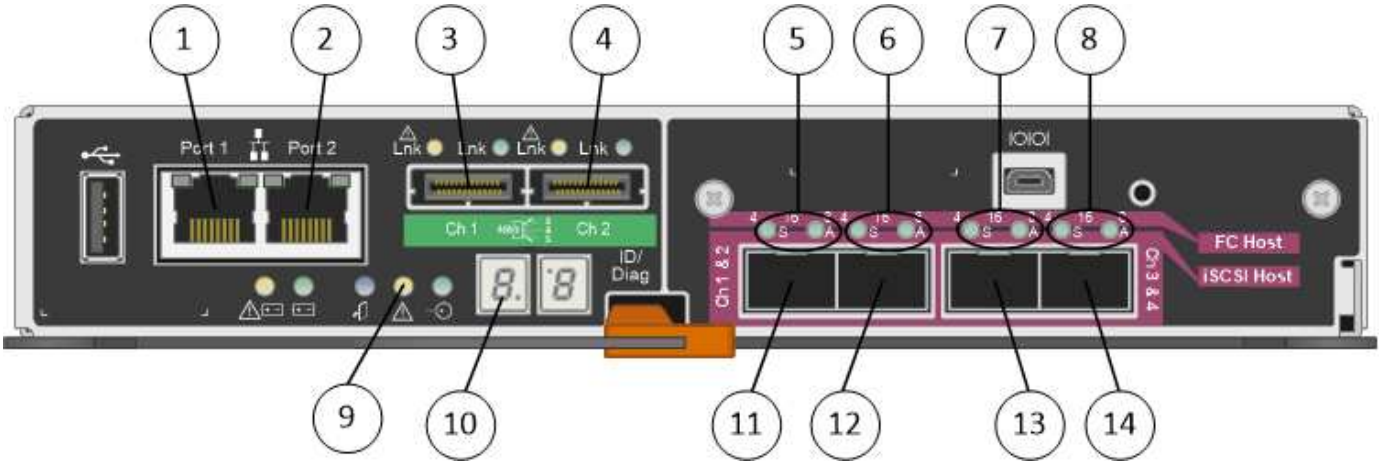
Vista traseira do controlador E2700



	Descrição
1	Porta de gerenciamento 1 (Conete-se à rede onde o SANtricity Storage Manager está instalado.)
2	Porta de gerenciamento 2 (use durante a instalação para conetar a um laptop.)
3	Porta de interconexão SAS 1
4	Porta de interconexão SAS 2
5	Porta de conexão serial
6	Visor de sete segmentos

As duas portas SAS com o rótulo Drive Expansion (verde) na parte traseira do controlador E2700 não são usadas. O dispositivo StorageGRID não é compatível com compartimentos de unidades de expansão.

Vista traseira do controlador E5600SG



	Descrição
1	Porta de gerenciamento 1 (conetar à rede de administração para StorageGRID.)
2	Opções da porta de gerenciamento 2: • Vincular com a porta de gerenciamento 1 para uma conexão redundante com a rede de administração para StorageGRID. • Deixe desconetado e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, use para configuração IP se os endereços IP atribuídos pelo DHCP não estiverem disponíveis.
3	Porta de interconexão SAS 1
4	Porta de interconexão SAS 2
5	LEDs de falha e ativos para a porta de rede 1 de 10 GbE
6	LEDs de falha e ativos para a porta de rede 2 de 10 GbE
7	LEDs de falha e ativos para a porta de rede 3 de 10 GbE
8	LEDs de falha e ativos para a porta de rede 4 de 10 GbE
9	Precisa de atenção LED
10	Visor de sete segmentos
11	Porta de rede de 10 GbE 1
12	Porta de rede de 10 GbE 2
13	Porta de rede de 10 GbE 3
14	Porta de rede de 10 GbE 4

A placa de interface do host (HIC) no controlador StorageGRID Appliance E5600SG suporta apenas conexões Ethernet de 10 GB. Não pode ser utilizado para ligações iSCSI.

Visão geral da instalação e implantação

Você pode instalar um ou mais dispositivos StorageGRID quando implantar o StorageGRID pela primeira vez ou adicionar nós de storage do dispositivo posteriormente como parte de uma expansão. Você também pode precisar instalar um nó de armazenamento de dispositivos como parte de uma operação de recuperação.

Adicionar um dispositivo de storage StorageGRID a um sistema StorageGRID inclui quatro etapas principais:

1. Preparação para a instalação:
   - Preparar o local de instalação
   - Desembalar as caixas e verificar o conteúdo
   - Obtenção de equipamentos e ferramentas adicionais
   - Recolha de endereços IP e informações de rede
   - Opcional: Configurando um servidor de gerenciamento de chaves externo (KMS) se você planeja criptografar todos os dados do dispositivo. Consulte detalhes sobre o gerenciamento de chaves externas nas instruções de administração do StorageGRID.
2. Instalar o hardware:
   - Registar o hardware
   - Instalar o aparelho num armário ou num rack
   - Instalar as unidades (apenas SG5660)
   - Fazer o cabeamento do dispositivo
   - Conexão dos cabos de energia e alimentação
   - Exibindo códigos de status de inicialização
3. Configurar o hardware:
   - Acessando o SANtricity Storage Manager, definindo um endereço IP estático para a porta de gerenciamento 1 no controlador E2700 e configurando as configurações do SANtricity Storage Manager
   - Acessando o Instalador do StorageGRID Appliance e configurando as configurações de IP de rede e link necessárias para se conetar a redes StorageGRID
   - Opcional: Habilitando a criptografia de nó se você planeja usar um KMS externo para criptografar dados do dispositivo.
   - Opcional: Alterar o modo RAID.
4. Implantando o dispositivo como nó de storage:

Tarefa	Consulte
Implantando um nó de storage de dispositivos em um novo sistema StorageGRID	"Implantando um nó de storage de dispositivos"
Adicionando um nó de storage de dispositivo a um sistema StorageGRID existente	Instruções para expandir um sistema StorageGRID
Implantando um nó de storage de dispositivos como parte de uma operação de recuperação de nó de storage	Instruções para recuperação e manutenção

Informações relacionadas

"Preparando-se para a instalação"

"Instalar o hardware"

"Configurar o hardware"

"Expanda sua grade"

"Manter recuperar"

"Administrar o StorageGRID"

Preparando-se para a instalação

Preparar a instalação de um dispositivo StorageGRID implica preparar o local e obter todo o hardware, cabos e ferramentas necessários. Você também deve coletar endereços IP e informações de rede.

Passos

- "Preparação do local (SG5600)"
- "Desembalar as caixas (SG5600)"
- "Obtenção de equipamentos e ferramentas adicionais (SG5600)"
- "Requisitos de manutenção do laptop"
- "Requisitos do navegador da Web"
- "Rever as ligações de rede do dispositivo"
- "Recolha de informações de instalação (SG5600)"

Preparação do local (SG5600)

Antes de instalar o aparelho, certifique-se de que o local e o gabinete ou rack que pretende utilizar cumprem as especificações de um dispositivo StorageGRID.

Passos

1. Confirme se o local atende aos requisitos de temperatura, umidade, faixa de altitude, fluxo de ar, dissipação de calor, fiação, energia e aterramento. Consulte o NetApp Hardware Universe para obter mais informações.
2. Obtenha um gabinete ou rack de 19 polegadas (48,3 cm) para encaixar prateleiras deste tamanho (sem cabos):

Modelo do aparelho	Altura	Largura	Profundidade	Peso máximo
SG5612 (12 unidades)	3,40 pol. (8,64 cm)	19,0 pol. (48,26 cm)	21,75 pol. (55,25 cm)	13 59,5 lb (27 kg)
SG5660 (60 unidades)	7,00 pol. (17,78 cm)	17,75 pol. (45,08 cm)	32,50 pol. (82,55 cm)	13 236,2 lb. (107,1 kg)

3. Instale todos os switches de rede necessários. Consulte a ferramenta de Matriz de interoperabilidade do NetApp para obter informações sobre compatibilidade.

Informações relacionadas

"NetApp Hardware Universe"

"Interoperabilidade do NetApp"

Desembalar as caixas (SG5600)

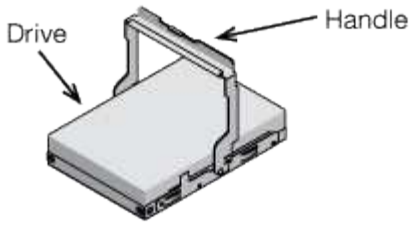
Antes de instalar o dispositivo StorageGRID, desembale todas as caixas e compare o conteúdo com os itens no saco de embalagem.

- * SG5660 gabinete, um chassi de 4UU com 60 unidades*

- * SG5612 gabinete, um chassi de 2UU com 12 unidades*

- * 4U bisel ou 2U endcaps*

- **Unidades NL-SAS**



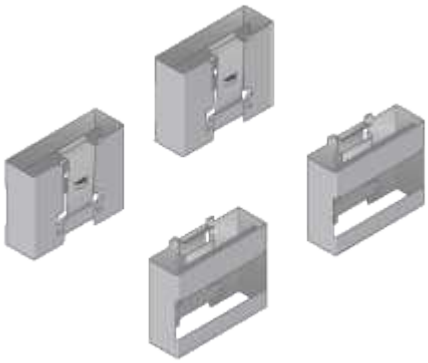
Os acionamentos são pré-instalados no 2U SG5612, mas não no 4U SG5660 para segurança de envio.

- **Controlador E5600SG**

- **Controlador E2700**

- * Trilhos de montagem e parafusos*

- * Alças de gabinete (apenas 4U gabinetes)*



Cabos e conetores

O envio para o dispositivo StorageGRID inclui os seguintes cabos e conetores:

- * Cabos de alimentação para o seu país*

O aparelho é fornecido com dois cabos de alimentação CA para ligação a uma fonte de alimentação externa, como uma ficha de parede. O gabinete pode ter cabos de alimentação especiais que você usa em vez dos cabos de alimentação fornecidos com o aparelho.

- **Cabos de interconexão SAS**

Dois cabos de interconexão SAS de 0,5 metros com conetores mini-SAS-HD e mini-SAS.

O conetor quadrado se coneta ao controlador E2700 e o conetor retangular se coneta ao controlador E5600SG.

Obtenção de equipamentos e ferramentas adicionais (SG5600)

Antes de instalar o aparelho SG5600, confirme se tem todo o equipamento e ferramentas adicionais de que necessita.

- **Chaves de fenda**

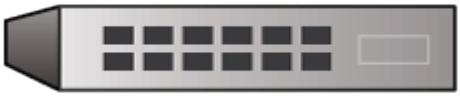
Chave de fendas Phillips n.o 2

Aparafusadoras de lâmina plana médias

- * Pulseira antiestática*

- **Cabos Ethernet**

- **Comutador Ethernet**



- * Serviço de laptop*

Requisitos de manutenção do laptop

Antes de instalar o hardware do dispositivo StorageGRID, você deve verificar se o laptop de serviço tem os recursos mínimos necessários.

O laptop de serviço, que é necessário para a instalação de hardware, deve atender aos seguintes requisitos:

- Sistema operativo Microsoft Windows
- Porta de rede
- Navegador da Web suportado
- NetApp SANtricity Storage Manager versão 11,40 ou posterior
- Cliente SSH (por exemplo, PuTTY)

Informações relacionadas

"Requisitos do navegador da Web"

"Documentação do NetApp: SANtricity Storage Manager"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Rever as ligações de rede do dispositivo

Antes de instalar o dispositivo StorageGRID, você deve entender quais redes podem ser conetadas ao dispositivo e como as portas em cada controlador são usadas.

Redes de dispositivos StorageGRID

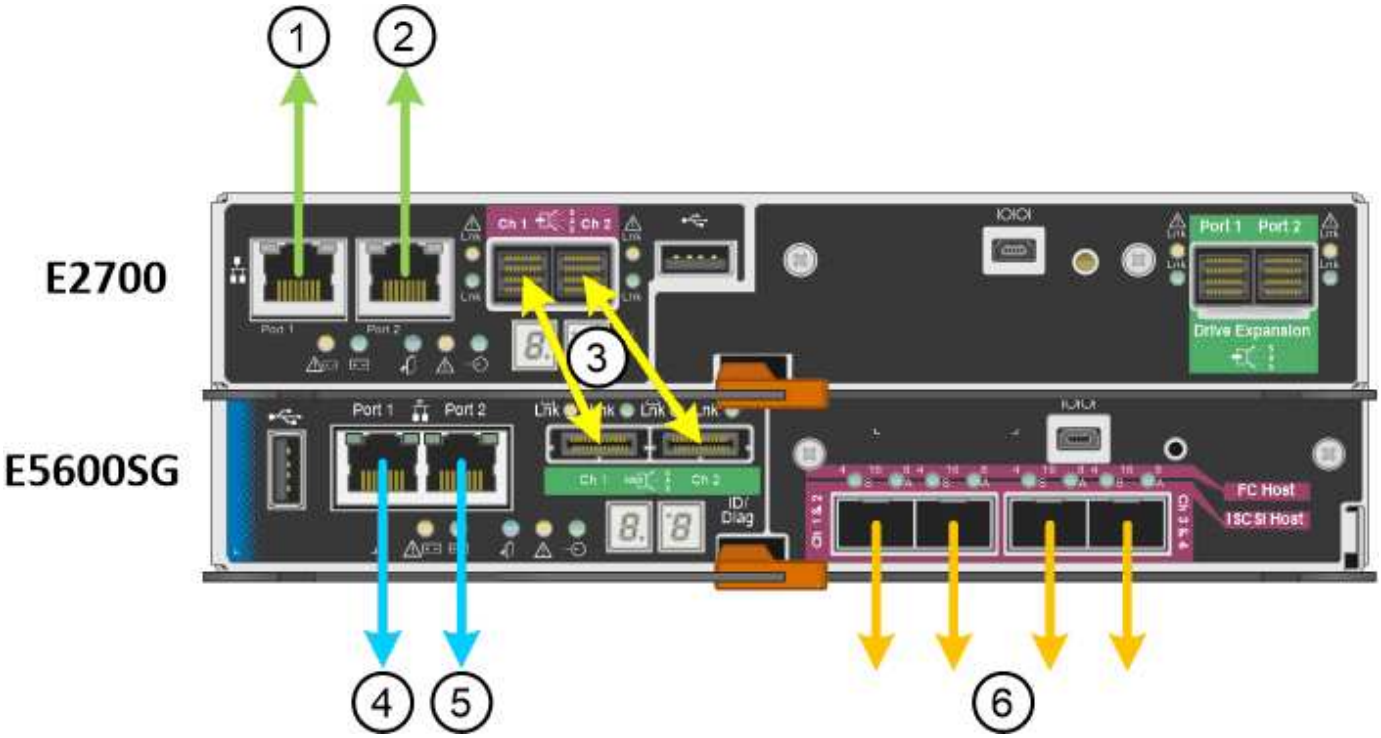
Ao implantar um dispositivo StorageGRID como nó de armazenamento, você pode conectá-lo às seguintes redes:

- **Rede de grade para StorageGRID**: A rede de grade é usada para todo o tráfego interno de StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes. A rede de Grade é necessária.
- **Rede de administração para StorageGRID**: A rede de administração é uma rede fechada usada para administração e manutenção do sistema. A rede Admin é normalmente uma rede privada e não precisa ser roteável entre sites. A rede de administração é opcional.
- **Rede do cliente para StorageGRID**: A rede do cliente é uma rede aberta usada para fornecer acesso a aplicações do cliente, incluindo S3 e Swift. A rede do cliente fornece acesso ao protocolo do cliente à grade, de modo que a rede da grade possa ser isolada e protegida. A rede do cliente é opcional.
- **Rede de gerenciamento para SANtricity Storage Manager**: O controlador E2700 se coneta à rede de gerenciamento onde o SANtricity Storage Manager está instalado, permitindo que você monitore e gerencie os componentes de hardware do dispositivo. Essa rede de gerenciamento pode ser a mesma rede de administração para StorageGRID ou pode ser uma rede de gerenciamento independente.

Para obter informações detalhadas sobre redes StorageGRID, consulte *Primer*.

Conexões de dispositivos StorageGRID

Ao instalar um dispositivo StorageGRID, você deve conetar os dois controladores entre si e às redes necessárias. A figura mostra os dois controladores no SG5660, com o controlador E2700 na parte superior e o controlador E5600SG na parte inferior. No SG5612, o controlador E2700 está à esquerda do controlador E5600SG.



Item	Porta	Tipo de porta	Função
1	Porta de gerenciamento 1 no controlador E2700	Ethernet de 1 GB (RJ-45)	Liga o controlador E2700 à rede onde o SANtricity Storage Manager está instalado.
2	Porta de gerenciamento 2 no controlador E2700	Ethernet de 1 GB (RJ-45)	Liga o controlador E2700 a um computador portátil de serviço durante a instalação.
3	Duas portas de interconexão SAS em cada controlador, identificadas como Ch 1 e Ch 2	Controlador E2700: Mini-SAS-HD Controlador E5600SG: Mini-SAS	Conete os dois controladores um ao outro.

Item	Porta	Tipo de porta	Função
4	Porta de gerenciamento 1 no controlador E5600SG	Ethernet de 1 GB (RJ-45)	Liga o controlador E5600SG à rede de administração para StorageGRID.
5	Porta de gerenciamento 2 no controlador E5600SG	Ethernet de 1 GB (RJ-45)	• Pode ser ligado com a porta de gerenciamento 1 se você quiser uma conexão redundante com a rede de administração. • Pode ser deixado sem fios e disponível para acesso local temporário (IP 169.254.0.1). • Pode ser usado para conetar o controlador E5600SG a um laptop de serviço durante a instalação, se um endereço IP atribuído pelo DHCP não estiver disponível.
6	Quatro portas de rede no controlador E5600SG	10 GbE (ótico)	Conete-se à rede de grade e à rede de cliente para StorageGRID. Consulte ""conexões de porta de 10 GbE para o controlador E5600SG."

Informações relacionadas

"Modos de ligação de porta para as portas do controlador E5600SG"

"Recolha de informações de instalação (SG5600)"

"Cabeamento do aparelho (SG5600)"

"Diretrizes de rede"

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Modos de ligação de porta para as portas do controlador E5600SG

Ao configurar links de rede para as portas do controlador E5600SG, você pode usar a ligação de porta para as portas de 10 GbE que se conetam à rede de Grade e à rede cliente opcional e as portas de gerenciamento de 1 GbE que se conetam à rede de administração opcional. A ligação de portas ajuda a proteger os seus dados fornecendo caminhos redundantes entre as redes StorageGRID e o dispositivo.

Informações relacionadas

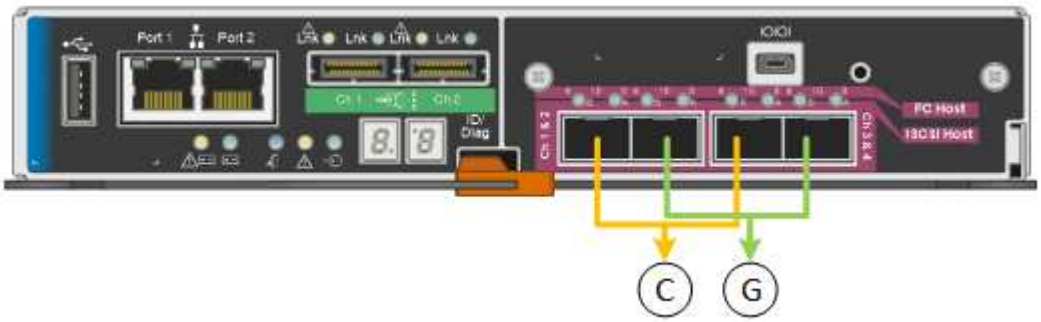
"Configurando links de rede (SG5600)"

Modos de ligação de rede para as portas de 10 GbE

As portas de rede de 10 GbE no controlador E5600SG suportam o modo de ligação de porta fixa ou o modo de ligação de porta agregada para as conexões de rede de Grade e rede de Cliente.

Modo de ligação de porta fixa

O modo fixo é a configuração padrão para as portas de rede de 10 GbE.



	Quais portas estão coladas
C	As portas 1 e 3 são Unidas para a rede do cliente, se esta rede for utilizada.
G	As portas 2 e 4 são Unidas para a rede de Grade.

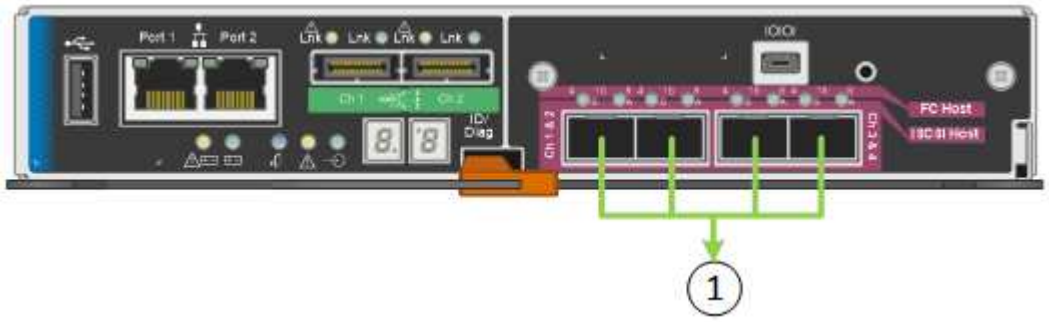
Ao usar o modo de ligação de porta fixa, as portas podem ser coladas usando o modo de backup ativo ou o modo de protocolo de controle de agregação de link (LACP 802,3ad).

- No modo de backup ativo (padrão), apenas uma porta está ativa por vez. Se a porta ativa falhar, sua porta de backup fornecerá automaticamente uma conexão de failover. A porta 4 fornece um caminho de backup para a porta 2 (rede de Grade) e a porta 3 fornece um caminho de backup para a porta 1 (rede de cliente).
- No modo LACP, cada par de portas forma um canal lógico entre o controlador e a rede, permitindo maior produtividade. Se uma porta falhar, a outra continua a fornecer o canal. A taxa de transferência é reduzida, mas a conetividade não é afetada.

Se não precisar de ligações redundantes, pode utilizar apenas uma porta para cada rede. No entanto, esteja ciente de que um alarme será gerado no Gerenciador de Grade após a instalação do StorageGRID, indicando que um cabo está desconetado. Pode reconhecer este alarme em segurança para o limpar.

Modo de ligação de porta agregada

O modo de ligação de porta agregada aumenta significativamente o em toda a rede StorageGRID e fornece caminhos de failover adicionais.



	Quais portas estão coladas
1	Todas as portas conetadas são agrupadas em uma única ligação LACP, permitindo que todas as portas sejam usadas para o tráfego de rede de Grade e rede de Cliente.

Se você planeja usar o modo de ligação de porta agregada:

- Você deve usar o modo de ligação de rede LACP.
- Você deve especificar uma tag VLAN exclusiva para cada rede. Essa tag VLAN será adicionada a cada pacote de rede para garantir que o tráfego de rede seja roteado para a rede correta.
- As portas devem ser conetadas a switches que possam suportar VLAN e LACP. Se vários switches estiverem participando da ligação LACP, os switches devem suportar grupos de agregação de links de vários gabinetes (MLAG) ou equivalente.
- Você deve entender como configurar os switches para usar VLAN, LACP e MLAG, ou equivalente.

Se você não quiser usar todas as quatro portas de 10 GbE, poderá usar uma, duas ou três portas. O uso de mais de uma porta maximiza a chance de que alguma conetividade de rede permaneça disponível se uma das portas de 10 GbE falhar.

Se você optar por usar menos de quatro portas, esteja ciente de que um ou mais alarmes serão levantados no Gerenciador de Grade após a instalação do StorageGRID, indicando que os cabos estão desconetados. Você pode reconhecer os alarmes com segurança para limpá-los.

Modos de ligação de rede para as portas de gerenciamento de 1 GbE

Para as duas portas de gerenciamento de 1 GbE no controlador E5600SG, você pode escolher o modo de ligação de rede independente ou o modo de ligação de rede ative-Backup para se conetar à rede Admin opcional.

No modo independente, apenas a porta de gerenciamento 1 está conetada à rede de administração. Este

modo não fornece um caminho redundante. A porta de gerenciamento 2 é deixada desconetada e disponível para conexões locais temporárias (use o endereço IP 169.254.0.1)

No modo ative-Backup, as portas de gerenciamento 1 e 2 estão conetadas à rede de administração. Apenas uma porta está ativa de cada vez. Se a porta ativa falhar, sua porta de backup fornecerá automaticamente uma conexão de failover. A ligação dessas duas portas físicas em uma porta de gerenciamento lógico fornece um caminho redundante para a rede de administração.

> Se você precisar fazer uma conexão local temporária ao controlador E5600SG quando as portas de gerenciamento de 1 GbE estiverem configuradas para o modo ative-Backup, remova os cabos de ambas as portas de gerenciamento, conete o cabo temporário à porta de gerenciamento 2 e acesse o dispositivo usando o endereço IP 169.254.0.1.

Recolha de informações de instalação (SG5600)

À medida que você instala e configura o dispositivo StorageGRID, você deve tomar decisões e coletar informações sobre portas de switch Ethernet, endereços IP e modos de ligação de porta e rede.

Sobre esta tarefa

Você pode usar as tabelas a seguir para gravar informações de cada rede conetada ao aparelho. Esses valores são necessários para instalar e configurar o hardware.

Informações necessárias para conetar o controlador E2700 ao SANtricity Storage Manager

Tem de ligar o controlador E2700 à rede de gestão que irá utilizar para o SANtricity Storage Manager.

Informações necessárias	O seu valor
Porta do switch Ethernet, você se conetará à porta de gerenciamento 1	
Endereço MAC da porta de gerenciamento 1 (impresso em uma etiqueta próxima à porta P1)	
Endereço IP atribuído pelo DHCP para a porta de gerenciamento 1, se disponível após a ativação **Observação:** se a rede que você se conetará ao controlador E2700 incluir um servidor DHCP, o administrador da rede poderá usar o endereço MAC para determinar o endereço IP atribuído pelo servidor DHCP.	

Informações necessárias	O seu valor
Velocidade e modo duplex **Nota:** você deve certificar-se de que o switch Ethernet para a rede de gerenciamento SANtricity Storage Manager está definido como negociação automática.	Deve ser: • Negociação automática (padrão)
Formato do endereço IP	Escolha uma: • IPv4 • IPv6
Endereço IP estático que pretende utilizar para o dispositivo na rede de gestão	Para IPv4: • Endereço IPv4: • Máscara de sub-rede: • Gateway: Para IPv6: • Endereço IPv6: • Endereço IP roteável: • Endereço IP do router do controlador E2700:

Informações necessárias para conetar o controlador E5600SG à rede de administração

A rede de administração para StorageGRID é uma rede opcional, usada para administração e manutenção do sistema. O dispositivo se coneta à rede Admin usando as portas de gerenciamento de 1 GbE no controlador E5600SG.

Informações necessárias	O seu valor
Rede de administração ativada	Escolha uma: • Não • Sim (predefinição)
Modo de ligação de rede	Escolha uma: • Independente • Ative-Backup
Porta do switch para a porta de gerenciamento 1 (P1)	
Porta do switch para a porta de gerenciamento 2 (P2; apenas modo de ligação de rede ative-Backup)	

Informações necessárias	O seu valor
Endereço MAC da porta de gerenciamento 1 (impresso em uma etiqueta próxima à porta P1)	
Endereço IP atribuído pelo DHCP para a porta de gerenciamento 1, se disponível após a ativação **Observação:** se a rede Admin incluir um servidor DHCP, o controlador E5600SG exibirá o endereço IP atribuído pelo DHCP em sua tela de sete segmentos depois que ele for inicializado. Você também pode determinar o endereço IP atribuído pelo DHCP usando o endereço MAC para procurar o IP atribuído.	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede de administração **Nota:** se a rede não tiver um gateway, especifique o mesmo endereço IPv4 estático para o gateway.	• Endereço IPv4 (CIDR): • Gateway:
Sub-redes de rede Admin (CIDR)	

Informações necessárias para conetar e configurar as portas de 10 GbE no controlador E5600SG

As quatro portas de 10 GbE no controlador E5600SG conetam-se à rede de Grade StorageGRID e à rede de Cliente.

Consulte "conexões de portas de 10 GbE para o controlador E5600SG" para obter mais informações sobre as opções dessas portas.

Informações necessárias	O seu valor
Modo de ligação da porta	Escolha uma: • Fixo (padrão) • Agregado
Porta do switch para a porta 1 (rede do cliente para o modo fixo)	
Porta do switch para a porta 2 (rede de grade para modo fixo)	
Porta do switch para a porta 3 (rede do cliente para o modo fixo)	

Informações necessárias	O seu valor
Porta do switch para a porta 4 (rede de grade para modo fixo)	

Informações necessárias para conetar o controlador E5600SG à rede de Grade

A rede de Grade para StorageGRID é uma rede necessária, usada para todo o tráfego interno de StorageGRID. O dispositivo se coneta à rede de Grade usando as portas de 10 GbE no controlador E5600SG.

Consulte "conexões de portas de 10 GbE para o controlador E5600SG" para obter mais informações sobre as opções dessas portas.

Informações necessárias	O seu valor
Modo de ligação de rede	Escolha uma: • Ative-Backup (padrão) • Bola de Futsal (802,3ad)
Marcação de VLAN ativada	Escolha uma: • Não (predefinição) • Sim
Tag VLAN (se a marcação VLAN estiver ativada)	Introduza um valor entre 0 e 4095:
Endereço IP atribuído pelo DHCP para a rede de Grade, se disponível após a ativação **Observação:** se a rede de Grade incluir um servidor DHCP, o controlador E5600SG exibirá o endereço IP atribuído pelo DHCP para a rede de Grade em sua tela de sete segmentos após a inicialização.	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede de grelha **Nota:** se a rede não tiver um gateway, especifique o mesmo endereço IPv4 estático para o gateway.	• Endereço IPv4 (CIDR): • Gateway:
Sub-redes de rede de rede (CIDR) **Nota:** se a rede do cliente não estiver ativada, a rota padrão no controlador usará o gateway especificado aqui.	

Informações necessárias para conetar o controlador E5600SG à rede do cliente

A rede de cliente para StorageGRID é uma rede opcional, usada para fornecer acesso ao protocolo de cliente à grade. O dispositivo se coneta à rede do cliente usando as portas de 10 GbE no controlador E5600SG.

Consulte "conexões de portas de 10 GbE para o controlador E5600SG" para obter mais informações sobre as opções dessas portas.

Informações necessárias	O seu valor
Rede cliente ativada	Escolha uma: • Não (predefinição) • Sim
Modo de ligação de rede	Escolha uma: • Ative-Backup (padrão) • Bola de Futsal (802,3ad)
Marcação de VLAN ativada	Escolha uma: • Não (predefinição) • Sim
Tag VLAN (se a marcação VLAN estiver ativada)	Introduza um valor entre 0 e 4095:
Endereço IP atribuído pelo DHCP para a rede do cliente, se disponível após a ligação	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de armazenamento do dispositivo na rede do cliente **Nota:** se a rede do cliente estiver ativada, a rota padrão no controlador usará o gateway especificado aqui.	• Endereço IPv4 (CIDR): • Gateway:

Informações relacionadas

"Rever as ligações de rede do dispositivo"

"Configurar o hardware"

"Modos de ligação de porta para as portas do controlador E5600SG"

Instalar o hardware

A instalação de hardware inclui várias tarefas importantes, incluindo a instalação de componentes de hardware, o cabeamento desses componentes e a configuração de portas.

Passos

- "Registar o hardware"
- "Instalar o aparelho em um gabinete ou rack (SG5600)"
- "Cabeamento do aparelho (SG5600)"
- "Ligar os cabos de alimentação CA (SG5600)"
- "Ligar a alimentação (SG5600)"
- "Visualização do status de inicialização e revisão dos códigos de erro nos controladores SG5600"

Registar o hardware

Registrar o hardware do aparelho fornece benefícios de suporte.

Passos

1. Localize o número de série do chassi.

   Pode encontrar o número no folheto de embalagem, no seu e-mail de confirmação ou no aparelho depois de o desembalar.

2. Vá para o site de suporte da NetApp em "mysupport.NetApp.com".
3. Determine se você precisa Registrar o hardware:

Se você é um…	Siga estes passos…
Cliente NetApp existente	a. Inicie sessão com o seu nome de utilizador e palavra-passe. b. Selecione **Produtos Meus Produtos**. c. Confirme se o novo número de série está listado. d. Se não estiver, siga as instruções para novos clientes NetApp.
Novo cliente da NetApp	a. Clique em **Registe-se agora** e crie uma conta. b. Selecione **Produtos Registe produtos**. c. Insira o número de série do produto e os detalhes solicitados. Após a aprovação do seu registo, pode transferir qualquer software necessário. O processo de aprovação pode demorar até 24 horas.

Instalar o aparelho em um gabinete ou rack (SG5600)

Tem de instalar calhas no armário ou no rack e, em seguida, deslizar o aparelho sobre os

trilhos. Se você tiver um SG5660, você também deve instalar as unidades depois de instalar o aparelho.

O que você vai precisar

- Você revisou o documento de Avisos de segurança incluído na caixa e entendeu as precauções para mover e instalar hardware.
- Você tem as instruções de instalação do e-Series para o hardware.

> Instale o hardware a partir da parte inferior do rack ou gabinete ou rack para cima para evitar que o equipamento tombe.

> O SG5612 pesa aproximadamente 60 lb (27 kg) quando totalmente carregado com unidades. Duas pessoas ou um elevador mecanizado são necessários para mover com segurança o SG5612.

> O SG5660 pesa aproximadamente 132 lb (60 kg) sem unidades instaladas. Quatro pessoas ou um elevador mecanizado são necessários para mover com segurança um SG5660 vazio.

> Para evitar danificar o hardware, nunca mova um SG5660 se as unidades estiverem instaladas. Deve remover todas as unidades antes de mover o aparelho.

Sobre esta tarefa

Execute as seguintes tarefas para instalar o dispositivo SG5660 em um gabinete ou rack.

- **Instale os trilhos de montagem**

  Instale os trilhos de montagem no gabinete ou rack.

  Consulte as instruções de instalação do e-Series para o E2700 ou o E5600.

- **Instale o aparelho no gabinete ou rack**

  Deslize o aparelho para dentro do gabinete ou rack e fixe-o.

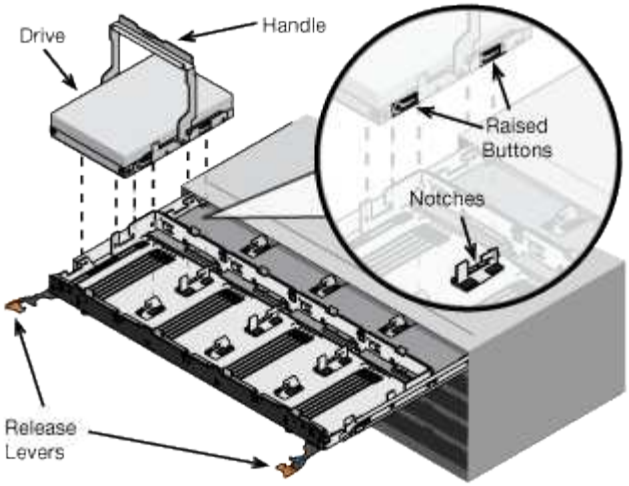
  > Se estiver a levantar o SG5660 manualmente, fixe as quatro pegas nas laterais do chassis. Retire estas pegas enquanto desliza o aparelho sobre os trilhos.

- **Instale as unidades**

  Se você tiver um SG5660, instale 12 unidades em cada uma das 5 gavetas de unidade.

  Você deve instalar todas as unidades 60 para garantir o funcionamento correto.

  a. Coloque a pulseira ESD e remova as unidades da embalagem.
  b. Solte as alavancas na gaveta superior da unidade e deslize a gaveta para fora usando as alavancas.
  c. Levante a alça da unidade para a vertical e alinhe os botões da unidade com os entalhes na gaveta.



d. Pressionando suavemente a parte superior da unidade, gire a alça da unidade para baixo até que ela se encaixe no lugar.

e. Depois de instalar as primeiras 12 unidades, deslize a gaveta para dentro, empurrando o centro e fechando ambas as alavancas com cuidado.

f. Repita estes passos para as outras quatro gavetas.

- **Fixe a moldura frontal**

  SG5612: Fixe as tampas das extremidades esquerda e direita à frente.

  SG5660: Fixe a moldura à frente.

Informações relacionadas

"E2700 Guia de instalação da bandeja de unidades e controlador relacionado"

"E5600 Guia de instalação da bandeja de unidades e controlador relacionado"

Cabeamento do aparelho (SG5600)

Você deve conetar os dois controladores entre si com cabos de interconexão SAS, conetar as portas de gerenciamento à rede de gerenciamento apropriada e conetar as portas de 10 GbE do controlador E5600SG à rede de grade e à rede de cliente opcional para StorageGRID.

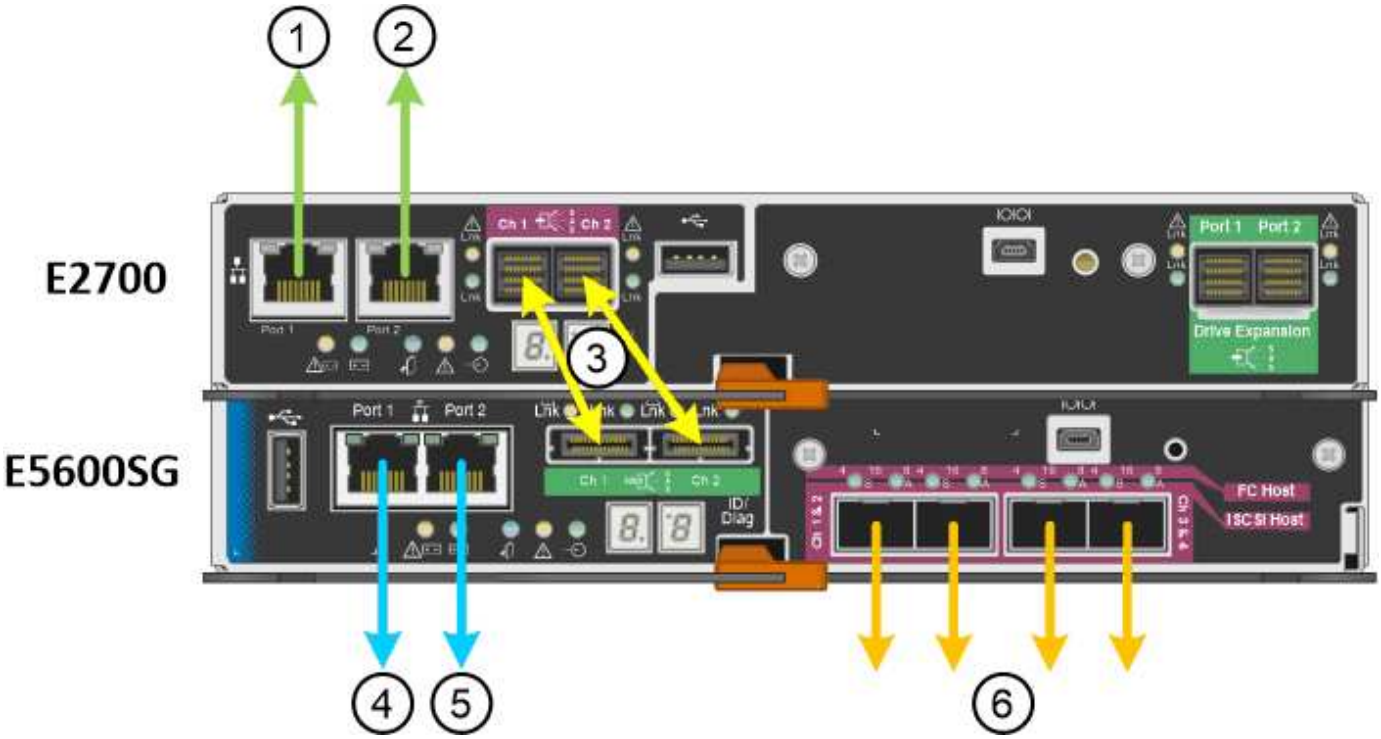
O que você vai precisar

- Você tem cabos Ethernet para conetar as portas de gerenciamento.
- Você tem cabos óticos para conetar as quatro portas de 10 GbE (elas não são fornecidas com o dispositivo).

Risco de exposição à radiação laser — não desmonte nem remova qualquer parte de um transcetor SFP. Você pode estar exposto à radiação laser.

Sobre esta tarefa

Ao conetar os cabos, consulte o diagrama a seguir, que mostra o controlador E2700 na parte superior e o controlador E5600SG na parte inferior. O diagrama mostra o modelo SG5660D; os controladores no modelo SG5612D estão lado a lado em vez de empilhados.



Item	Porta	Tipo de porta	Função
1	Porta de gerenciamento 1 no controlador E2700	Ethernet de 1 GB (RJ-45)	Liga o controlador E2700 à rede onde o SANtricity Storage Manager está instalado.
2	Porta de gerenciamento 2 no controlador E2700	Ethernet de 1 GB (RJ-45)	Liga o controlador E2700 a um computador portátil de serviço durante a instalação.
3	Duas portas de interconexão SAS em cada controlador, identificadas como Ch 1 e Ch 2	Controlador E2700: Mini-SAS-HD Controlador E5600SG: Mini-SAS	Conete os dois controladores um ao outro.
4	Porta de gerenciamento 1 no controlador E5600SG	Ethernet de 1 GB (RJ-45)	Liga o controlador E5600SG à rede de administração para StorageGRID.

Item	Porta	Tipo de porta	Função
5	Porta de gerenciamento 2 no controlador E5600SG	Ethernet de 1 GB (RJ-45)	• Pode ser ligado com a porta de gerenciamento 1 se você quiser uma conexão redundante com a rede de administração. • Pode ser deixado sem fios e disponível para acesso local temporário (IP 169.254.0.1). • Pode ser usado para conetar o controlador E5600SG a um laptop de serviço durante a instalação se os endereços IP atribuídos pelo DHCP não estiverem disponíveis.
6	Quatro portas de rede no controlador E5600SG	10 GbE (ótico)	Ligue o controlador E5600SG à rede de grelha e à rede de cliente (se utilizada) para o StorageGRID. As portas podem ser Unidas para fornecer caminhos redundantes para o controlador.

Passos

1. Conete o controlador E2700 ao controlador E5600SG usando os dois cabos de interconexão SAS.

Ligar esta porta…	Para este porto…
Porta de interconexão SAS 1 (identificada como Ch 1) no controlador E2700	Porta de interconexão SAS 1 (identificada como Ch 1) no controlador E5600SG
Porta de interconexão SAS 2 (identificada como Ch 2) no controlador E2700	Porta de interconexão SAS 2 (identificada como Ch 2) no controlador E5600SG

Use o conetor quadrado (mini-SAS HD) para o controlador E2700 e use o conetor retangular (mini-SAS) para o controlador E5600SG.

Certifique-se de que as patilhas de puxar nos conetores SAS estão na parte inferior e insira cuidadosamente cada conetor até encaixar no lugar. Não pressione o conetor se houver resistência. Verifique a posição da patilha de puxar antes de continuar.

2. Conete o controlador E2700 à rede de gerenciamento em que o software SANtricity Storage Manager está instalado, usando um cabo Ethernet.

Ligar esta porta…	Para este porto…
Porta 1 no controlador E2700 (a porta RJ-45 à esquerda)	Porta do switch na rede de gerenciamento usada para o SANtricity Storage Manager
Porta 2 no controlador E2700	Computador portátil de serviço, se não estiver a utilizar DHCP

3. Se pretender utilizar a rede de administração para StorageGRID, ligue o controlador E5600SG utilizando um cabo Ethernet.

Ligar esta porta…	Para este porto…
Porta 1 no controlador E5600SG (a porta RJ-45 à esquerda)	Switch port on the Admin Network for StorageGRID
Porta 2 no controlador E5600SG	Computador portátil de serviço, se não estiver a utilizar DHCP

4. Conete as portas de 10 GbE no controlador E5600SG aos switches de rede apropriados, usando cabos óticos e transcetores SFP.
   - Se você planeja usar o modo de ligação de porta fixa (padrão), conete as portas à rede StorageGRID e às redes de clientes, conforme mostrado na tabela.

Porta	Liga a…
Porta 1	Rede cliente (opcional)
Porta 2	Rede de rede
Porta 3	Rede cliente (opcional)
Porta 4	Rede de rede

   - Se você planeja usar o modo de ligação de porta agregada, conete uma ou mais portas de rede a um ou mais switches. Você deve conetar pelo menos duas das quatro portas para evitar ter um único ponto de falha. Se você usar mais de um switch para uma única ligação LACP, os switches devem suportar MLAG ou equivalente.

Informações relacionadas

"Modos de ligação de porta para as portas do controlador E5600SG"

"Acessando o instalador do StorageGRID Appliance"

Ligar os cabos de alimentação CA (SG5600)

É necessário conetar os cabos de alimentação CA à fonte de alimentação externa e ao conetor de alimentação CA em cada controlador. Depois de conetar os cabos de energia, você pode ligar a energia.

O que você vai precisar

Ambos os interrutores de alimentação do aparelho devem estar desligados antes de ligar a alimentação.

Risco de choque elétrico — antes de ligar os cabos de alimentação, certifique-se de que os dois interrutores de alimentação do aparelho estão desligados.

Sobre esta tarefa

- Você deve usar fontes de alimentação separadas para cada fonte de alimentação.

  A ligação a fontes de alimentação independentes mantém a redundância de energia.

- Você pode usar os cabos de alimentação enviados com o controlador com tomadas típicas usadas no país de destino, como tomadas de parede de uma fonte de alimentação ininterrupta (UPS).

  No entanto, esses cabos de alimentação não se destinam a ser usados na maioria dos gabinetes compatíveis com EIA.

Passos

1. Desligue os interruptores de energia no gabinete ou chassi.
2. Desligue os interrutores de alimentação dos controladores.
3. Conete os cabos de alimentação primários do gabinete às fontes de alimentação externas.
4. Conete os cabos de alimentação ao conetor de alimentação CA em cada controlador.

Ligar a alimentação (SG5600)

A ativação do gabinete fornece energia a ambos os controladores.

Passos

1. Ligue os dois interrutores da fonte de alimentação na parte traseira do compartimento.

   Enquanto a energia está sendo aplicada, os LEDs nos controladores acendem e apagam intermitentemente.

   O processo de ativação pode levar até dez minutos para ser concluído. Os controladores reiniciam várias vezes durante a sequência inicial de inicialização, o que faz com que os ventiladores aumentem e diminuam e os LEDs pisquem.

2. Verifique o LED de alimentação e os LEDs ativos do Host Link em cada controlador para verificar se a alimentação foi ligada.
3. Aguarde que todas as unidades mostrem um LED verde persistente, indicando que elas estão online.
4. Verifique se existem LEDs verdes na parte frontal e traseira do compartimento.

Se vir algum LED âmbar, anote as suas localizações.

5. Observe o visor de sete segmentos para o controlador E5600SG.

   Este visor mostra **HO**, seguido de uma sequência de repetição de dois dígitos.

   ```
   HO -- IP address for Admin Network -- IP address for Grid Network HO
   ```

   Na sequência, o primeiro conjunto de números é o endereço IP atribuído pelo DHCP para a porta de gerenciamento 1 do controlador. Este endereço é utilizado para ligar o controlador à rede de administração para StorageGRID. O segundo conjunto de números é o endereço IP atribuído pelo DHCP utilizado para ligar o dispositivo à rede de grelha para StorageGRID.

   Se um endereço IP não puder ser atribuído usando DHCP, 0.0.0.0 será exibido.

Visualização do status de inicialização e revisão dos códigos de erro nos controladores SG5600

O visor de sete segmentos em cada controlador mostra os códigos de estado e de erro quando o dispositivo liga, enquanto o hardware está a ser inicializado, e quando o hardware falha e tem de ser retirado da inicialização. Se estiver a monitorizar o progresso ou a resolução de problemas, deve observar a sequência dos códigos à medida que estes aparecem.

Sobre esta tarefa

Os códigos de status e erro do controlador E5600SG não são os mesmos do controlador E2700.

Passos

1. Durante a inicialização, veja os códigos mostrados nas telas de sete segmentos para monitorar o progresso.
2. Para rever os códigos de erro do controlador E5600SG, consulte as informações de status e código de erro do visor de sete segmentos.
3. Para revisar os códigos de erro do controlador E2700, consulte a documentação do controlador E2700 no site de suporte.

Informações relacionadas

"E5600SG códigos de exibição de sete segmentos do controlador"

"Documentação do NetApp: Série E2700"

E5600SG códigos de exibição de sete segmentos do controlador

O visor de sete segmentos no controlador E5600SG mostra os códigos de estado e de erro enquanto o aparelho liga e enquanto o hardware está a ser inicializado. Você pode usar esses códigos para determinar o status e solucionar erros.

Ao analisar os códigos de status e de erro no controlador E5600SG, você deve observar os seguintes tipos de códigos:

- **Códigos gerais de inicialização**

Representar os eventos de inicialização padrão.

- **Códigos de inicialização normais**

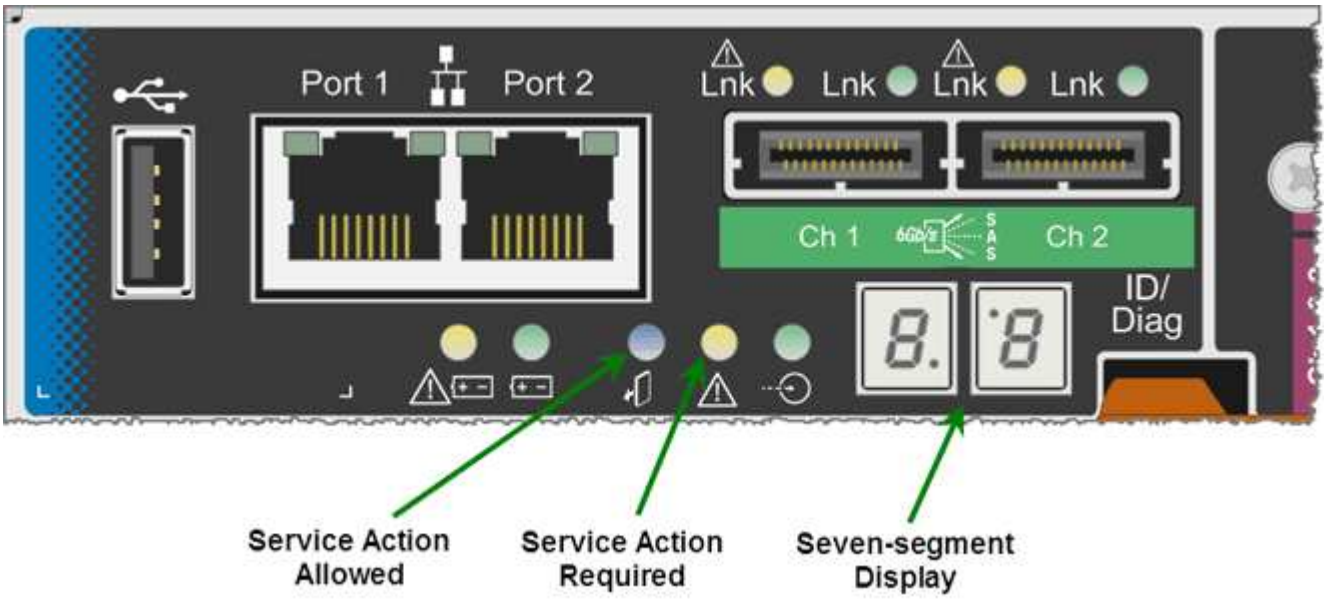
  Representa os eventos normais de arranque que ocorrem no aparelho.

- **Códigos de erro**

  Indique problemas durante os eventos de inicialização.

O StorageGRID controla apenas os seguintes LEDs no controlador E5600SG e apenas depois de o Instalador de dispositivos StorageGRID ter iniciado:

- LED Ação de Serviço permitida
- LED de ação de assistência necessária
- Visor de sete segmentos



Os pontos decimais no visor de sete segmentos não são utilizados pelo dispositivo StorageGRID:

- O ponto decimal superior adjacente ao dígito menos significativo é o LED de diagnóstico da plataforma.

  Isso é ativado durante a reinicialização e a configuração inicial do hardware. Caso contrário, ele é desligado.

- O ponto decimal inferior adjacente ao dígito mais significativo é desligado.

Para diagnosticar outros problemas, você pode querer olhar para estes recursos:

- Para ver todas as outras informações de diagnóstico ambiental e de hardware, consulte o diagnóstico de hardware do sistema operacional e-Series.

  Isso inclui a busca de problemas de hardware, como energia, temperatura e unidades de disco. O dispositivo depende do sistema operacional e-Series para monitorar todos os status ambientais da plataforma.

- Para determinar problemas de firmware e driver, observe as luzes de link nas portas SAS e de rede.

  Para obter detalhes, consulte a documentação do e-Series E5600.

Códigos gerais de arranque

Durante a inicialização ou após uma reinicialização total do hardware, os LEDs Ação de Serviço permitida e Ação de Serviço necessária acendem-se enquanto o hardware está sendo inicializado. O visor de sete segmentos mostra uma sequência de códigos iguais para o hardware e-Series e não específicos para o controlador E5600SG.

Durante a inicialização, o Field Programmable Gate Array (FPGA) controla as funções e a inicialização do hardware.

Código	Indicação
19	Inicialização do FPGA.
68	Inicialização do FPGA.
…	Inicialização FPGA. Esta é uma rápida sucessão de códigos.
AA	Inicialização do BIOS da plataforma.
FF	Inicialização do BIOS concluída. Este é um estado intermediário antes do controlador E5600SG inicializar e gerenciar LEDs para indicar o status.

Depois que os códigos AA e FF aparecem, os códigos de inicialização normais aparecem ou os códigos de erro aparecem. Além disso, os LEDs Ação de Serviço permitida e Ação de Serviço necessária estão desligados.

Códigos de arranque normais

Estes códigos representam os eventos normais de arranque que ocorrem no aparelho, por ordem cronológica.

Código	Indicação
OLÁ	O script de inicialização mestre foi iniciado.
DE PP	O firmware da plataforma FPGA está verificando se há atualizações.
HP	A placa de interface do host (HIC) está verificando se há atualizações.
RB	Após atualizações de firmware, o sistema está reiniciando, se necessário.

Código	Indicação
FP	As verificações de atualização de firmware foram concluídas. Iniciar o processo (utmagent) para se comunicar e gerenciar o controlador E2700. Esse processo facilita o provisionamento de dispositivos.
ELE	O sistema está sincronizando com o sistema operacional e-Series.
HC	A instalação do StorageGRID está sendo verificada.
HO	O gerenciamento da instalação e a interface ativa estão ocorrendo.
HA	O sistema operacional Linux e o StorageGRID estão em execução.

E5600SG códigos de erro do controlador

Estes códigos representam condições de erro que podem ser apresentadas no controlador E5600SG à medida que o aparelho arranca. Códigos hexadecimais de dois dígitos adicionais são exibidos se ocorrerem erros específicos de hardware de baixo nível. Se algum destes códigos persistir durante mais de um segundo ou dois, ou se não conseguir resolver o erro seguindo um dos procedimentos de resolução de problemas prescritos, contacte o suporte técnico.

Código	Indicação
22	Nenhum Registro mestre de inicialização encontrado em qualquer dispositivo de inicialização.
23	Nenhuma unidade SATA instalada.
2A, 2B	Barramento preso, não é possível ler dados SPD do DIMM.
40	DIMMs inválidos.
41	DIMMs inválidos.
42	Falha no teste de memória.
51	Falha na leitura de SPD.
92 a 96	Inicialização do barramento PCI.
A0 a A3	Inicialização da unidade SATA.

Código	Indicação
AB	Código de inicialização alternativo.
AE	A arrancar o SO.
EA	DDR3 a formação falhou.
E8	Nenhuma memória instalada.
UE	O script de instalação não foi encontrado.
EP	O código "ManageSGA" indica que a comunicação pré-grid com o controlador E2700 falhou.

Informações relacionadas

"Solução de problemas da instalação do hardware"

"Suporte à NetApp"

Configurar o hardware

Depois de aplicar energia ao dispositivo, você deve configurar o SANtricity Storage Manager, que é o software que você usará para monitorar o hardware. Você também deve configurar as conexões de rede que serão usadas pelo StorageGRID.

Passos

- "Configurando conexões StorageGRID"
- "Configurando o SANtricity Storage Manager"
- "Opcional: Habilitando a criptografia de nó"
- "Opcional: Mudar para o modo RAID6 (apenas SG5660)"
- "Opcional: Remapeamento de portas de rede para o dispositivo"

Configurando conexões StorageGRID

Antes de implantar um dispositivo StorageGRID como nó de armazenamento em uma grade StorageGRID, você deve configurar as conexões entre o dispositivo e as redes que você planeja usar. Você pode configurar a rede navegando até o Instalador de dispositivos StorageGRID, que está incluído no controlador E5600SG (o controlador de computação no dispositivo).

Passos

- "Acessando o instalador do StorageGRID Appliance"
- "Verificando e atualizando a versão do Instalador de dispositivos StorageGRID"
- "Configurando links de rede (SG5600)"

- "Definir a configuração IP"
- "Verificando conexões de rede"
- "Verificando conexões de rede no nível da porta"

Acessando o instalador do StorageGRID Appliance

Você deve acessar o Instalador do StorageGRID Appliance para configurar as conexões entre o appliance e as três redes StorageGRID: A rede de grade, a rede de administração (opcional) e a rede de cliente (opcional).

O que você vai precisar

- Você está usando um navegador da Web compatível.
- O dispositivo está ligado a todas as redes StorageGRID que pretende utilizar.
- Você sabe o endereço IP, o gateway e a sub-rede do dispositivo nessas redes.
- Configurou os comutadores de rede que pretende utilizar.

Sobre esta tarefa

Ao acessar pela primeira vez o Instalador do StorageGRID Appliance, você pode usar o endereço IP atribuído pelo DHCP para a rede Admin (assumindo que o dispositivo esteja conetado à rede Admin) ou o endereço IP atribuído pelo DHCP para a rede de Grade. É preferível utilizar o endereço IP da rede de administração. Caso contrário, se você acessar o Instalador do StorageGRID Appliance usando o endereço DHCP da rede de Grade, poderá perder a conexão com o Instalador do StorageGRID Appliance ao alterar as configurações de link e ao inserir um IP estático.

Passos

1. Obtenha o endereço DHCP do dispositivo na rede Admin (se estiver ligado) ou na rede Grid (se a rede Admin não estiver ligada).

   Você pode fazer um dos seguintes procedimentos:

   - Forneça o endereço MAC da porta de gerenciamento 1 ao administrador da rede, para que ele possa procurar o endereço DHCP dessa porta na rede de administração. O endereço MAC é impresso em uma etiqueta no controlador E5600SG, ao lado da porta.
   - Observe o visor de sete segmentos no controlador E5600SG. Se as portas de gerenciamento 1 e 10 GbE 2 e 4 no controlador E5600SG estiverem conetadas a redes com servidores DHCP, o controlador tentará obter endereços IP atribuídos dinamicamente ao ligar o gabinete. Depois que o controlador tiver concluído o processo de ativação, o visor de sete segmentos mostra **HO**, seguido de uma sequência repetida de dois números.

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     Na sequência:

     - O primeiro conjunto de números é o endereço DHCP para o nó de armazenamento do dispositivo na rede Admin, se estiver conetado. Este endereço IP é atribuído à porta de gerenciamento 1 no controlador E5600SG.
     - O segundo conjunto de números é o endereço DHCP para o nó de armazenamento do dispositivo na rede de Grade. Esse endereço IP é atribuído às portas 2 e 4 de 10 GbE quando você aplica

energia pela primeira vez ao dispositivo.

Se um endereço IP não puder ser atribuído usando DHCP, 0.0.0.0 será exibido.

2. Se você conseguiu obter um dos endereços DHCP:

   a. Abra um navegador da Web no laptop de serviço.

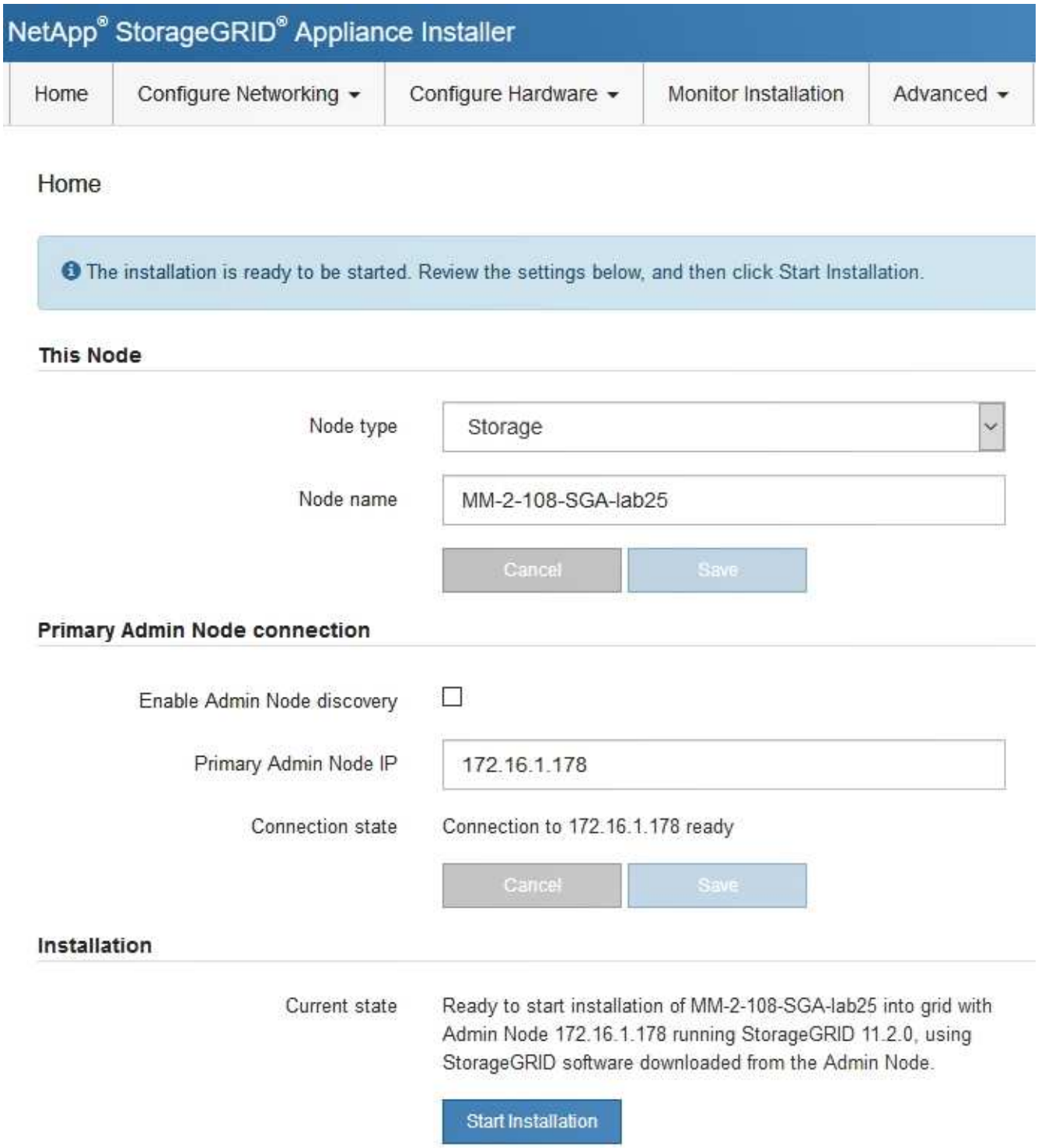
   b. Digite este URL para o instalador do StorageGRID Appliance
   `https://E5600SG_Controller_IP:8443`

   Para *`E5600SG_Controller_IP`*, utilize o endereço DHCP do controlador (utilize o endereço IP da rede de administração, se o tiver).

   c. Se for solicitado um alerta de segurança, exiba e instale o certificado usando o assistente de instalação do navegador.

   O alerta não aparecerá na próxima vez que você acessar este URL.

   A página inicial do instalador do dispositivo StorageGRID é exibida. As informações e as mensagens mostradas quando você acessa esta página pela primeira vez dependem de como o dispositivo está conetado atualmente às redes StorageGRID. Podem aparecer mensagens de erro que serão resolvidas em etapas posteriores.



3. Se o controlador E5600SG não conseguir adquirir um endereço IP utilizando DHCP:

   a. Conete o notebook de serviço à porta de gerenciamento 2 no controlador E5600SG, usando um cabo Ethernet.

b. Abra um navegador da Web no laptop de serviço.

c. Digite este URL para o instalador do StorageGRID Appliance
`https://169.254.0.1:8443`

A página inicial do instalador do dispositivo StorageGRID é exibida. As informações e as mensagens apresentadas quando acede pela primeira vez a esta página dependem da forma como o seu aparelho está atualmente ligado.

> ⓘ Se não conseguir aceder à página inicial através de uma ligação local, configure o endereço IP do computador portátil de serviço como `169.254.0.2`, e tente novamente.

4. Reveja as mensagens apresentadas na página inicial e configure a configuração da ligação e a configuração IP, conforme necessário.

Informações relacionadas

"Requisitos do navegador da Web"

Verificando e atualizando a versão do Instalador de dispositivos StorageGRID

A versão do Instalador de dispositivos StorageGRID no dispositivo deve corresponder à versão de software instalada no sistema StorageGRID para garantir que todos os recursos do StorageGRID sejam suportados.

O que você vai precisar

Você acessou o Instalador de dispositivos StorageGRID.

Os dispositivos StorageGRID vêm da fábrica pré-instalados com o Instalador de dispositivos StorageGRID. Se você estiver adicionando um dispositivo a um sistema StorageGRID atualizado recentemente, talvez seja necessário atualizar manualmente o Instalador de dispositivos StorageGRID antes de instalar o dispositivo como um novo nó.

O Instalador de dispositivos StorageGRID é atualizado automaticamente quando você atualiza para uma nova versão do StorageGRID. Não é necessário atualizar o Instalador de dispositivos StorageGRID nos nós de dispositivos instalados. Este procedimento só é necessário quando estiver a instalar um dispositivo que contenha uma versão anterior do Instalador de dispositivos StorageGRID.

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Avançado Atualização de firmware**.
2. Compare a versão atual do firmware com a versão de software instalada no seu sistema StorageGRID (no Gerenciador de Grade, selecione **Ajuda sobre**).

   O segundo dígito nas duas versões deve corresponder. Por exemplo, se o seu sistema StorageGRID estiver executando a versão 11.**5**.*x*.*y*, a versão do Instalador de dispositivos StorageGRID deve ser 3.**5**.*z*.

3. Se o aparelho tiver uma versão de nível inferior do instalador do dispositivo StorageGRID, vá para a

página de downloads do NetApp para StorageGRID.

"NetApp Downloads: StorageGRID"

Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.

4. Baixe a versão apropriada do arquivo **suporte para dispositivos StorageGRID** e o arquivo de checksum correspondente.

   O arquivo de suporte para dispositivos StorageGRID é um `.zip` arquivo que contém as versões de firmware atuais e anteriores para todos os modelos de dispositivos StorageGRID, em subdiretórios para cada tipo de controlador.

   Depois de baixar o arquivo de suporte para o arquivo de dispositivos StorageGRID, extraia o `.zip` arquivo e consulte o arquivo README para obter informações importantes sobre a instalação do Instalador de dispositivos StorageGRID.

5. Siga as instruções na página Atualizar firmware do Instalador de dispositivos StorageGRID para executar estas etapas:
   a. Carregue o ficheiro de suporte apropriado (imagem de firmware) para o seu tipo de controlador e o ficheiro de checksum.
   b. Atualize a partição inativa.
   c. Reinicie e troque partições.
   d. Atualize a segunda partição.

Informações relacionadas

"Acessando o instalador do StorageGRID Appliance"

Configurando links de rede (SG5600)

Você pode configurar links de rede para as portas usadas para conetar o dispositivo à rede de Grade, à rede de cliente e à rede de administração. Você pode definir a velocidade do link, bem como os modos de ligação de porta e rede.

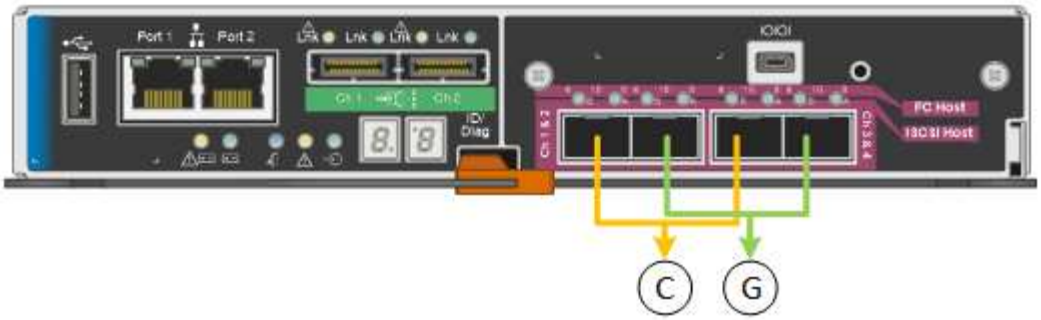
O que você vai precisar

Se você planeja usar o modo de ligação de porta agregada, o modo de ligação de rede LACP ou a marcação de VLAN:

- Você conetou as portas de 10 GbE no dispositivo a switches que podem suportar VLAN e LACP.
- Se vários switches estiverem participando da ligação LACP, os switches suportam grupos de agregação de links de vários gabinetes (MLAG) ou equivalente.
- Você entende como configurar os switches para usar VLAN, LACP e MLAG ou equivalente.
- Você conhece a tag VLAN exclusiva a ser usada para cada rede. Essa tag VLAN será adicionada a cada pacote de rede para garantir que o tráfego de rede seja roteado para a rede correta.

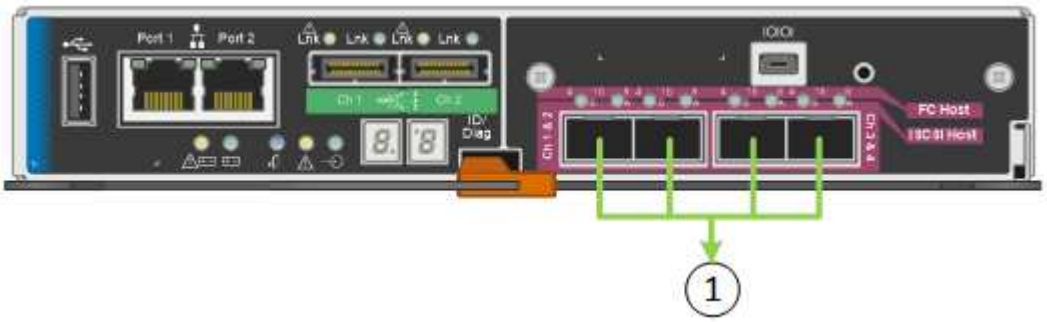
Sobre esta tarefa

Esta figura mostra como as quatro portas de 10 GbE são ligadas no modo de ligação de porta fixa (configuração padrão).



	Quais portas estão coladas
C	As portas 1 e 3 são Unidas para a rede do cliente, se esta rede for utilizada.
G	As portas 2 e 4 são Unidas para a rede de Grade.

Esta figura mostra como as quatro portas de 10 GbE são ligadas no modo de ligação de porta agregada.



	Quais portas estão coladas
1	Todas as quatro portas são agrupadas em uma única ligação LACP, permitindo que todas as portas sejam usadas para o tráfego de rede de Grade e rede de Cliente.

A tabela resume as opções de configuração das quatro portas de 10 GbE. Só é necessário configurar as definições na página Configuração de ligação se pretender utilizar uma definição não predefinida.

- **Modo de ligação de porta fixo (padrão)**

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Ative-Backup (padrão)	• As portas 2 e 4 usam uma ligação de backup ativo para a rede de Grade. • As portas 1 e 3 não são usadas. • Uma etiqueta VLAN é opcional.	• As portas 2 e 4 usam uma ligação de backup ativo para a rede de Grade. • As portas 1 e 3 usam uma ligação de backup ativo para a rede do cliente. • Tags VLAN podem ser especificadas para ambas as redes para a conveniência do administrador de rede.

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Bola de Futsal (802,3ad)	• As portas 2 e 4 usam uma ligação LACP para a rede de Grade. • As portas 1 e 3 não são usadas. • Uma etiqueta VLAN é opcional.	• As portas 2 e 4 usam uma ligação LACP para a rede de Grade. • As portas 1 e 3 usam uma ligação LACP para a rede de clientes. • Tags VLAN podem ser especificadas para ambas as redes para a conveniência do administrador de rede.

- **Modo de ligação de porta agregada**

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Apenas LACP (802,3ad)	• As portas 1-4 usam uma única ligação LACP para a rede de Grade. • Uma única etiqueta VLAN identifica pacotes de rede de Grade.	• As portas 1-4 usam uma única ligação LACP para a rede de Grade e a rede do Cliente. • Duas etiquetas VLAN permitem que os pacotes de rede de Grade sejam segregados dos pacotes de rede de Cliente.

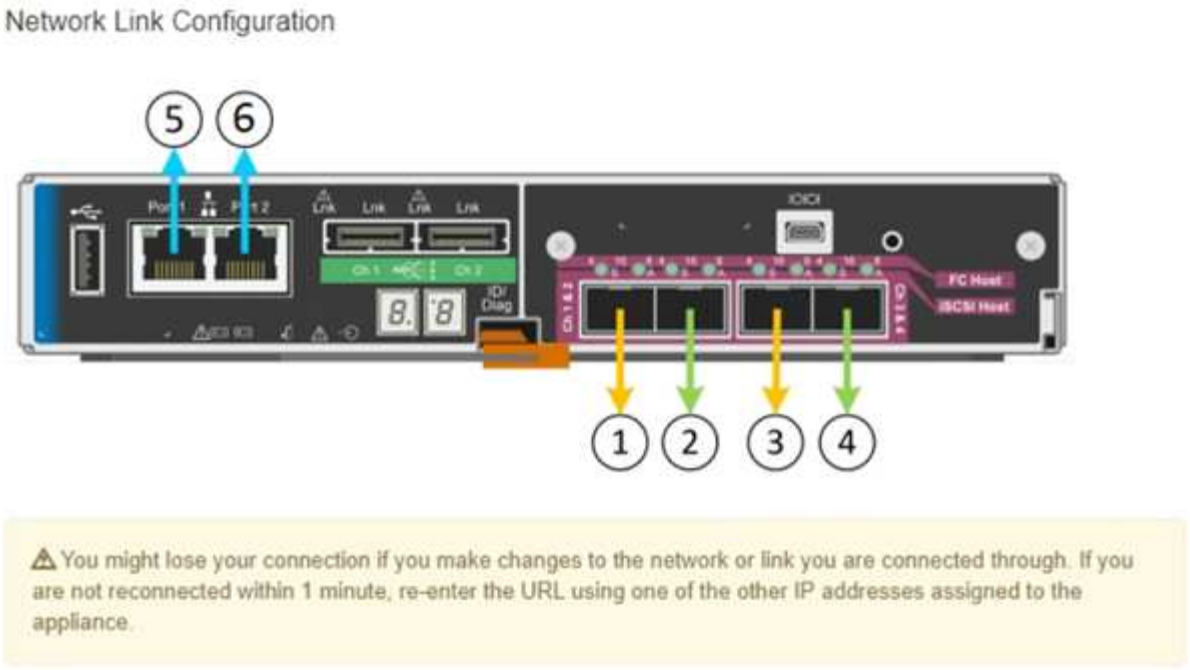
Consulte ""conexões de porta de 10 GbE para o controlador E5600SG" para obter mais informações sobre os modos de ligação de porta e ligação de rede.

Esta figura mostra como as duas portas de gerenciamento de 1 GbE na controladora E5600SG são ligadas no modo de ligação de rede ative-Backup para a rede Admin.

Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Configuração de ligação**.

   A página Network Link Configuration (Configuração da ligação de rede) apresenta um diagrama do seu dispositivo com as portas de rede e de gestão numeradas.



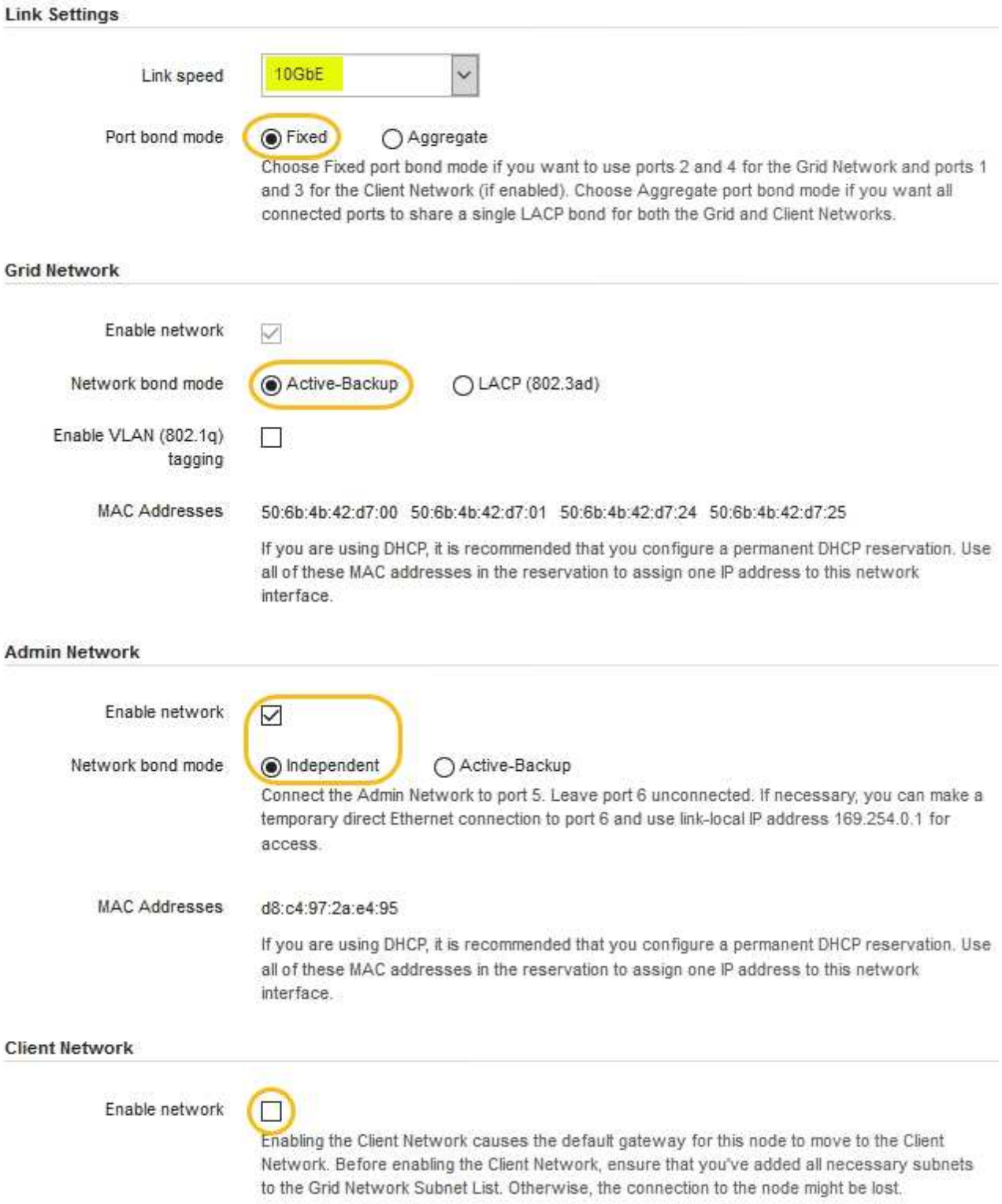
A tabela Status da ligação lista o estado da ligação (para cima/para baixo) e a velocidade (1/10/25/40/100 Gbps) das portas numeradas.

Link Status

Link	State	Speed (Gbps)
1	Down	N/A
2	Up	10
3	Up	10
4	Down	N/A
5	Up	1
6	Up	1

A primeira vez que aceder a esta página:

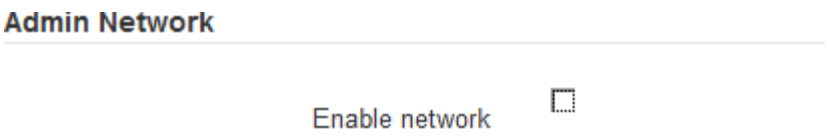
- **Link Speed** está definido para **10GbE**. Esta é a única velocidade de ligação disponível para o controlador E5600SG.
- **Port bond mode** está definido como **Fixed**.
- **O modo de ligação de rede** para a rede de Grade está definido como **ative-Backup**.
- A **Admin Network** está ativada e o modo de ligação de rede está definido como **Independent**.
- A **rede do cliente** está desativada.



2. Ative ou desative as redes StorageGRID que pretende utilizar.

   A rede de Grade é necessária. Não é possível desativar esta rede.

   a. Se o dispositivo não estiver conetado à rede Admin, desmarque a caixa de seleção **Ativar rede** para a rede Admin.



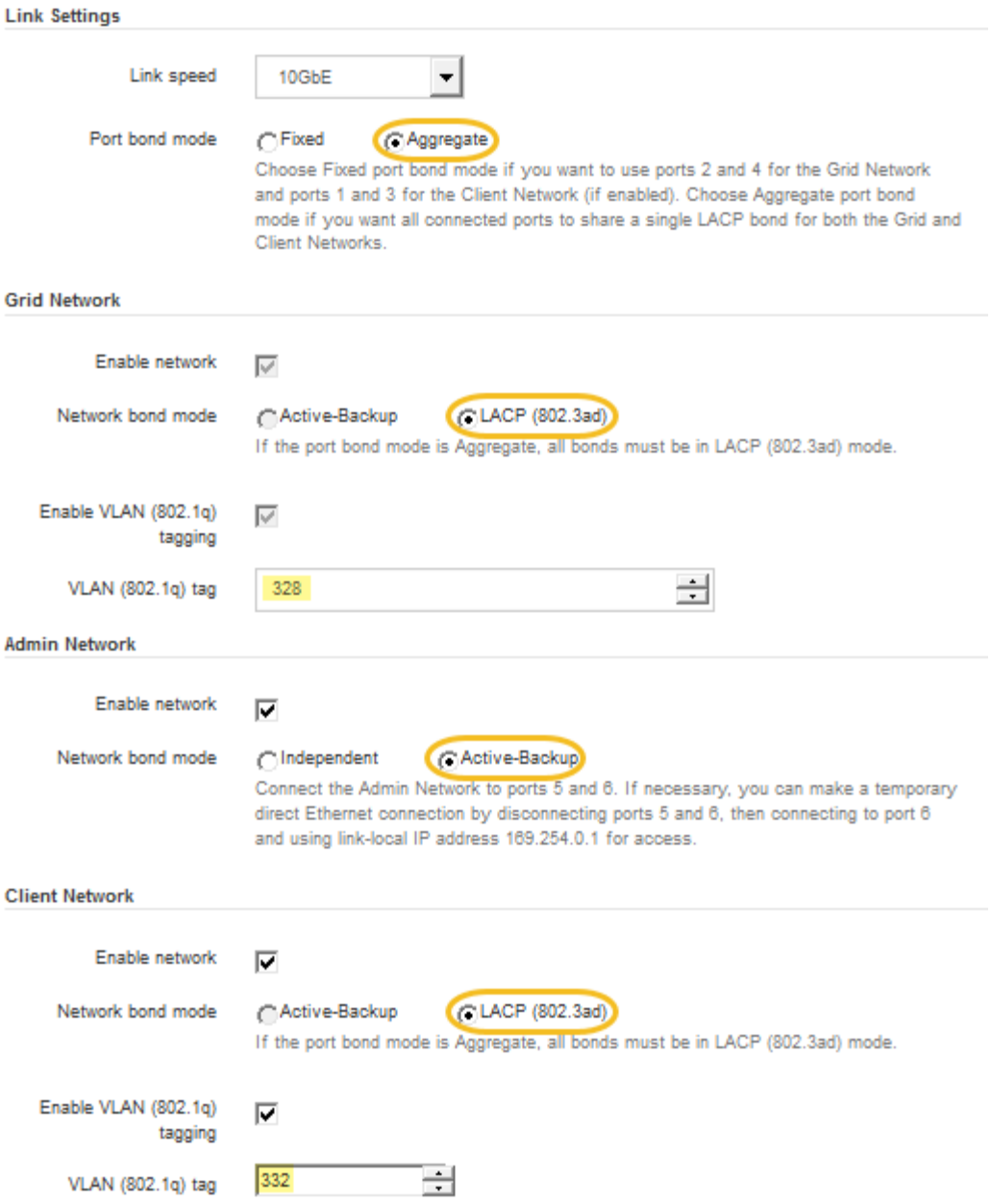
b. Se o dispositivo estiver conetado à rede do cliente, marque a caixa de seleção **Ativar rede** para a rede do cliente.

   As configurações de rede do cliente para as portas de 10 GbE são agora mostradas.

3. Consulte a tabela e configure o modo de ligação de porta e o modo de ligação de rede.

   O exemplo mostra:

   - **Aggregate** e **LACP** selecionados para as redes Grid e Client. Você deve especificar uma tag VLAN exclusiva para cada rede. Pode selecionar valores entre 0 e 4095.
   - **Ative-Backup** selecionado para a rede Admin.



4. Quando estiver satisfeito com suas seleções, clique em **Salvar**.

> Poderá perder a ligação se tiver efetuado alterações à rede ou à ligação através da qual está ligado. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do Instalador de appliance StorageGRID usando um dos outros endereços IP atribuídos ao appliance
> **`https://E5600SG_Controller_IP:8443`**

Informações relacionadas

"Modos de ligação de porta para as portas do controlador E5600SG"

Definir a configuração IP

Você usa o Instalador de dispositivos StorageGRID para configurar os endereços IP e as informações de roteamento usados para o nó de armazenamento de dispositivos nas

redes StorageGRID, Admin e cliente.

Sobre esta tarefa

Você deve atribuir um IP estático para o dispositivo em cada rede conetada ou atribuir uma concessão permanente para o endereço no servidor DHCP.

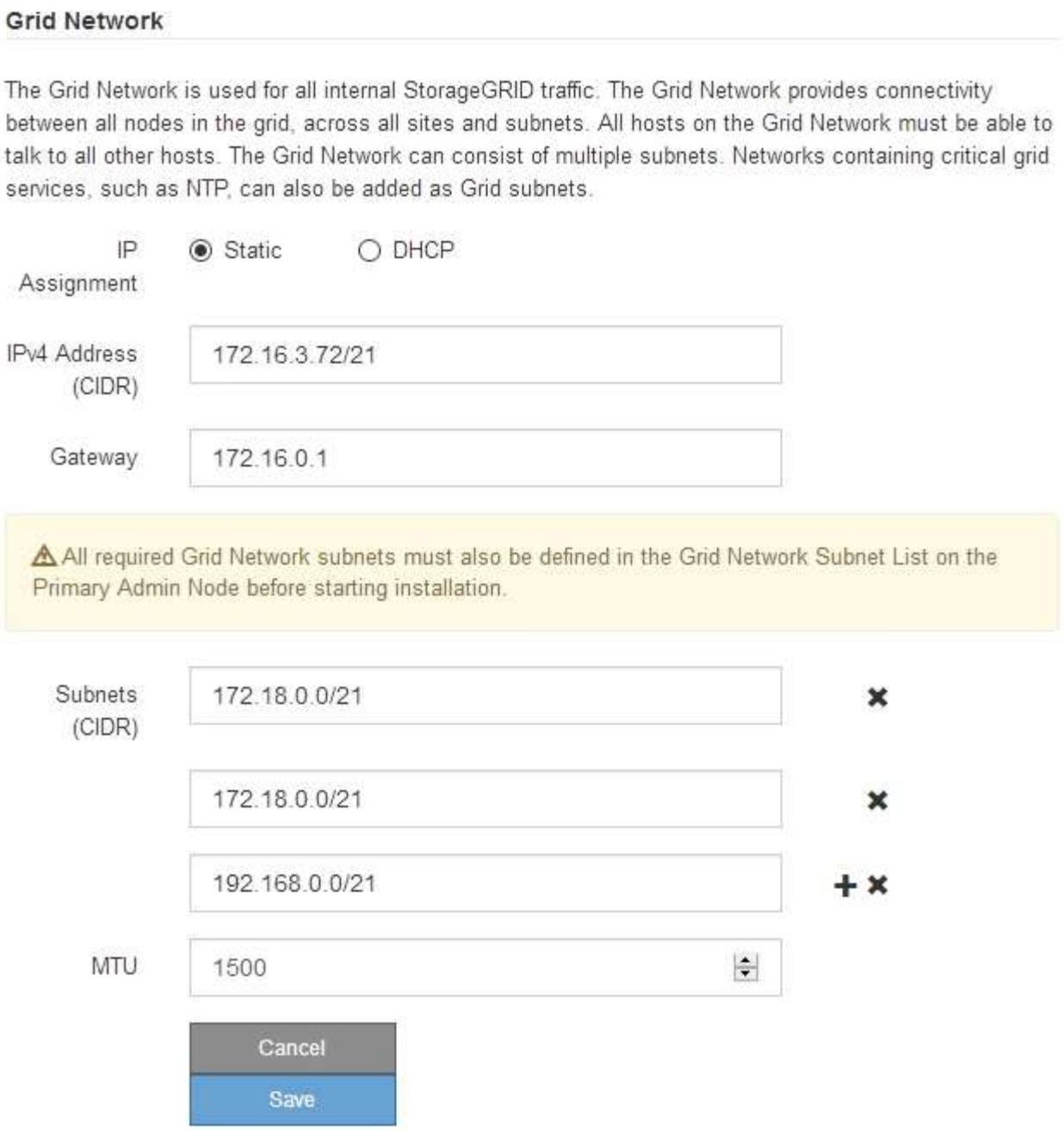
Se você quiser alterar a configuração do link, consulte as instruções para alterar a configuração do link do controlador E5600SG.

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração IP**.

   É apresentada a página Configuração IP.

2. Para configurar a rede de Grade, selecione **Static** ou **DHCP** na seção **Grid Network** da página.



3. Se você selecionou **Static**, siga estas etapas para configurar a rede de Grade:
   a. Insira o endereço IPv4 estático, usando a notação CIDR.
   b. Entre no gateway.

      Se a rede não tiver um gateway, insira novamente o mesmo endereço IPv4 estático.

   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

      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.

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.

d. Clique em **Salvar**.

Quando você altera o endereço IP, o gateway e a lista de sub-redes também podem mudar.

Se você perder a conexão com o Instalador do StorageGRID Appliance, insira novamente o URL usando o novo endereço IP estático que você acabou de atribuir. Por exemplo `https://services_appliance_IP:8443`

e. Confirme se a lista de sub-redes da rede de Grade está correta.

Se você tiver 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. Essas sub-redes de rede de grade também devem ser definidas na lista de sub-redes de rede de grade no nó de administração principal quando você iniciar a instalação do StorageGRID.

A rota padrão não está listada. Se a rede do cliente não estiver ativada, a rota padrão usará o gateway de rede de grade.

- Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
- Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

f. Clique em **Salvar**.

4. Se você selecionou **DHCP**, siga estas etapas para configurar a rede de Grade:

a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

Os campos **IPv4 Address**, **Gateway** e **sub-redes** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

b. Confirme se a lista de sub-redes da rede de Grade está correta.

Se você tiver 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. Essas sub-redes de rede de grade também devem ser definidas na lista de sub-redes de rede de grade no nó de administração principal quando você iniciar a instalação do StorageGRID.

A rota padrão não está listada. Se a rede do cliente não estiver ativada, a rota padrão usará o gateway de rede de grade.

- Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
- Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros

jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

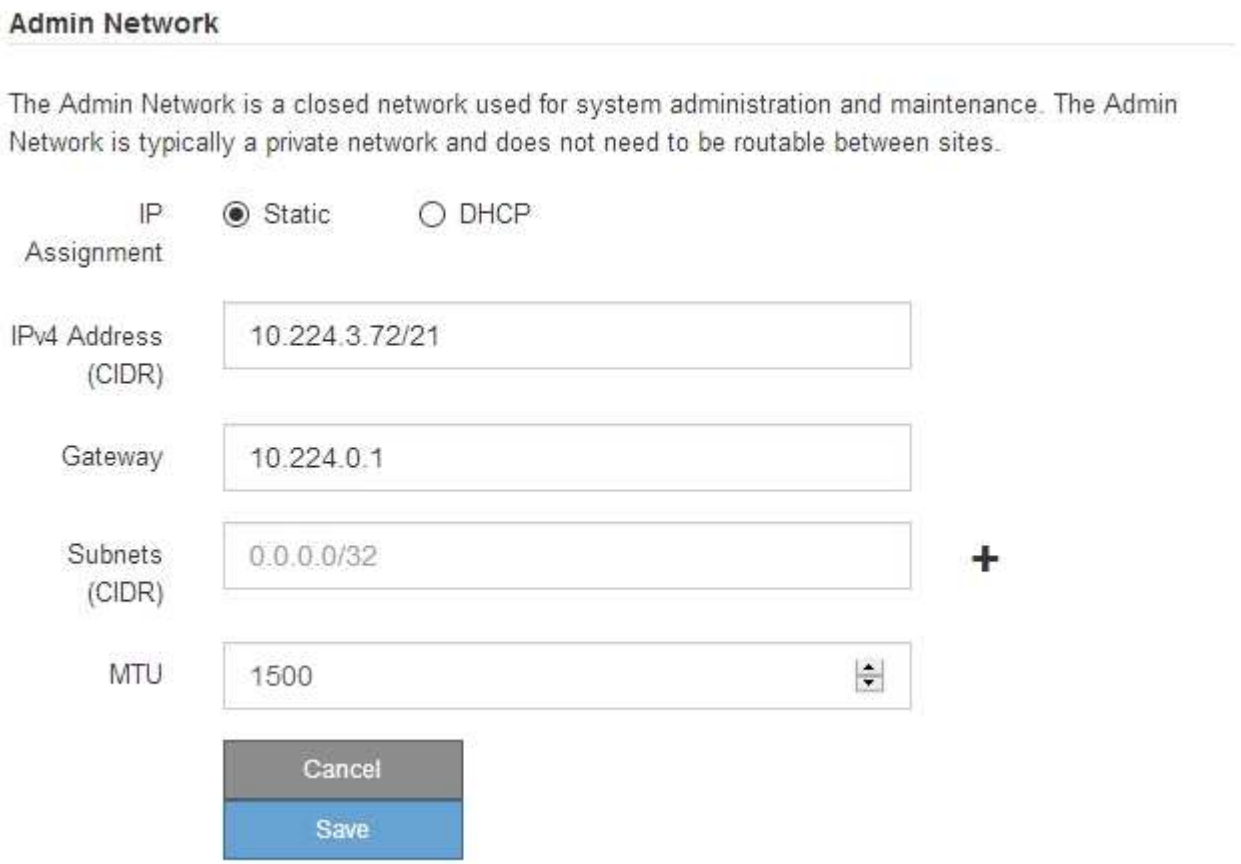
> O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

> 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.

a. Clique em **Salvar**.

5. Para configurar a rede Admin, selecione **Static** (estático) ou **DHCP** (DHCP) na secção Admin Network (rede Admin) da página.

> Para configurar a rede de administração, você deve ativar a rede de administração na página Configuração de ligação.



6. Se você selecionou **Static**, siga estas etapas para configurar a rede Admin:

a. Introduza o endereço IPv4 estático, utilizando a notação CIDR, para a porta de gestão 1 no dispositivo.

A porta de gerenciamento 1 fica à esquerda das duas portas RJ45 de 1 GbE na extremidade direita do dispositivo.

b. Entre no gateway.

   Se a rede não tiver um gateway, insira novamente o mesmo endereço IPv4 estático.

c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

   > 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.

d. Clique em **Salvar**.

   Quando você altera o endereço IP, o gateway e a lista de sub-redes também podem mudar.

   Se você perder a conexão com o Instalador do StorageGRID Appliance, insira novamente o URL usando o novo endereço IP estático que você acabou de atribuir. Por exemplo `https://services_appliance:8443`

e. Confirme se a lista de sub-redes Admin Network está correta.

   Você deve verificar se todas as sub-redes podem ser alcançadas usando o gateway fornecido.

   > A rota padrão não pode ser feita para usar o gateway de rede Admin.

   - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
   - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

f. Clique em **Salvar**.

7. Se você selecionou **DHCP**, siga estas etapas para configurar a rede Admin:

   a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

      Os campos **IPv4 Address**, **Gateway** e **sub-redes** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

      O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

   b. Confirme se a lista de sub-redes Admin Network está correta.

      Você deve verificar se todas as sub-redes podem ser alcançadas usando o gateway fornecido.

      > A rota padrão não pode ser feita para usar o gateway de rede Admin.

      - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
      - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

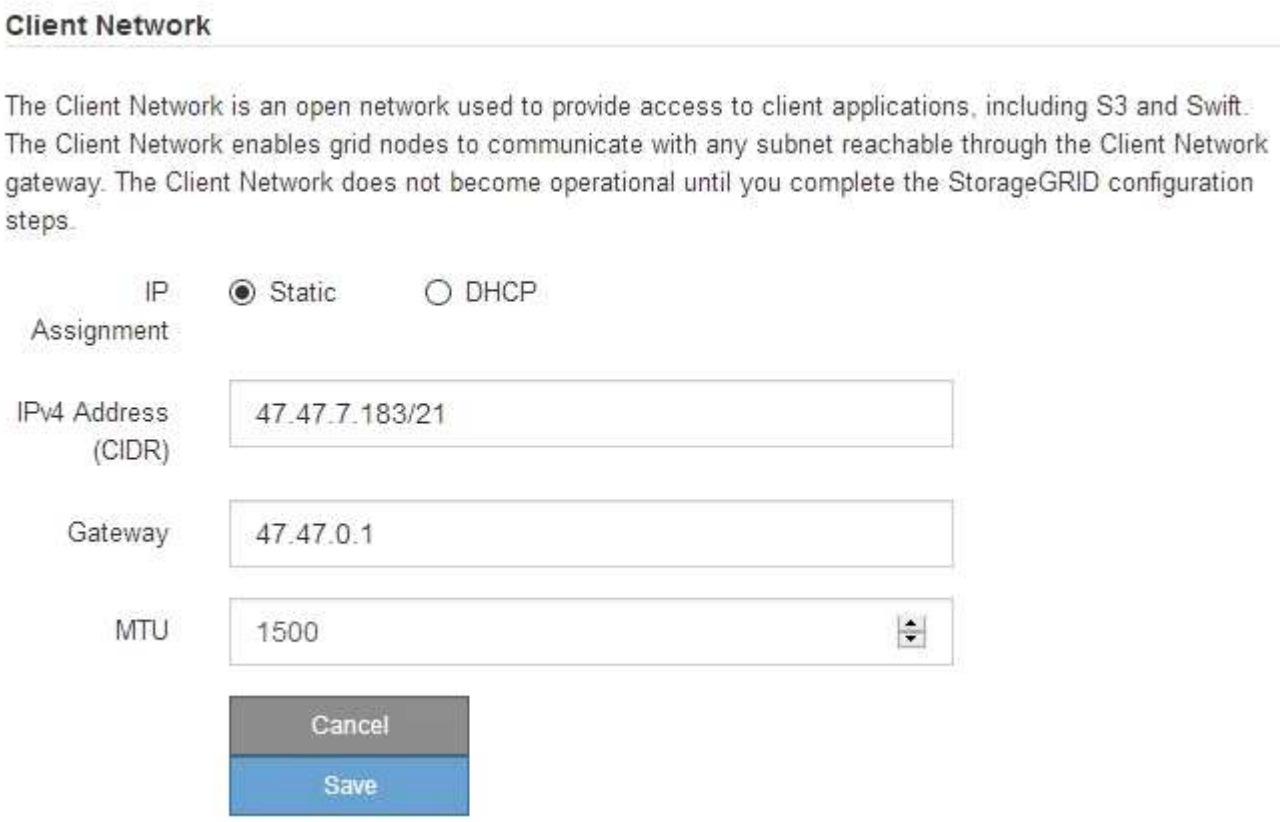
   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

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.

d. Clique em **Salvar**.

8. Para configurar a rede do cliente, selecione **estático** ou **DHCP** na seção **rede do cliente** da página.

Para configurar a rede do cliente, tem de ativar a rede do cliente na página Configuração da ligação.



9. Se você selecionou **Static**, siga estas etapas para configurar a rede do cliente:

a. Insira o endereço IPv4 estático, usando a notação CIDR.

b. Clique em **Salvar**.

c. Confirme se o endereço IP do gateway de rede do cliente está correto.

Se a rede do cliente estiver ativada, é apresentada a rota predefinida. A rota padrão usa o gateway de rede do cliente e não pode ser movida para outra interface enquanto a rede do cliente está ativada.

d. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

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.

e. Clique em **Salvar**.

10. Se você selecionou **DHCP**, siga estas etapas para configurar a rede do cliente:

    a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

       Os campos **IPv4 Address** e **Gateway** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

    O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

    a. Confirme se o gateway está correto.

       > ⓘ Se a rede do cliente estiver ativada, é apresentada a rota predefinida. A rota padrão usa o gateway de rede do cliente e não pode ser movida para outra interface enquanto a rede do cliente está ativada.

    b. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

       > ⓘ 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.

Informações relacionadas

"Alterar a configuração do link do controlador E5600SG"

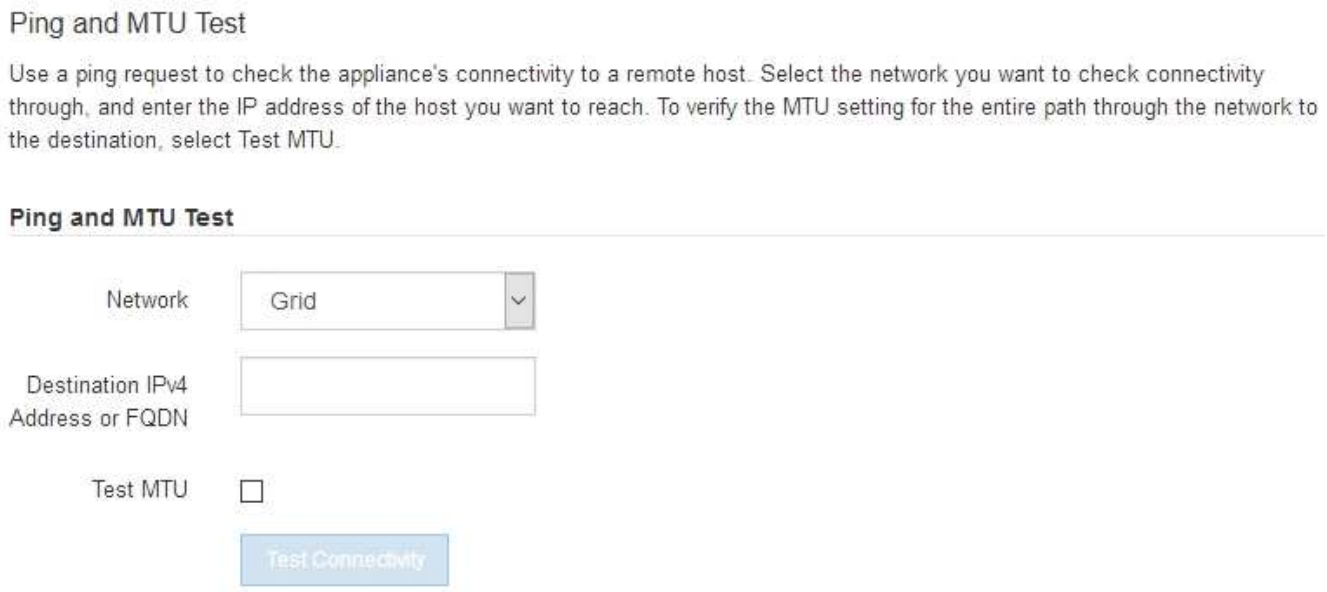
Verificando conexões de rede

Confirme que pode aceder às redes StorageGRID que está a utilizar a partir do dispositivo. Para validar o roteamento por meio de gateways de rede, você deve testar a conetividade entre o Instalador de dispositivos StorageGRID e endereços IP em diferentes sub-redes. Você também pode verificar a configuração MTU.

Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Teste de Ping e MTU**.

   A página Ping e MTU Test (Teste de Ping e MTU) é exibida.



2. Na caixa suspensa **rede**, selecione a rede que deseja testar: Grade, Admin ou Cliente.
3. Insira o endereço IPv4 ou o nome de domínio totalmente qualificado (FQDN) para um host nessa rede.

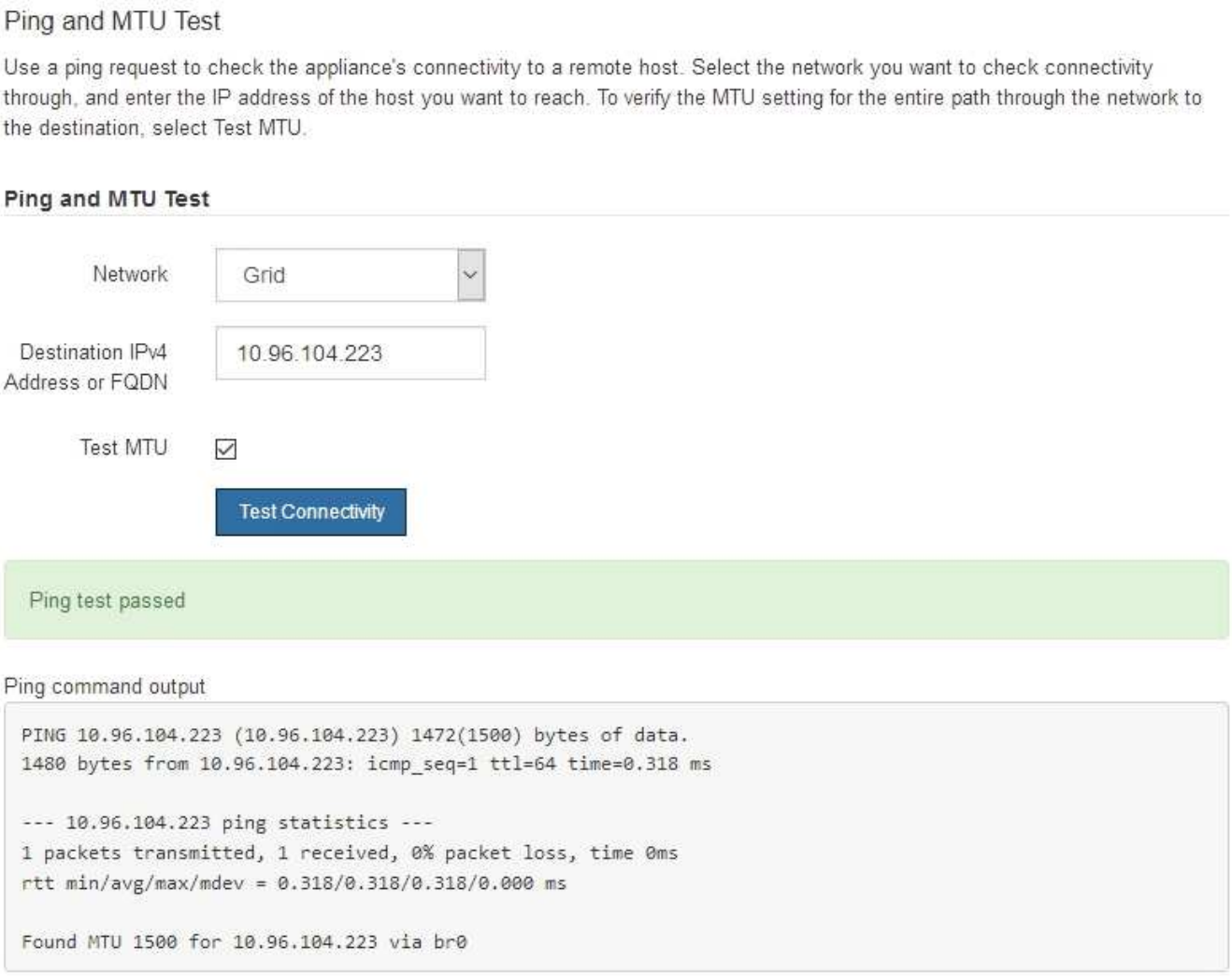
   Por exemplo, você pode querer fazer ping no gateway na rede ou no nó de administração principal.

4. Opcionalmente, marque a caixa de seleção **Test MTU** para verificar a configuração de MTU para todo o caminho através da rede até o destino.

   Por exemplo, você pode testar o caminho entre o nó do dispositivo e um nó em um local diferente.

5. Clique em **testar conetividade**.

   Se a conexão de rede for válida, a mensagem "Teste de ping aprovado" será exibida, com a saída do comando ping listada.



Informações relacionadas

"Configurando links de rede (SG5600)"

"Alterar a definição MTU"

Verificando conexões de rede no nível da porta

Para garantir que o acesso entre o Instalador de dispositivos StorageGRID e outros nós não esteja obstruído por firewalls, confirme se o Instalador de dispositivos StorageGRID pode se conetar a uma porta TCP específica ou conjunto de portas no endereço IP ou intervalo de endereços especificado.

Sobre esta tarefa

Usando a lista de portas fornecida no Instalador de dispositivos StorageGRID, você pode testar a conetividade entre o dispositivo e os outros nós da rede de Grade.

Além disso, você pode testar a conetividade nas redes Admin e Client e nas portas UDP, como as usadas para servidores NFS ou DNS externos. Para obter uma lista dessas portas, consulte a referência de porta nas diretrizes de rede do StorageGRID.

As portas de rede de grade listadas na tabela de conetividade de portas são válidas apenas para o StorageGRID versão 11,5.0. Para verificar quais portas estão corretas para cada tipo de nó, você deve sempre consultar as diretrizes de rede para sua versão do StorageGRID.

Passos

1. No Instalador de dispositivos StorageGRID, clique em **Configurar rede Teste de conetividade de porta (nmap)**.

   A página Teste de conetividade de porta é exibida.

   A tabela de conetividade de porta lista os tipos de nós que exigem conetividade TCP na rede de Grade. Para cada tipo de nó, a tabela lista as portas de rede de Grade que devem ser acessíveis ao seu dispositivo.

   The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

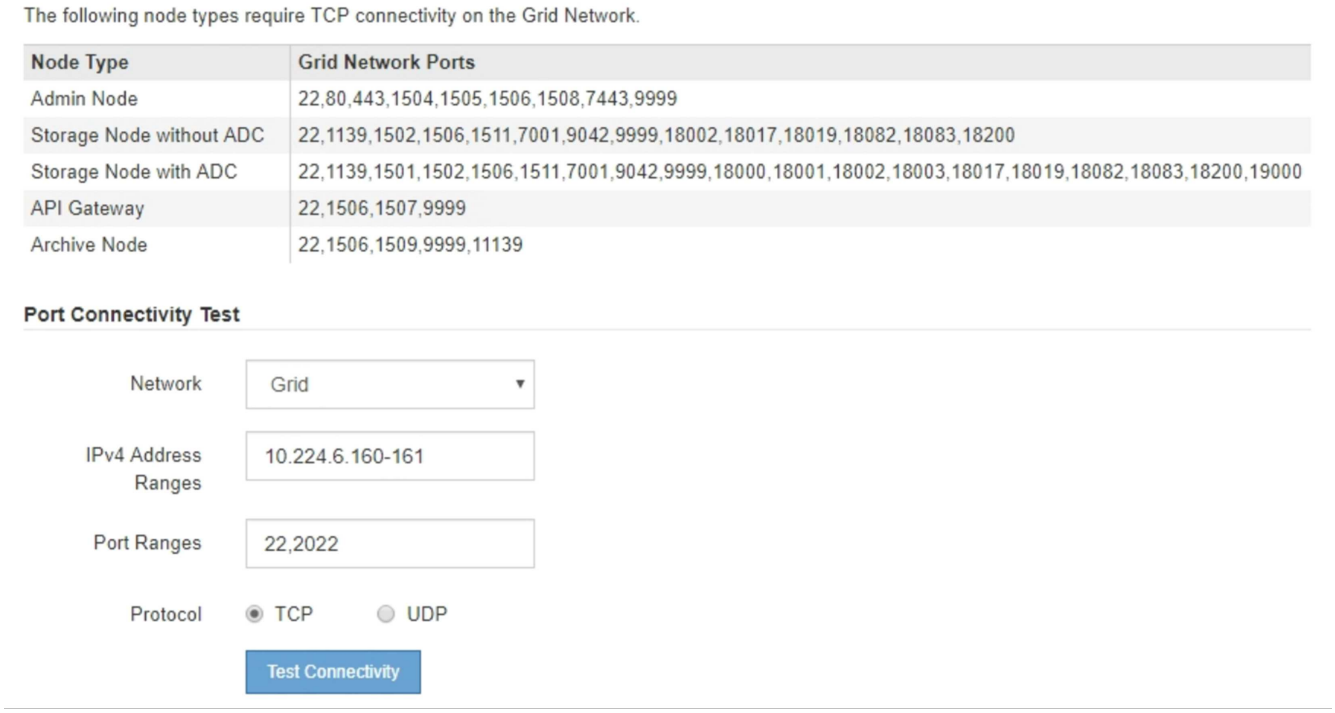
   Você pode testar a conetividade entre as portas do dispositivo listadas na tabela e os outros nós da rede de Grade.

2. Na lista suspensa **Network**, selecione a rede que deseja testar: **Grid**, **Admin** ou **Client**.
3. Especifique um intervalo de endereços IPv4 para os hosts nessa rede.

   Por exemplo, você pode querer pesquisar o gateway na rede ou no nó de administração principal.

   Especifique um intervalo usando um hífen, como mostrado no exemplo.

4. Insira um número de porta TCP, uma lista de portas separadas por vírgulas ou um intervalo de portas.



5. Clique em **testar conetividade**.

   - Se as conexões de rede no nível da porta selecionadas forem válidas, a mensagem ""Teste de conetividade de porta aprovado"" aparecerá em um banner verde. A saída do comando nmap está listada abaixo do banner.

   - Se uma conexão de rede no nível da porta for feita ao host remoto, mas o host não estiver ouvindo em uma ou mais das portas selecionadas, a mensagem ""Falha no teste de conetividade da porta"" aparecerá em um banner amarelo. A saída do comando nmap está listada abaixo do banner.

     Qualquer porta remota que o host não esteja ouvindo tem um estado de "fechado". Por exemplo, você pode ver esse banner amarelo quando o nó ao qual você está tentando se conetar estiver em um estado pré-instalado e o serviço StorageGRID NMS ainda não estiver sendo executado nesse nó.

- Se uma conexão de rede no nível de porta não puder ser feita para uma ou mais portas selecionadas, a mensagem "Falha no teste de conetividade de porta" aparecerá em um banner vermelho. A saída do comando nmap está listada abaixo do banner.

  O banner vermelho indica que uma tentativa de conexão TCP para uma porta no host remoto foi feita, mas nada foi retornado ao remetente. Quando nenhuma resposta é retornada, a porta tem um estado de "filtrada" e é provavelmente bloqueada por um firewall.

  Os portos com "fechado" também são listados.

Informações relacionadas

"Diretrizes de rede"

Configurando o SANtricity Storage Manager

Você pode usar o SANtricity Storage Manager para monitorar o status dos discos de

storage e componentes de hardware no dispositivo StorageGRID. Para acessar este software, você deve saber o endereço IP da porta de gerenciamento 1 no controlador E2700 (o controlador de armazenamento no dispositivo).

Passos

- "Definir o endereço IP do controlador E2700"
- "Adicionar o dispositivo ao SANtricity Storage Manager"
- "Configurar o SANtricity Storage Manager"

Definir o endereço IP do controlador E2700

A porta de gerenciamento 1 no controlador E2700 coneta o dispositivo à rede de gerenciamento do SANtricity Storage Manager. Você deve definir um endereço IP estático para o controlador E2700 para garantir que não perca a conexão de gerenciamento com o hardware e o firmware do controlador no dispositivo StorageGRID.

O que você vai precisar

Você está usando um navegador da Web compatível.

Sobre esta tarefa

Os endereços atribuídos pelo DHCP podem mudar a qualquer momento. Atribua um endereço IP estático ao controlador para garantir uma acessibilidade consistente.

Passos

1. No cliente, insira o URL para o instalador do StorageGRID Appliance
   `https://E5600SG_Controller_IP:8443`

   Para *`E5600SG_Controller_IP`*, use o endereço IP do dispositivo em qualquer rede StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configuração de hardware Configuração de rede do controlador de armazenamento**.

   A página Configuração da rede do controlador de armazenamento é exibida.

3. Dependendo da configuração da rede, selecione **Enabled** para IPv4, IPv6 ou ambos.
4. Anote o endereço IPv4 que é exibido automaticamente.

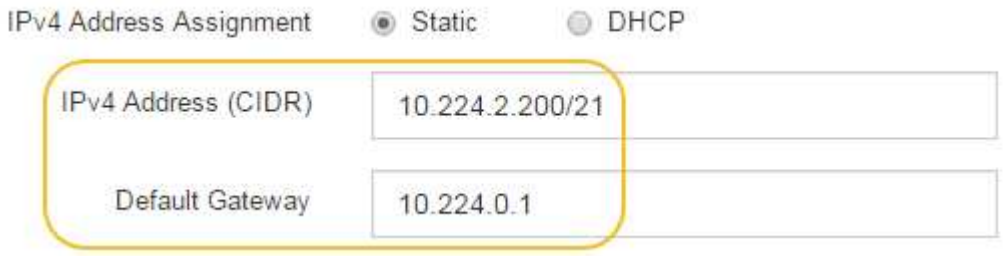
   DHCP é o método padrão para atribuir um endereço IP a esta porta.

   Pode demorar alguns minutos para que os valores DHCP apareçam.

5. Opcionalmente, defina um endereço IP estático para a porta de gerenciamento do controlador E2700.

> Você deve atribuir um IP estático para a porta de gerenciamento ou atribuir uma concessão permanente para o endereço no servidor DHCP.

   a. Selecione **estático**.
   b. Introduza o endereço IPv4, utilizando a notação CIDR.
   c. Introduza o gateway predefinido.



   d. Clique em **Salvar**.

      Pode levar alguns minutos para que suas alterações sejam aplicadas.

Quando você se conetar ao SANtricity Storage Manager, você usará o novo endereço IP estático como URL
`https://E2700_Controller_IP`

Informações relacionadas

"Documentação do NetApp: SANtricity Storage Manager"

Adicionar o dispositivo ao SANtricity Storage Manager

Ligue o controlador E2700 do dispositivo ao SANtricity Storage Manager e, em seguida, adicione o dispositivo como uma matriz de armazenamento.

O que você vai precisar

Você está usando um navegador da Web compatível.

Sobre esta tarefa

Para obter instruções detalhadas, consulte a documentação do SANtricity Storage Manager.

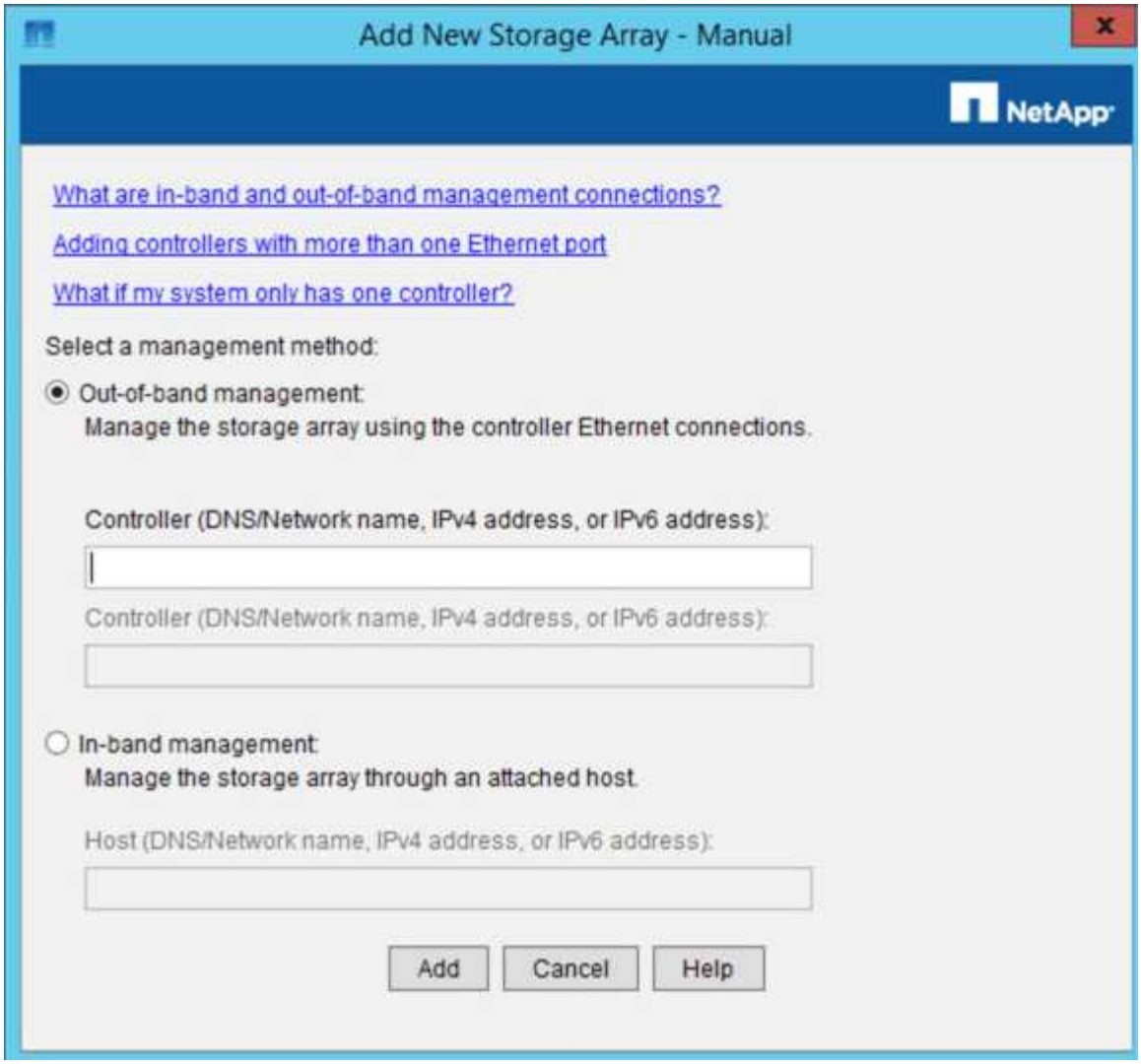
Passos

1. Abra um navegador da Web e insira o endereço IP como o URL do SANtricity Storage Manager
`https://E2700_Controller_IP`

   É apresentada a página de início de sessão do SANtricity Storage Manager.

2. Na página **Selecionar método de adição**, selecione **Manual** e clique em **OK**.
3. Selecione **Editar Adicionar matriz de armazenamento**.

   A página Adicionar nova matriz de armazenamento - manual é exibida.



4. Na caixa **Gerenciamento fora da banda**, insira um dos seguintes valores:
   - **Usando DHCP:** o endereço IP atribuído pelo servidor DHCP à porta de gerenciamento 1 no controlador E2700
   - **Não utilizar DHCP:** `192.168.128.101`

   > Apenas um dos controladores do dispositivo está ligado ao SANtricity Storage Manager, pelo que só precisa de introduzir um endereço IP.

5. Clique em **Add**.

Informações relacionadas

"Documentação do NetApp: SANtricity Storage Manager"

Configurar o SANtricity Storage Manager

Depois de acessar o SANtricity Storage Manager, você pode usá-lo para configurar as configurações de hardware. Normalmente, você configura essas configurações antes de implantar o dispositivo como nó de armazenamento em um sistema StorageGRID.

Passos

- "Configurando o AutoSupport"
- "Verificando o recebimento do AutoSupport"
- "Configurando notificações de alerta de intercetação de e-mail e SNMP"
- "Definindo senhas para SANtricity Storage Manager"

Configurando o AutoSupport

A ferramenta AutoSupport coleta dados em um pacote de suporte ao cliente do dispositivo e envia os dados automaticamente para o suporte técnico. A configuração do AutoSupport auxilia o suporte técnico com solução remota de problemas e análise de problemas.

O que você vai precisar

- A funcionalidade AutoSupport tem de estar ativada e ativada no aparelho.

  O recurso AutoSupport é ativado e desativado globalmente em uma estação de gerenciamento de storage.

- O Monitor de eventos do Gestor de armazenamento tem de estar a funcionar em pelo menos uma máquina com acesso ao aparelho e, de preferência, em não mais do que uma máquina.

Sobre esta tarefa

Todos os dados são compatados em um único formato de arquivo compactado (.7z) no local especificado.

O AutoSupport fornece os seguintes tipos de mensagens:

Tipos de mensagens	Descrição
Mensagens de evento	• Enviado quando ocorre um evento de suporte no dispositivo gerenciado • Incluir informações de configuração e diagnóstico do sistema
Mensagens diárias	• Enviado uma vez por dia durante um intervalo de tempo configurável pelo utilizador na hora local do aparelho • Inclua os logs de eventos do sistema e os dados de desempenho atuais
Mensagens semanais	• Enviado uma vez por semana durante um intervalo de tempo configurável pelo utilizador na hora local do aparelho • Inclua informações de configuração e estado do sistema

Passos

1. Na janela Gerenciamento Empresarial no SANtricity Storage Manager, selecione a guia **dispositivos** e, em seguida, selecione **matrizes de armazenamento descobertas**.

2. Selecione **Ferramentas AutoSupport Configuração**.
3. Use a ajuda on-line do SANtricity Storage Manager, se necessário, para concluir a tarefa.

Informações relacionadas

"Documentação do NetApp: SANtricity Storage Manager"

Verificando o recebimento do AutoSupport

Você deve verificar se o suporte técnico está recebendo suas mensagens do AutoSupport. Você pode encontrar o status do AutoSupport para seus sistemas no portal do Active IQ. Verificar o recebimento dessas mensagens garante que o suporte técnico tenha suas informações se precisar de assistência.

Sobre esta tarefa

O AutoSupport pode apresentar um dos seguintes Estados:

- **LIGADO**

  Um STATUS LIGADO indica que o suporte técnico está recebendo mensagens AutoSupport do sistema.

- **OFF**

  Um status OFF sugere que você pode ter desabilitado o AutoSupport porque o suporte técnico não recebeu um Registro semanal do sistema nos últimos 15 dias de calendário ou pode ter ocorrido uma alteração no ambiente ou na configuração (por exemplo).

- **DECLÍNIO**

  Um status DE REJEIÇÃO significa que você notificou o suporte técnico de que não ativará o AutoSupport.

Depois que o suporte técnico recebe um Registro semanal do sistema, o status do AutoSupport muda para ATIVADO.

Passos

1. Vá para o site de suporte da NetApp em "mysupport.NetApp.com"e entre no portal da Active IQ.
2. Se o estado do AutoSupport estiver DESLIGADO e acreditar que está incorreto, efetue o seguinte:
   a. Verifique a configuração do sistema para garantir que você ativou o AutoSupport.
   b. Verifique o ambiente e a configuração da rede para garantir que o sistema possa enviar mensagens para o suporte técnico.

Configurando notificações de alerta de intercetação de e-mail e SNMP

A SANtricity Storage Manager pode notificá-lo quando o status do aparelho ou de um de seus componentes mudar. Isso é chamado de notificação de alerta. Você pode receber notificações de alerta por dois métodos diferentes: Traps de e-mail e SNMP. Você deve configurar as notificações de alerta que deseja receber.

Passos

1. Na janela Gerenciamento Empresarial no SANtricity Storage Manager, selecione a guia **dispositivos** e, em seguida, selecione um nó.

2. Selecione **Editar Configurar alertas**.
3. Selecione a guia **Email** para configurar notificações de alerta por e-mail.
4. Selecione o separador **SNMP** para configurar notificações de alerta de trap SNMP.
5. Use a ajuda on-line do SANtricity Storage Manager, se necessário, para concluir a tarefa.

Definindo senhas para SANtricity Storage Manager

Você pode definir as senhas usadas para o dispositivo no SANtricity Storage Manager. A definição de palavras-passe mantém a segurança do sistema.

Passos

1. Na janela Gerenciamento Empresarial no SANtricity Storage Manager, clique duas vezes no controlador.
2. Na janela Gerenciamento de matrizes, selecione o menu **Storage Array** e selecione **Security Set Password**.
3. Configure as senhas.
4. Use a ajuda on-line do SANtricity Storage Manager, se necessário, para concluir a tarefa.

Opcional: Habilitando a criptografia de nó

Se você ativar a criptografia de nó, os discos do seu dispositivo podem ser protegidos pela criptografia de servidor de gerenciamento de chaves (KMS) seguro contra perda física ou remoção do site. Você deve selecionar e ativar a criptografia de nó durante a instalação do dispositivo e não pode desmarcar a criptografia de nó depois que o processo de criptografia KMS for iniciado.

O que você vai precisar

Consulte as informações sobre o KMS nas instruções de administração do StorageGRID.

Sobre esta tarefa

Um dispositivo com criptografia de nó ativada se coneta ao servidor de gerenciamento de chaves externas (KMS) configurado para o site StorageGRID. Cada cluster KMS (ou KMS) gerencia as chaves de criptografia para todos os nós de dispositivo no local. Essas chaves criptografam e descriptografam os dados em cada disco em um dispositivo que tem criptografia de nó ativada.

Um KMS pode ser configurado no Gerenciador de Grade antes ou depois que o dispositivo é instalado no StorageGRID. Consulte as informações sobre a configuração do KMS e do appliance nas instruções de administração do StorageGRID para obter detalhes adicionais.

- Se um KMS for configurado antes de instalar o dispositivo, a criptografia controlada pelo KMS será iniciada quando você ativar a criptografia de nó no dispositivo e adicioná-la a um site do StorageGRID onde o KMS está configurado.
- Se um KMS não for configurado antes de instalar o dispositivo, a criptografia controlada por KMS é executada em cada dispositivo que tem criptografia de nó ativada assim que um KMS é configurado e disponível para o site que contém o nó do dispositivo.

Todos os dados existentes antes de um dispositivo que tenha criptografia de nó ativada se conetarem ao KMS configurado são criptografados com uma chave temporária que não é segura. O aparelho não está protegido contra remoção ou roubo até que a chave esteja definida para um valor fornecido pelo KMS.

Sem a chave KMS necessária para descriptografar o disco, os dados no dispositivo não podem ser recuperados e são efetivamente perdidos. Este é o caso sempre que a chave de descriptografia não pode ser recuperada do KMS. A chave fica inacessível se um cliente limpar a configuração do KMS, uma chave KMS expira, a conexão com o KMS é perdida ou o dispositivo é removido do sistema StorageGRID onde suas chaves KMS são instaladas.

Passos

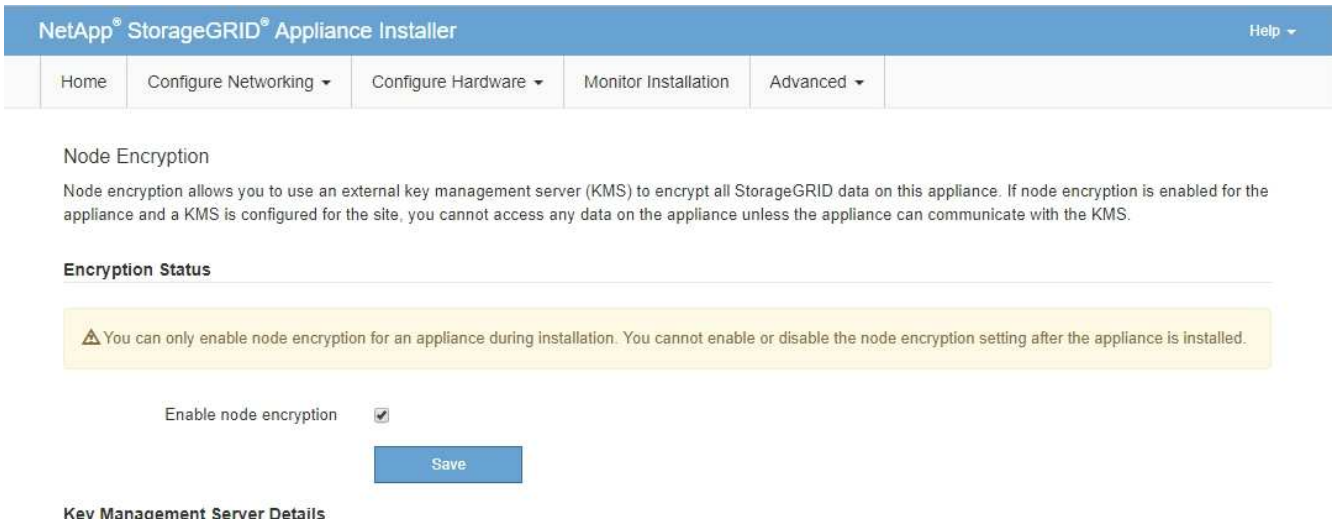
1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

   Depois que o dispositivo tiver sido criptografado com uma chave KMS, os discos do appliance não podem ser descriptografados sem usar a mesma chave KMS.

2. Selecione **Configure hardware Node Encryption**.



3. Selecione **Ativar criptografia de nó**.

   Você pode desmarcar **Ativar criptografia de nó** sem risco de perda de dados até selecionar **Salvar** e o nó do dispositivo acessar as chaves de criptografia KMS em seu sistema StorageGRID e iniciar a criptografia de disco. Não é possível desativar a criptografia de nó após a instalação do dispositivo.

   Depois de adicionar um dispositivo que tenha a criptografia de nó ativada a um site do StorageGRID que tenha um KMS, você não poderá parar de usar a criptografia KMS para o nó.

4. Selecione **Guardar**.

5. Implante o dispositivo como um nó no sistema StorageGRID.

   A encriptação controlada POR KMS começa quando o dispositivo acede às chaves KMS configuradas para o seu site StorageGRID. O instalador exibe mensagens de progresso durante o processo de criptografia KMS, o que pode levar alguns minutos, dependendo do número de volumes de disco no dispositivo.

   > Os dispositivos são configurados inicialmente com uma chave de criptografia aleatória não KMS atribuída a cada volume de disco. Os discos são criptografados usando essa chave de criptografia temporária, que não é segura, até que o dispositivo que tem criptografia de nó habilitada acesse as chaves KMS configuradas para o site do StorageGRID.

Depois de terminar

Você pode exibir o status da criptografia do nó, os detalhes do KMS e os certificados em uso quando o nó do dispositivo está no modo de manutenção.

Informações relacionadas

"Administrar o StorageGRID"

"Monitorização da encriptação do nó no modo de manutenção"

Opcional: Mudar para o modo RAID6 (apenas SG5660)

Se você tiver um SG5660 com 60 unidades, poderá alterar a configuração de volume de sua configuração padrão e recomendada, Dynamic Disk Pools (DDP), para RAID6. Você só pode alterar o modo antes de implantar o nó de storage do dispositivo StorageGRID.

O que você vai precisar

- Você tem um SG5660. O SG5612 não suporta RAID6. Se tiver um SG5612, tem de utilizar o modo DDP.

> Se algum volume já tiver sido configurado ou se o StorageGRID tiver sido instalado anteriormente, a alteração do modo RAID fará com que os volumes sejam removidos e substituídos. Quaisquer dados sobre esses volumes serão perdidos.

Sobre esta tarefa

Antes de implantar um nó de storage do dispositivo StorageGRID, você pode escolher entre duas opções de configuração de volume:

- **Dynamic Disk Pools (DDP)** — esta é a configuração padrão e recomendada. O DDP é um esquema de proteção de dados de hardware aprimorado que oferece melhor performance do sistema, tempos de reconstrução reduzidos após falhas de unidade e facilidade de gerenciamento.
- **RAID6** — este é um esquema de proteção de hardware que usa listras de paridade em cada disco e permite duas falhas de disco no conjunto RAID antes que qualquer dado seja perdido.

> O uso do RAID6 não é recomendado para a maioria dos ambientes StorageGRID. Embora o RAID6 possa aumentar a eficiência de storage para 88% (em comparação com 80% no DDP), o modo DDP oferece recuperação mais eficiente de falhas de unidade.

Passos

1. Usando o laptop de serviço, abra um navegador da Web e acesse o Instalador do StorageGRID Appliance

`https://E5600SG_Controller_IP:8443`

`_E5600SG_Controller_IP_`Onde está qualquer um dos endereços IP para o controlador E5600SG.

2. Na barra de menus, selecione **Avançado modo RAID**.
3. Na página **Configure RAID Mode**, selecione **RAID6** na lista suspensa Mode (modo).
4. Clique em **Salvar**.

Opcional: Remapeamento de portas de rede para o dispositivo

Talvez seja necessário remapear as portas internas no nó de armazenamento do dispositivo para diferentes portas externas. Por exemplo, talvez seja necessário remapear as portas devido a um problema de firewall.

O que você vai precisar

- Você acessou anteriormente o Instalador de dispositivos StorageGRID.
- Você não configurou e não planeja configurar pontos de extremidade do balanceador de carga.

> Se você remapear quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Se você quiser configurar pontos de extremidade do balanceador de carga e já tiver portas remapeadas, siga as etapas nas instruções de recuperação e manutenção para remover os remapes de portas.

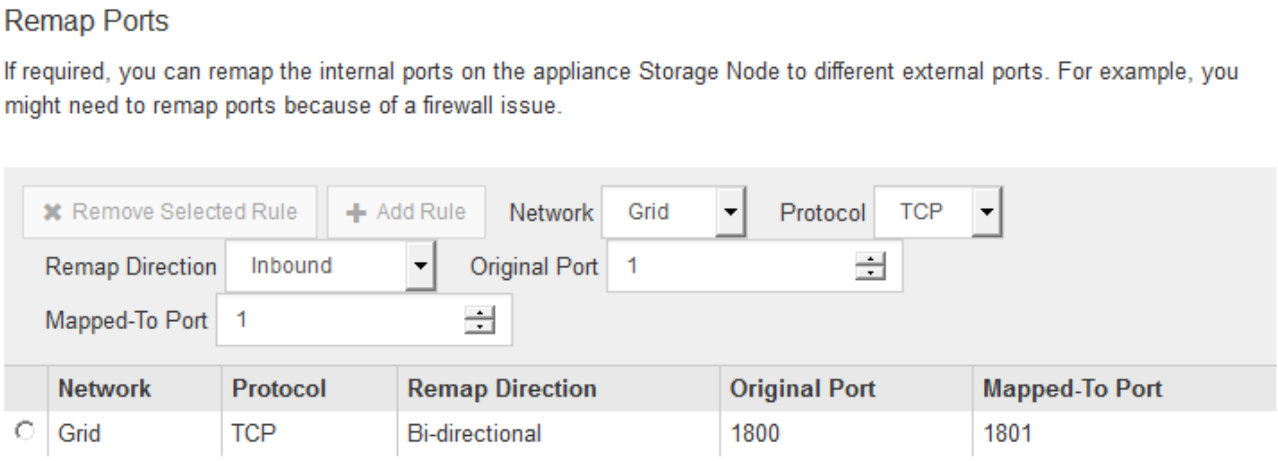
Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Remapear portas**.

   É apresentada a página Remapear porta.

2. Na caixa suspensa **rede**, selecione a rede para a porta que deseja remapear: Grade, Admin ou Cliente.
3. Na caixa suspensa **Protocol** (Protocolo), selecione o protocolo IP: TCP ou UDP.
4. Na caixa suspensa **Remap Direction**, selecione qual direção de tráfego você deseja remapear para esta porta: Inbound, Outbound ou Bi-direcional.
5. Para **original Port**, insira o número da porta que deseja remapear.
6. Para **Mapped-to Port**, insira o número da porta que deseja usar.
7. Clique em **Adicionar regra**.

   O novo mapeamento de portas é adicionado à tabela e o remapeamento entra em vigor imediatamente.



8. Para remover um mapeamento de portas, selecione o botão de opção da regra que deseja remover e clique em **Remover regra selecionada**.

Informações relacionadas

"Manter recuperar"

Implantando um nó de storage de dispositivos

Depois de instalar e configurar o dispositivo de storage, você pode implantá-lo como um nó de storage em um sistema StorageGRID. Ao implantar um dispositivo como nó de storage, você usa o Instalador de dispositivos StorageGRID incluído no dispositivo.

O que você vai precisar

- Se você estiver clonando um nó de dispositivo, continue seguindo o processo de recuperação e manutenção.

  "Manter recuperar"

- O dispositivo foi instalado em um rack ou gabinete, conetado às redes e ligado.
- Links de rede, endereços IP e remapeamento de portas (se necessário) foram configurados para o dispositivo usando o Instalador de dispositivos StorageGRID.
- Você conhece um dos endereços IP atribuídos ao controlador de computação do dispositivo. Você pode usar o endereço IP de qualquer rede StorageGRID conetada.
- O nó de administração principal do sistema StorageGRID foi implantado.
- 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.
- Você tem um laptop de serviço com um navegador da Web suportado.

Sobre esta tarefa

Cada dispositivo de storage funciona como um nó de storage único. Qualquer dispositivo pode se conetar à rede de Grade, à rede Admin e à rede Cliente

Para implantar um nó de armazenamento de dispositivos em um sistema StorageGRID, você acessa o Instalador de dispositivos StorageGRID e executa as seguintes etapas:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do nó de armazenamento.
- Você inicia a implantação e espera à medida que os volumes são configurados e o software é instalado.
- Quando a instalação é interrompida parcialmente nas tarefas de instalação do dispositivo, você retoma a instalação iniciando sessão no Gerenciador de Grade, aprovando todos os nós de grade e concluindo os processos de instalação e implantação do StorageGRID.

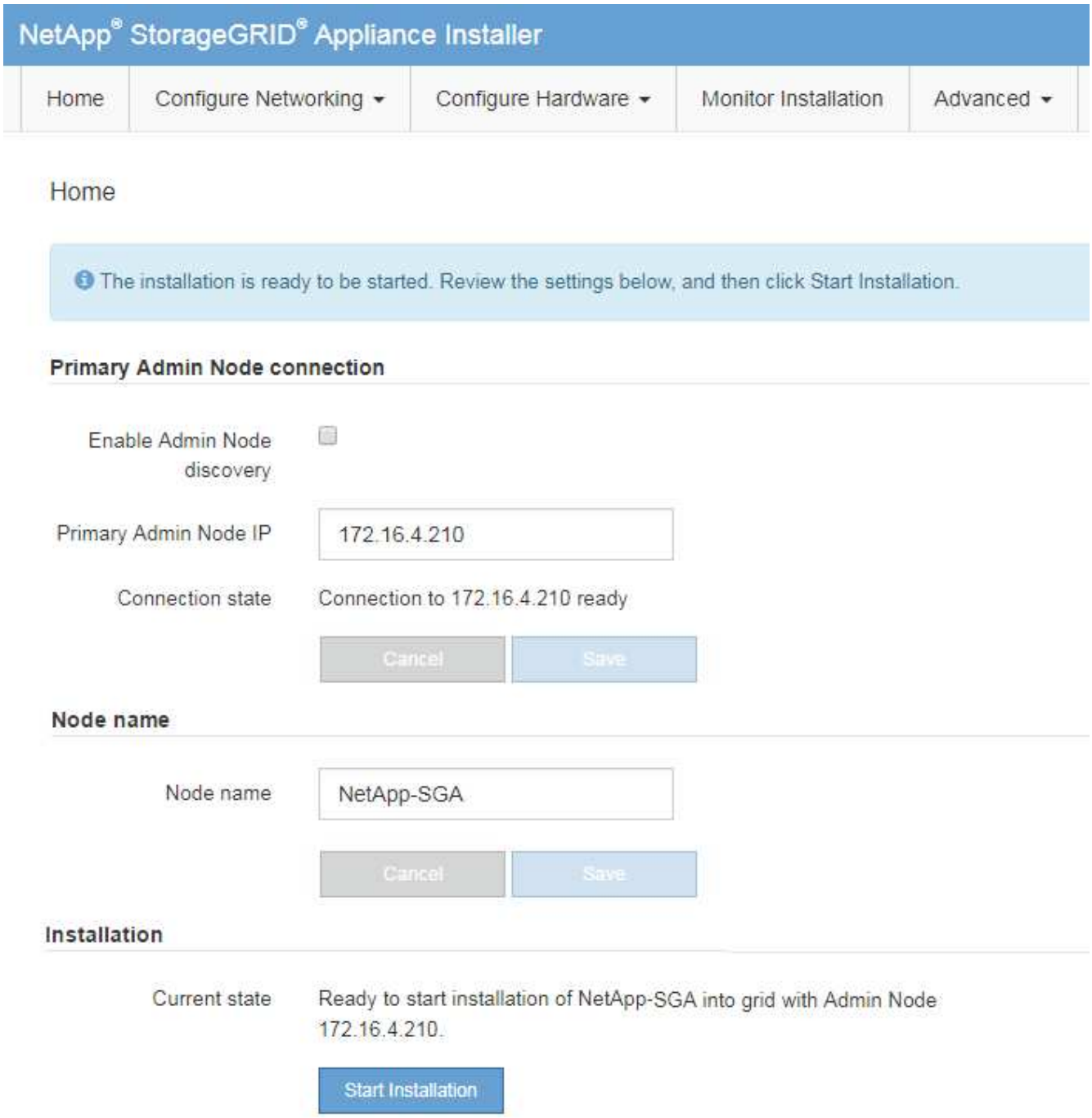
> Se você precisar implantar vários nós de dispositivo de uma só vez, você pode automatizar o processo de instalação usando o `configure-sga.py` script de instalação do dispositivo.

- Se você estiver executando uma operação de expansão ou recuperação, siga as instruções apropriadas:
  - Para adicionar um nó de storage do dispositivo a um sistema StorageGRID existente, consulte as instruções para expandir um sistema StorageGRID.
  - Para implantar um nó de armazenamento de dispositivos como parte de uma operação de recuperação, consulte as instruções para recuperação e manutenção.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `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 clique em **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 `node name` na grade com nó Admin primário `admin_ip` " e se o botão **Iniciar instalação** está ativado.

   Se o botão **Start Installation** (Iniciar instalação) não estiver ativado, poderá ser necessário alterar a configuração da rede ou as definições da porta. Para obter instruções, consulte as instruções de instalação e manutenção do seu aparelho.

   > Se você estiver implantando o dispositivo Storage Node como um destino de clonagem de nós, interrompa o processo de implantação aqui e continue o procedimento de clonagem de nós na recuperação e na manutenção.

   "Manter recuperar"

6. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.

   O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

   > Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor**.

7. Se a grade incluir vários nós de storage do dispositivo, repita estas etapas 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 `configure-sga.py` script de instalação do dispositivo. Este script se aplica somente aos nós de storage.

Informações relacionadas

"Expanda sua grade"

"Manter recuperar"

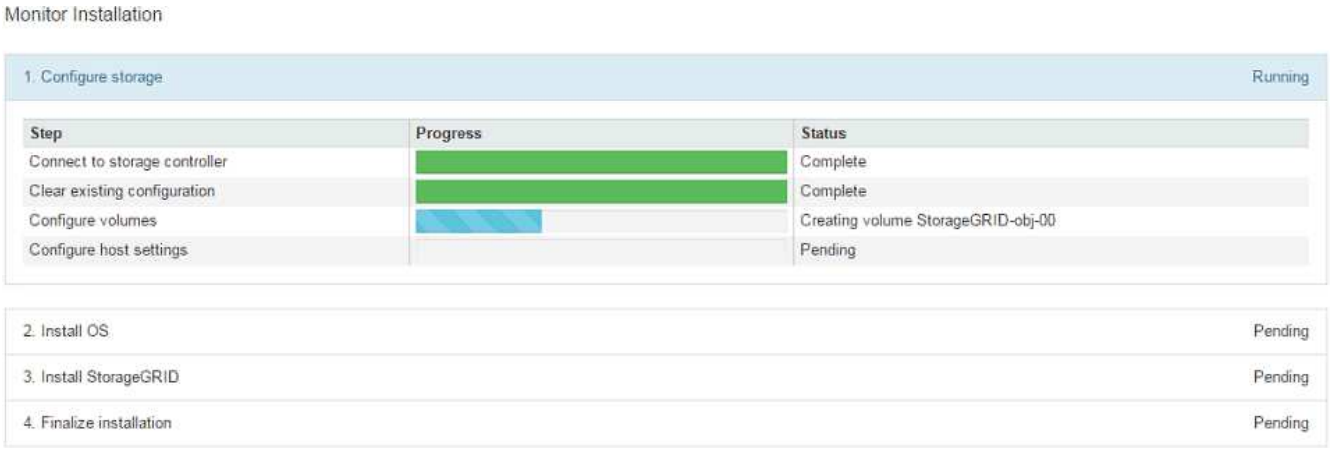
Monitorização da instalação do dispositivo de armazenamento

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**.

   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 serão mostradas com uma barra de status verde e um status de ""pulado"".

2. Reveja o progresso das duas primeiras fases de instalação.

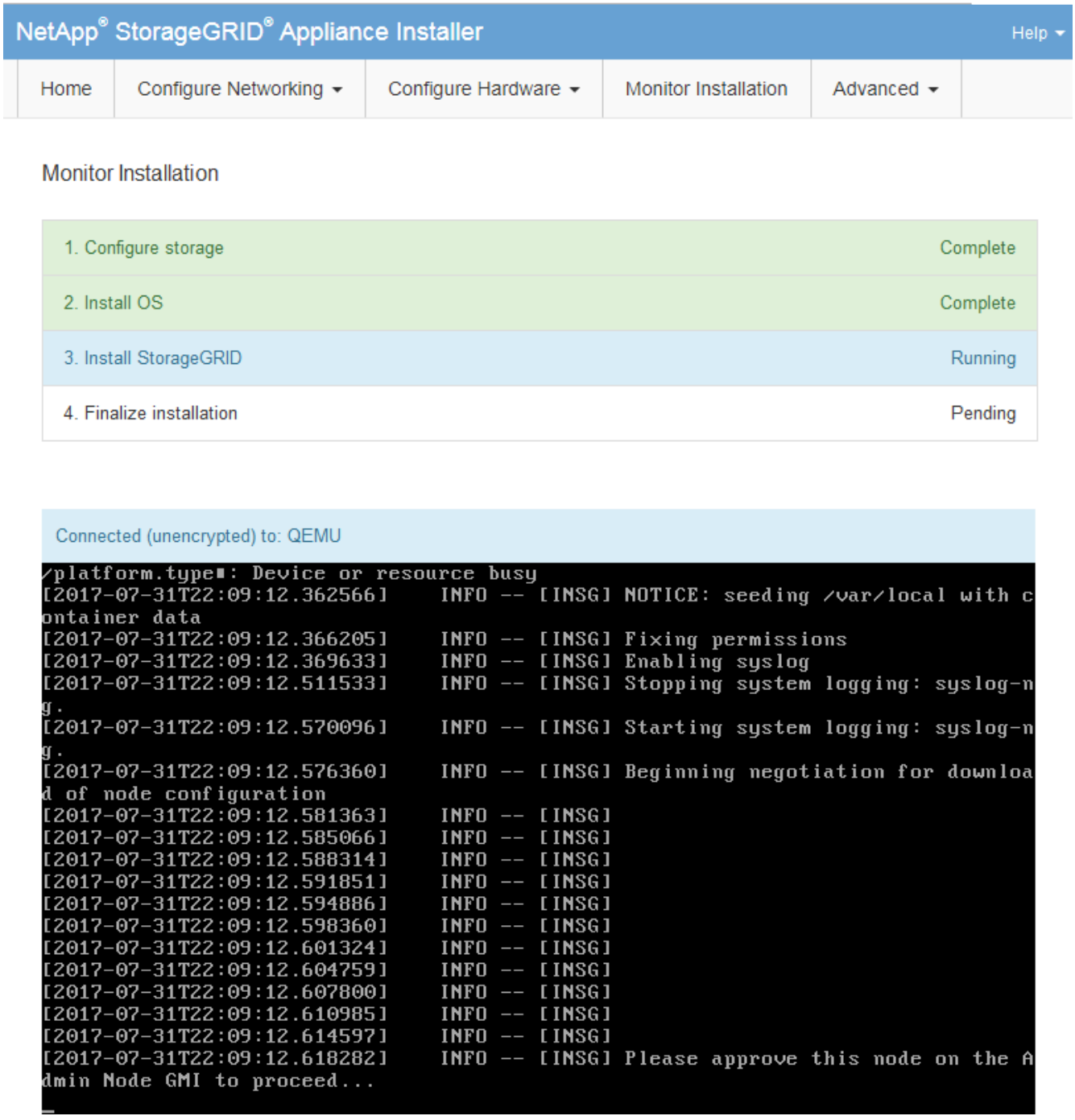
   1. Configurar armazenamento

   Durante essa etapa, o instalador se coneta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o software SANtricity para configurar volumes e configura as configurações do host.

   2. Instale o os

Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID para o dispositivo.

3. Continue monitorando o progresso da instalação até que o estágio **Install StorageGRID** pare e uma mensagem seja exibida no console incorporado, solicitando que você aprove esse nó no nó Admin usando o Gerenciador de Grade. Vá para a próxima etapa.



4. Vá para o Gerenciador de Grade, aprove o nó de armazenamento pendente e conclua o processo de instalação do StorageGRID.

   Quando você clica em **Install** no Gerenciador de Grade, o estágio 3 é concluído e o estágio 4, **Finalize a instalação**, começa. Quando a fase 4 é concluída, o controlador é reinicializado.

Automatizando a instalação e a configuração do dispositivo

Você pode automatizar a instalação e configuração de seus dispositivos e a configuração de todo o sistema StorageGRID.

Sobre esta tarefa

A automação da instalação e configuração pode ser útil para implantar várias instâncias do StorageGRID ou uma instância grande e complexa do StorageGRID.

Para automatizar a instalação e a configuração, use uma ou mais das seguintes opções:

- Crie um arquivo JSON que especifique as configurações para seus dispositivos. Carregue o arquivo JSON usando o instalador do dispositivo StorageGRID.

  Você pode usar o mesmo arquivo para configurar mais de um dispositivo.

- Use o script Python do StorageGRID`configure-sga.py` para automatizar a configuração de seus dispositivos.
- Use scripts Python adicionais para configurar outros componentes de todo o sistema StorageGRID (a "grade").

Você pode usar os scripts Python de automação do StorageGRID diretamente ou usá-los como exemplos de como usar a API REST de instalação do StorageGRID nas ferramentas de implantação e configuração de grade que você mesmo desenvolve. Consulte as informações sobre como baixar e extrair os arquivos de instalação do StorageGRID nas instruções de recuperação e manutenção.

Automatizando a configuração do dispositivo usando o Instalador de dispositivos StorageGRID

Você pode automatizar a configuração de um appliance usando um arquivo JSON que contém as informações de configuração. Você carrega o arquivo usando o Instalador do StorageGRID Appliance.

O que você vai precisar

- O seu dispositivo tem de estar no firmware mais recente compatível com o StorageGRID 11,5 ou superior.
- Você deve estar conetado ao Instalador do StorageGRID Appliance no dispositivo que você está configurando usando um navegador compatível.

Sobre esta tarefa

É possível automatizar as tarefas de configuração do dispositivo, como configurar o seguinte:

- Rede de grade, rede de administração e endereços IP da rede de cliente
- Interface BMC
- Ligações de rede
  - Modo de ligação da porta
  - Modo de ligação de rede
  - Velocidade da ligação

Configurar o dispositivo usando um arquivo JSON carregado geralmente é mais eficiente do que executar a

configuração manualmente usando várias páginas no Instalador de dispositivos StorageGRID, especialmente se você tiver que configurar muitos nós. Você deve aplicar o arquivo de configuração para cada nó um de cada vez.

> Usuários experientes que desejam automatizar tanto a instalação quanto a configuração de seus dispositivos podem usar o `configure-sga.py` script. E "Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py"

Passos

1. Gere o arquivo JSON usando um dos seguintes métodos:
   - O aplicativo ConfigBuilder

     "ConfigBuilder.NetApp.com"

   - O `configure-sga.py` script de configuração do dispositivo. Você pode baixar o script do Instalador do StorageGRID Appliance (**Ajuda Script de configuração do appliance**). Consulte as instruções sobre como automatizar a configuração usando o script configure-sga.py.

     "Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py"

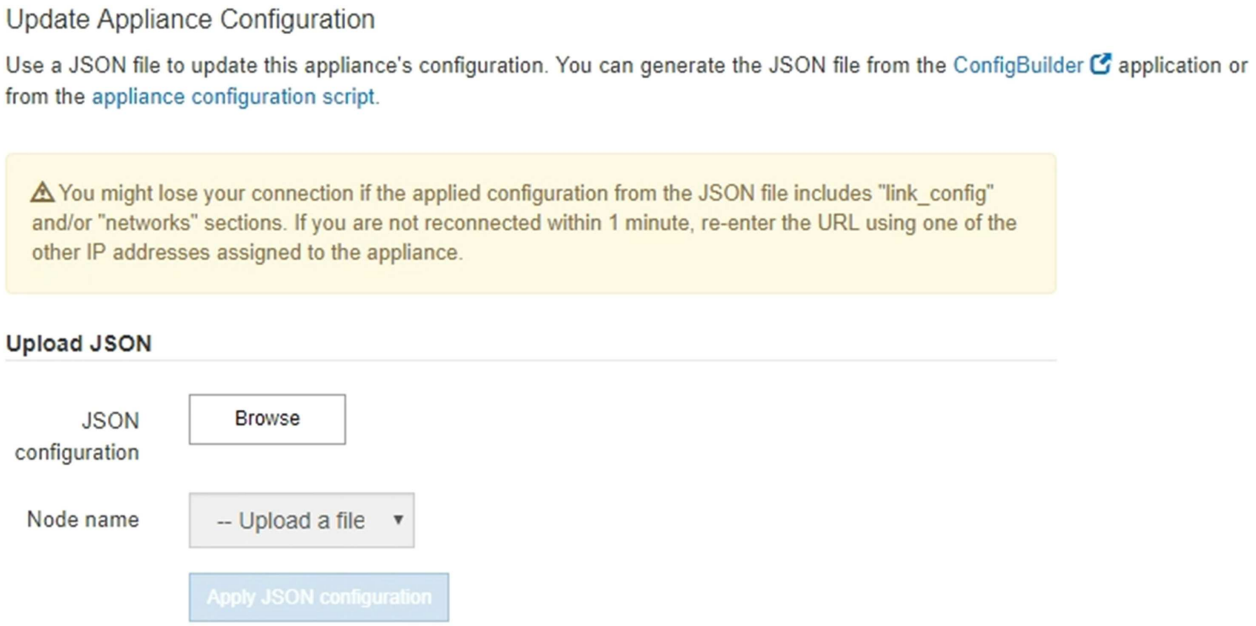
     Os nomes de nós no arquivo JSON devem seguir estes requisitos:

     - Deve ser um nome de host válido contendo pelo menos 1 e não mais de 32 carateres
     - Pode usar letras, números e hífens são permitidos
     - Não é possível iniciar ou terminar com um hífen ou conter apenas números

     > Certifique-se de que os nomes dos nós (os nomes de nível superior) no arquivo JSON sejam únicos, ou você não poderá configurar mais de um nó usando o arquivo JSON.

2. Selecione **Avançado Atualizar Configuração do dispositivo**.

   É apresentada a página Update Appliance Configuration (Atualizar configuração do dispositivo).



3. Selecione o arquivo JSON com a configuração que você deseja carregar.

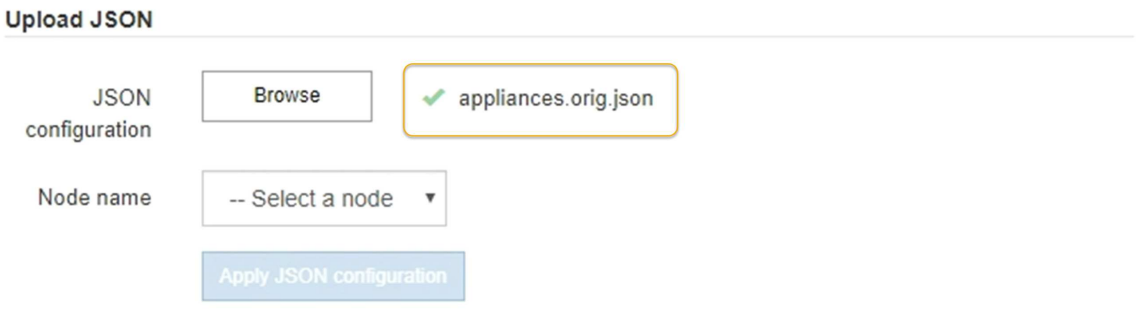
   a. Selecione **Procurar**.

   b. Localize e selecione o ficheiro.

   c. Selecione **Open**.

   O arquivo é carregado e validado. Quando o processo de validação estiver concluído, o nome do ficheiro é apresentado junto a uma marca de verificação verde.

   > Você pode perder a conexão com o dispositivo se a configuração do arquivo JSON incluir seções para "link_config", "redes" ou ambos. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do dispositivo usando um dos outros endereços IP atribuídos ao dispositivo.

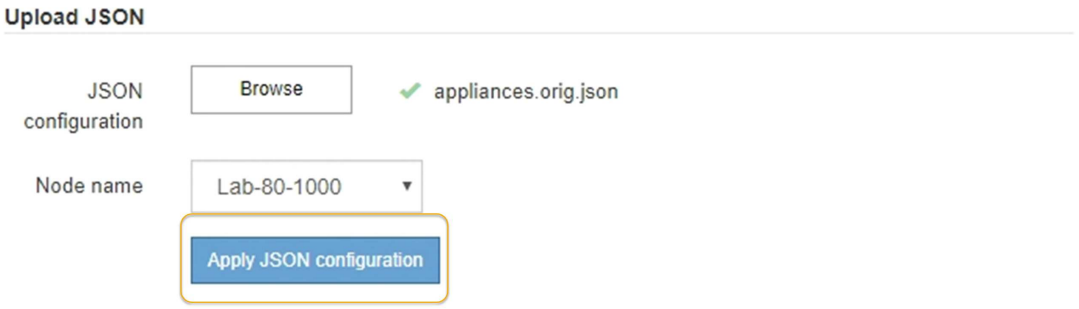


   A lista suspensa **Nome do nó** é preenchida com os nomes de nós de nível superior definidos no arquivo JSON.

Se o arquivo não for válido, o nome do arquivo será exibido em vermelho e uma mensagem de erro será exibida em um banner amarelo. O ficheiro inválido não é aplicado ao dispositivo. Você pode usar o ConfigBuilder para garantir que você tenha um arquivo JSON válido.

4. Selecione um nó na lista suspensa **Nome do nó**.

   O botão **Apply JSON Configuration** está ativado.



5. Selecione **Apply JSON Configuration**.

   A configuração é aplicada ao nó selecionado.

Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py

Você pode usar `configure-sga.py` o script para automatizar muitas das tarefas de instalação e configuração para os nós de dispositivos StorageGRID, incluindo a instalação e configuração de um nó de administrador principal. Este script pode ser útil se você tiver um grande número de dispositivos para configurar. Você também pode usar o script para gerar um arquivo JSON que contém informações de configuração do dispositivo.

O que você vai precisar

- O dispositivo foi instalado em um rack, conetado às redes e ligado.
- Links de rede e endereços IP foram configurados para o nó de administração principal usando o instalador do dispositivo StorageGRID.
- Se você estiver instalando o nó Admin principal, você saberá seu endereço IP.
- Se você estiver instalando e configurando outros nós, o nó Admin principal foi implantado e você sabe seu endereço IP.
- Para todos os nós que não o nó de administração principal, 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.
- Você baixou o `configure-sga.py` arquivo. O arquivo está incluído no arquivo de instalação, ou você pode acessá-lo clicando em **Ajuda Script de Instalação do dispositivo** no Instalador do StorageGRID Appliance.

Este procedimento é para usuários avançados com alguma experiência usando interfaces de linha de comando. Como alternativa, você também pode usar o Instalador de dispositivos StorageGRID para automatizar a configuração. E "Automatizando a configuração do dispositivo usando o Instalador de dispositivos StorageGRID"

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Para obter ajuda geral com a sintaxe do script e para ver uma lista dos parâmetros disponíveis, digite o seguinte:

```
configure-sga.py --help
```

O `configure-sga.py` script usa cinco subcomandos:

- `advanced` Para interações avançadas do StorageGRID Appliance, incluindo a configuração do BMC e a criação de um arquivo JSON contendo a configuração atual do dispositivo
- `configure` Para configurar o modo RAID, o nome do nó e os parâmetros de rede
- `install` Para iniciar uma instalação do StorageGRID
- `monitor` Para monitorar uma instalação do StorageGRID
- `reboot` para reiniciar o aparelho

Se você inserir um argumento de subcomando (avançado, configurar, instalar, monitorar ou reiniciar) seguido da `--help` opção, você receberá um texto de ajuda diferente fornecendo mais detalhes sobre as opções disponíveis dentro desse subcomando
`configure-sga.py` *`subcommand`* `--help`

3. Para confirmar a configuração atual do nó do dispositivo, digite o seguinte local *`SGA-install-ip`* onde está qualquer um dos endereços IP do nó do dispositivo
`configure-sga.py configure` *`SGA-INSTALL-IP`*

Os resultados mostram informações de IP atuais para o dispositivo, incluindo o endereço IP do nó de administração principal e informações sobre as redes de administração, grade e cliente.

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200
```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
             192.168.0.0/21
```

```
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

########################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
########################################################################
```

4. Se você precisar alterar qualquer um dos valores na configuração atual, use o `configure` subcomando para atualizá-los. Por exemplo, se você quiser alterar o endereço IP que o dispositivo usa para conexão com o nó Admin principal para `172.16.2.99`, digite o seguinte
`configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP`
5. Se você quiser fazer backup da configuração do appliance em um arquivo JSON, use os `advanced` subcomandos e `backup-file` . Por exemplo, se você quiser fazer backup da configuração de um dispositivo com endereço IP *SGA-INSTALL-IP* para um arquivo chamado `appliance-SG1000.json`, digite o seguinte
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

   O arquivo JSON contendo as informações de configuração é gravado no mesmo diretório do qual você executou o script.

   > Verifique se o nome do nó de nível superior no arquivo JSON gerado corresponde ao nome do dispositivo. Não faça alterações neste arquivo, a menos que você seja um usuário experiente e tenha uma compreensão completa das APIs do StorageGRID.

6. Quando estiver satisfeito com a configuração do aparelho, utilize os `install` subcomandos e `monitor` para instalar o aparelho
`configure-sga.py install --monitor SGA-INSTALL-IP`
7. Se pretender reiniciar o aparelho, introduza o seguinte
`configure-sga.py reboot SGA-INSTALL-IP`

Automatizando a configuração do StorageGRID

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

O que você vai precisar

- 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 amostra (`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
   ```

Depois de terminar

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, você precisa extrair o `Passwords.txt` arquivo e procurar 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.
```

Visão geral das APIs REST de instalação

O StorageGRID fornece duas APIs REST para executar tarefas de instalação: A API de instalação do StorageGRID e a API do instalador do dispositivo StorageGRID.

Ambas as APIs usam 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 (JavaScript Object Notation).

> Todas as operações de API que você executa usando a página da Web do API Docs 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 seu sistema StorageGRID e, caso precise 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.

API do instalador do dispositivo StorageGRID

A API do instalador do dispositivo StorageGRID pode ser acessada por HTTPS a partir `*Controller_IP*:8443`do .

Para acessar a documentação da API, vá para o Instalador do StorageGRID Appliance no appliance e selecione **Ajuda Documentação da API** na barra de menus.

A API do instalador do StorageGRID Appliance inclui as seguintes seções:

- **Clone** — operações para configurar e controlar a clonagem de nós.
- **Encryption** — operações para gerenciar a criptografia e visualizar o status da criptografia.
- **Configuração de hardware** — operações para configurar as configurações do sistema no hardware conetado.
- **Installation** — operações para iniciar a instalação do aparelho e para monitorar o status da instalação.
- **Networking** — operações relacionadas à configuração de rede, administrador e rede cliente para um dispositivo StorageGRID e configurações de porta de dispositivo.
- **Setup** — operações para ajudar na configuração inicial da instalação do dispositivo, incluindo solicitações para obter informações sobre o sistema e atualizar o IP do nó de administração principal.
- **Support** — operações para reiniciar o controlador e obter logs.
- **Upgrade** — operações relacionadas à atualização do firmware do appliance.
- * Uploadsg* — operações para upload de arquivos de instalação do StorageGRID.

Solução de problemas da instalação do hardware

Se você encontrar problemas durante a instalação, talvez seja útil revisar informações de solução de problemas relacionadas a problemas de configuração de hardware e

conetividade.

Informações relacionadas

"A configuração do hardware parece travar"

"Solução de problemas de conexão"

A configuração do hardware parece travar

O Instalador de dispositivos StorageGRID pode não estar disponível se falhas de hardware ou erros de cabeamento impedirem que a controladora E5600SG conclua seu processamento de inicialização.

Passos

1. Verifique o LED precisa de atenção em qualquer um dos controladores e procure um código de erro intermitente.

   Durante a inicialização, os LEDs Ação de Serviço permitida e Ação de Serviço necessária são ligados enquanto o hardware está sendo inicializado. O ponto decimal superior do dígito inferior, chamado de *LED de diagnóstico*, também se acende. O visor de sete segmentos percorre uma sequência de códigos comuns para ambos os controladores. Isso é normal e não é uma indicação de erro. Quando o hardware é inicializado com êxito, os LEDs de Ação de Serviço são desligados e os monitores são acionados pelo firmware.

2. Reveja os códigos no visor de sete segmentos para o controlador E5600SG.

   > A instalação e o provisionamento demoram. Algumas fases de instalação não relatam atualizações para o instalador do StorageGRID Appliance por vários minutos.

   Se ocorrer um erro, o visor de sete segmentos pisca uma sequência, COMO HE.

3. Para entender o que esses códigos significam, consulte os seguintes recursos:

Controlador	Referência
Controlador E5600SG	• "HE error: Erro ao sincronizar com o software SANtricity os" • "'E5600SG controlador de sete segmentos de códigos de exibição ""
Controlador E2700	Documentação do e-Series **Nota:** os códigos descritos para o controlador e-Series E5600 não se aplicam ao controlador E5600SG no aparelho.

4. Se isso não resolver o problema, entre em Contato com o suporte técnico.

Informações relacionadas

"E5600SG códigos de exibição de sete segmentos do controlador"

"Erro HE: Erro ao sincronizar com o software SANtricity os"

"E2700 Guia de instalação da bandeja de unidades e controlador relacionado"

"Documentação do NetApp: Série E2700"

Erro HE: Erro ao sincronizar com o software SANtricity os

A exibição de sete segmentos no controlador de computação mostra um código de erro HE se o Instalador de dispositivos StorageGRID não puder sincronizar com o software SANtricity os.

Sobre esta tarefa

Se for apresentado um código de erro HE, efetue esta ação corretiva.

Passos

1. Verifique a integridade dos dois cabos de interconexão SAS e confirme se estão bem conetados.
2. Se necessário, substitua um ou ambos os cabos e tente novamente.
3. Se isso não resolver o problema, entre em Contato com o suporte técnico.

Solução de problemas de conexão

Se você encontrar problemas de conexão durante a instalação do StorageGRID Appliance, execute as etapas de ação corretiva listadas.

Não foi possível ligar ao dispositivo StorageGRID através da rede

Se não conseguir ligar ao dispositivo, poderá haver um problema de rede ou a instalação do hardware poderá não ter sido concluída com êxito.

- **Emissão**

  Não pode ligar ao aparelho.

- **Causa**

  Isso pode ocorrer se houver um problema de rede ou se a instalação do hardware não tiver sido concluída com êxito.

- **Ações corretivas**

  a. Faça ping ao aparelho
  `ping E5600_controller_IP`

  b. Acesse o Instalador do StorageGRID Appliance abrindo um navegador e inserindo o seguinte
  `https://Management_Port_IP:8443`

  Para Management_Port_IP, insira o endereço IP da porta de gerenciamento 1 no controlador E5600SG (provisionado durante a instalação física).

  c. Clique em **Configurar rede Admin** e verifique o IP.

  d. Se você receber uma resposta do ping, verifique se a porta 8443 está aberta nos firewalls.

e. Reinicie o aparelho.

f. Atualize a página da Web de instalação.

g. Se isso não resolver o problema de conexão, entre em Contato com o suporte técnico do site de suporte da NetApp em "mysupport.NetApp.com".

Informações relacionadas

"E5600SG códigos de exibição de sete segmentos do controlador"

Reinicializando o controlador enquanto o Instalador de dispositivos StorageGRID está em execução

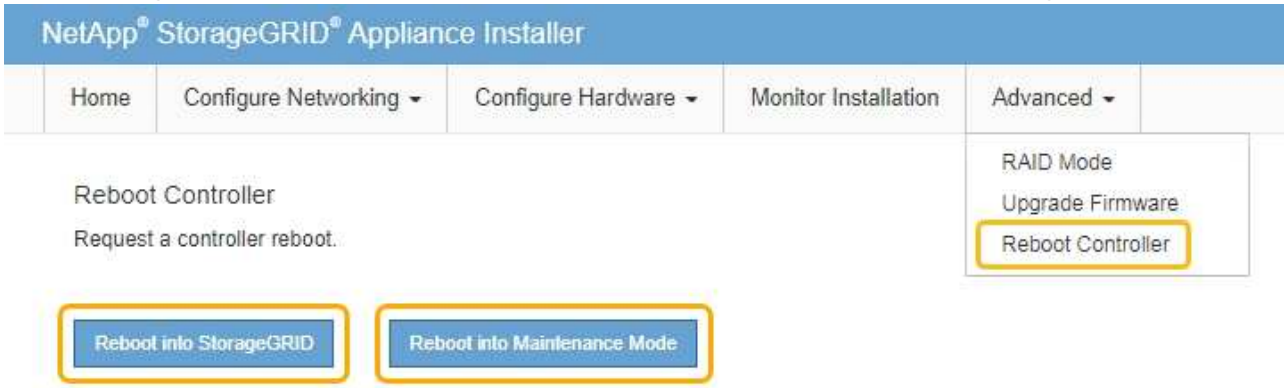
Talvez seja necessário reiniciar o controlador de computação enquanto o Instalador de dispositivos StorageGRID estiver em execução. Por exemplo, você pode precisar reiniciar o controlador se a instalação falhar.

Sobre esta tarefa

Este procedimento só se aplica quando o controlador de computação está executando o Instalador de dispositivos StorageGRID. Depois que a instalação estiver concluída, esta etapa não funcionará mais porque o Instalador de dispositivos StorageGRID não está mais disponível.

Passos

1. No Instalador do StorageGRID Appliance, clique em **Avançado controlador de reinicialização** e selecione uma destas opções:
   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



O controlador SG6000-CN é reinicializado.

Manutenção do aparelho SG5600

Talvez seja necessário atualizar o software SANtricity os na controladora E2700, substituir a controladora E2700 ou a controladora E5600SG ou substituir componentes

específicos. Os procedimentos nesta seção pressupõem que o dispositivo já foi implantado como nó de storage em um sistema StorageGRID.

Passos

- "Colocar um aparelho no modo de manutenção"
- "Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade"
- "Atualizando o SANtricity os no controlador E2700 usando o modo de manutenção"
- "Atualizando o firmware da unidade usando o SANtricity Storage Manager"
- "Substituição do controlador E2700"
- "Substituição do controlador E5600SG"
- "Substituição de outros componentes de hardware"
- "Alterar a configuração do link do controlador E5600SG"
- "Alterar a definição MTU"
- "Verificar a configuração do servidor DNS"
- "Monitorização da encriptação do nó no modo de manutenção"

Colocar um aparelho no modo de manutenção

Deve colocar o aparelho no modo de manutenção antes de efetuar procedimentos de manutenção específicos.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

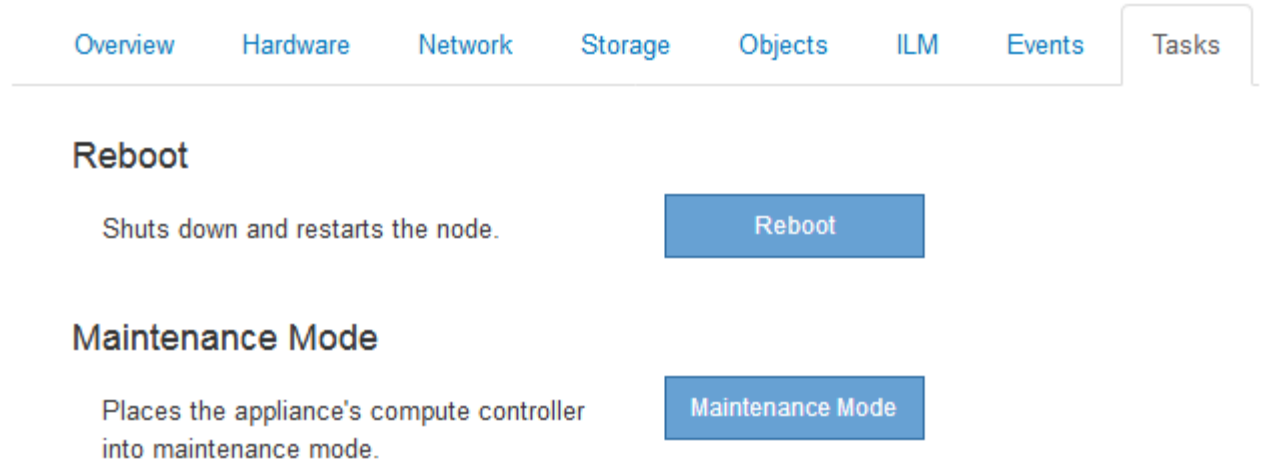
Sobre esta tarefa

Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

> ⓘ A senha e a chave de host de um dispositivo StorageGRID no modo de manutenção permanecem as mesmas que eram quando o aparelho estava em serviço.

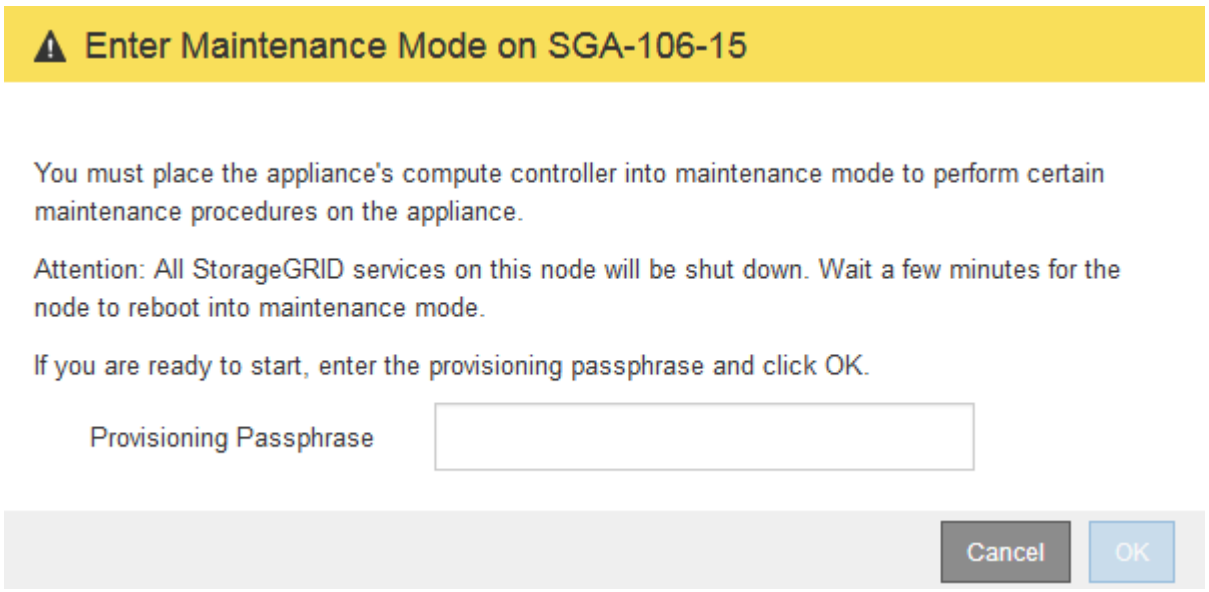
Passos

1. No Gerenciador de Grade, selecione **nós**.
2. Na exibição em árvore da página nós, selecione o nó de storage do dispositivo.
3. Selecione **tarefas**.



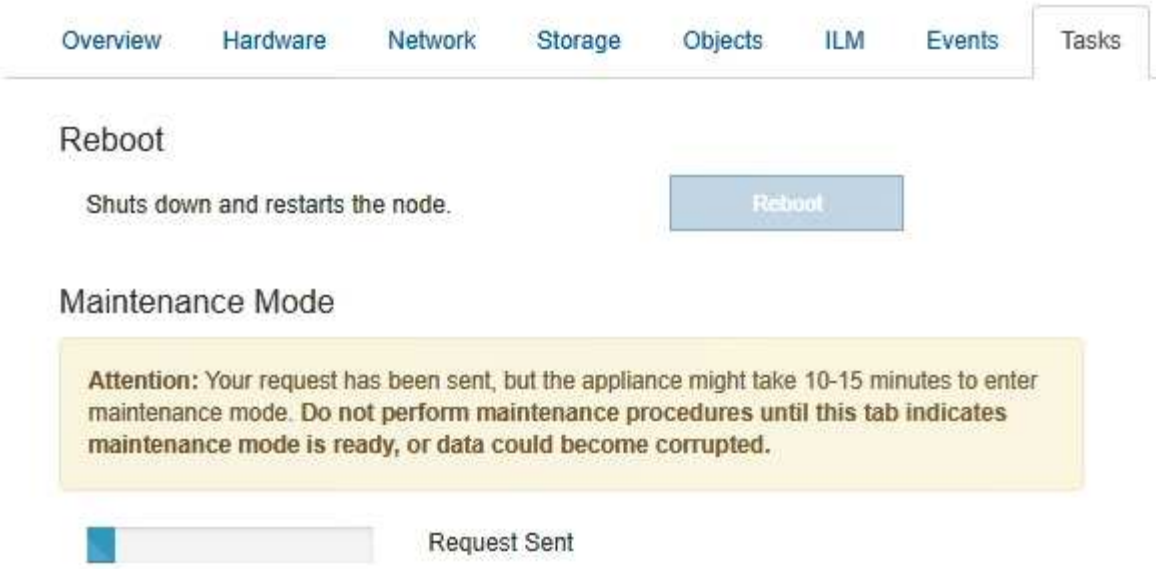
4. Selecione **Maintenance Mode** (modo de manutenção).

   É apresentada uma caixa de diálogo de confirmação.

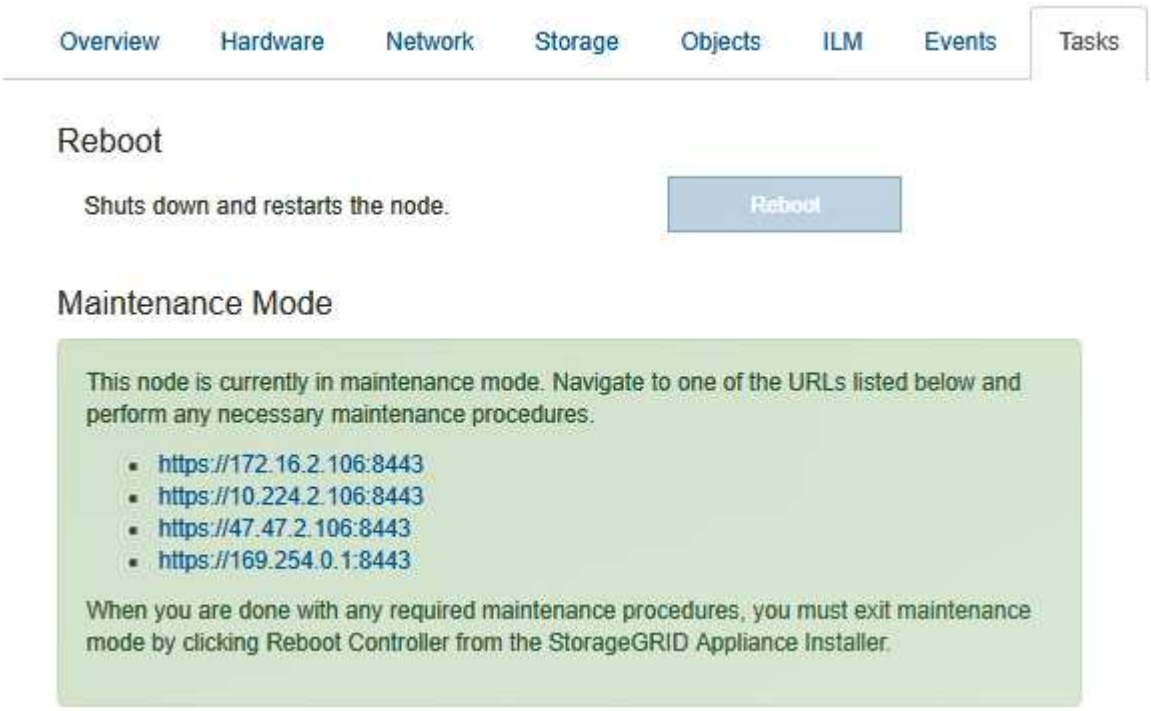


5. Introduza a frase-passe de aprovisionamento e selecione **OK**.

   Uma barra de progresso e uma série de mensagens, incluindo "Request Sent" (pedido enviado), "Stop" (Paragem de StorageGRID) e "Reboot" (reinício), indicam que o aparelho está a concluir os passos para entrar no modo de manutenção.



Quando o dispositivo está no modo de manutenção, uma mensagem de confirmação lista os URLs que você pode usar para acessar o Instalador do StorageGRID Appliance.



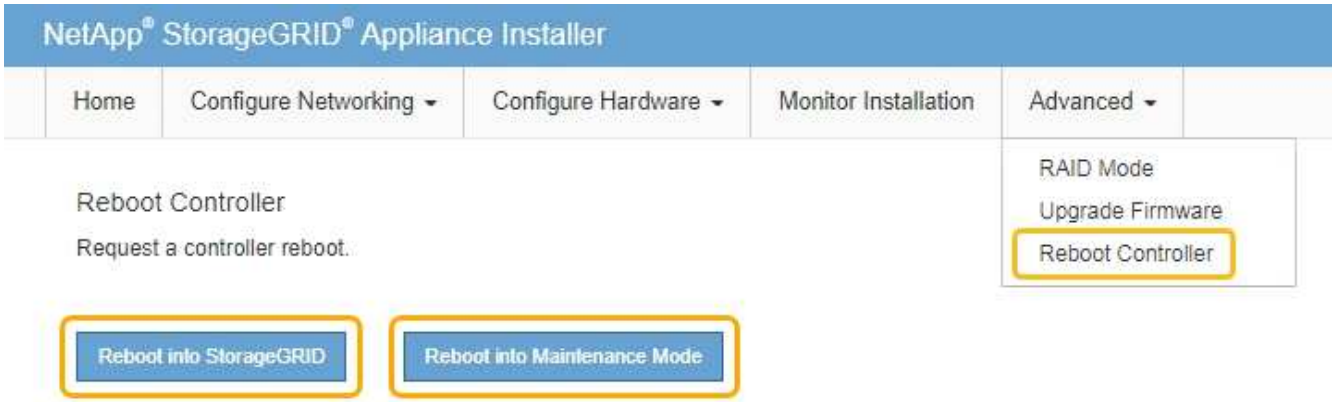
6. Para acessar o Instalador do StorageGRID Appliance, navegue até qualquer um dos URLs exibidos.

   Se possível, use o URL que contém o endereço IP da porta Admin Network do dispositivo.

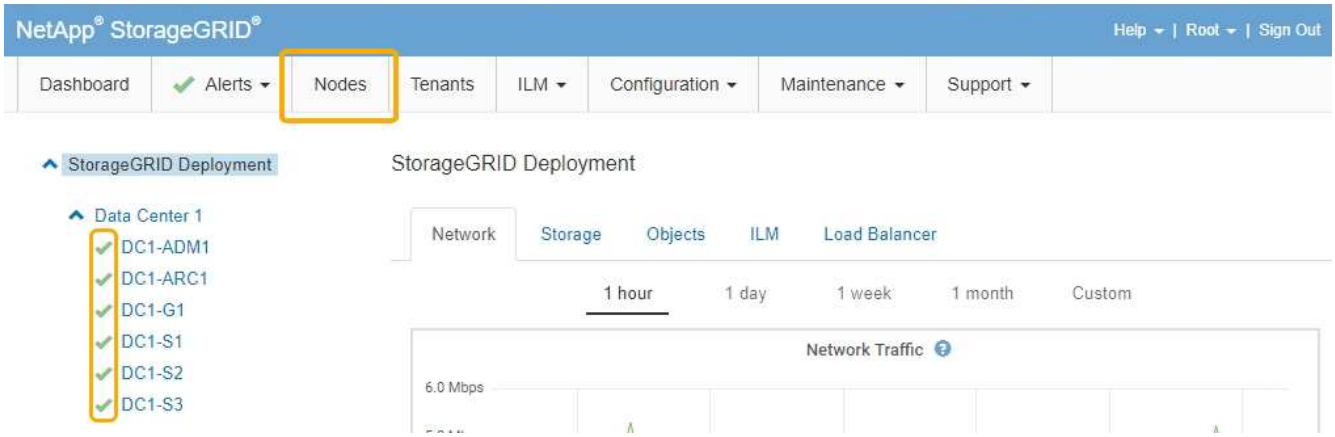
   > O acesso `https://169.254.0.1:8443` requer uma conexão direta com a porta de gerenciamento local.

7. A partir do instalador do dispositivo StorageGRID, confirme se o aparelho está no modo de manutenção.

8. Execute todas as tarefas de manutenção necessárias.
9. Depois de concluir as tarefas de manutenção, saia do modo de manutenção e retome a operação normal do nó. No Instalador de dispositivos StorageGRID, selecione **Avançado controlador de reinicialização** e, em seguida, selecione **Reiniciar no StorageGRID**.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade

Use o Gerenciador de Grade para aplicar uma atualização do SANtricity os.

O que você vai precisar

- Você consultou a ferramenta de Matriz de interoperabilidade (IMT) do NetApp para confirmar que a versão do SANtricity os que você está usando para a atualização é compatível com o seu dispositivo.
- Tem de ter a permissão Manutenção.

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a senha de provisionamento.
- Você deve ter acesso à página de downloads do NetApp para o SANtricity os.

Sobre esta tarefa

Não é possível executar outras atualizações de software (atualização de software StorageGRID ou hotfix) até concluir o processo de atualização do SANtricity os. Se você tentar iniciar um hotfix ou uma atualização de software StorageGRID antes do processo de atualização do SANtricity os terminar, você será redirecionado para a página de atualização do SANtricity os.

O procedimento não será concluído até que a atualização do SANtricity os tenha sido aplicada com êxito a todos os nós aplicáveis. Pode levar mais de 30 minutos para carregar o SANtricity os em cada nó e até 90 minutos para reinicializar cada dispositivo de storage StorageGRID.

As etapas a seguir são aplicáveis somente quando você estiver usando o Gerenciador de Grade para executar a atualização.

Este procedimento atualizará automaticamente a NVSRAM para a versão mais recente associada à atualização do sistema operacional SANtricity. Não é necessário aplicar um ficheiro de atualização NVSRAM separado.

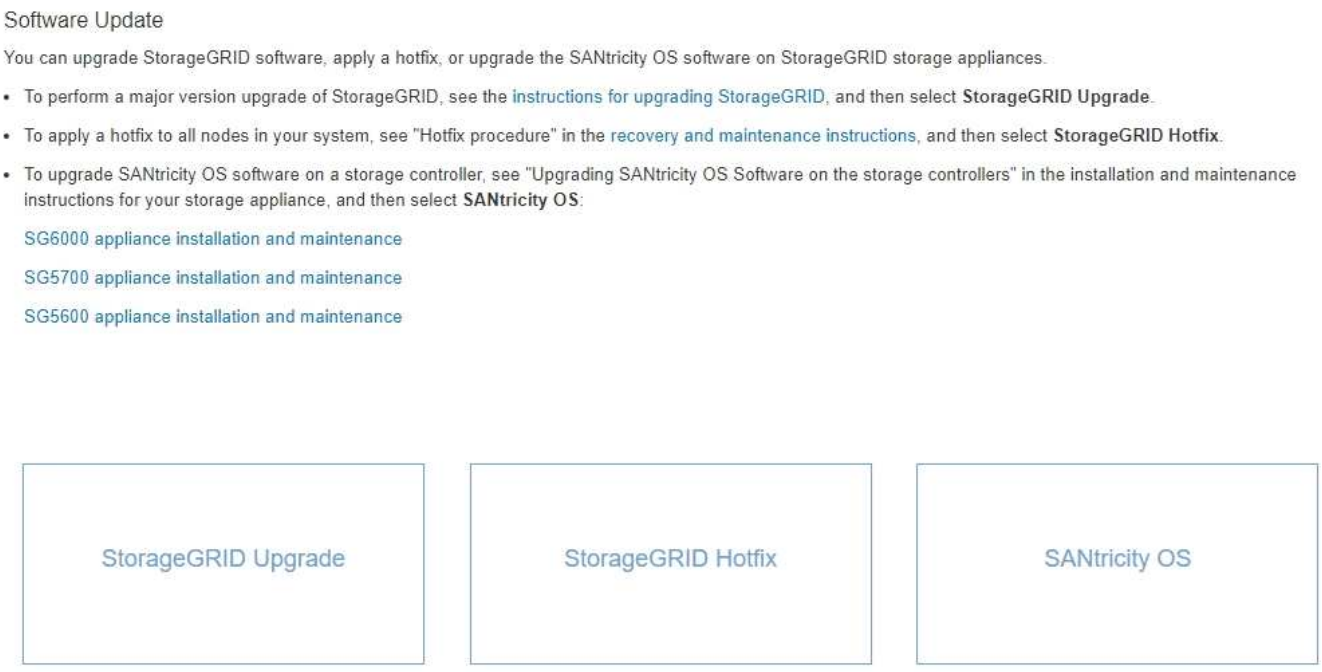
Passos

1. A partir de um portátil de serviço, transfira o novo ficheiro SANtricity os a partir do site de suporte da NetApp.

   Certifique-se de escolher a versão do SANtricity os para o controlador de storage E2700.

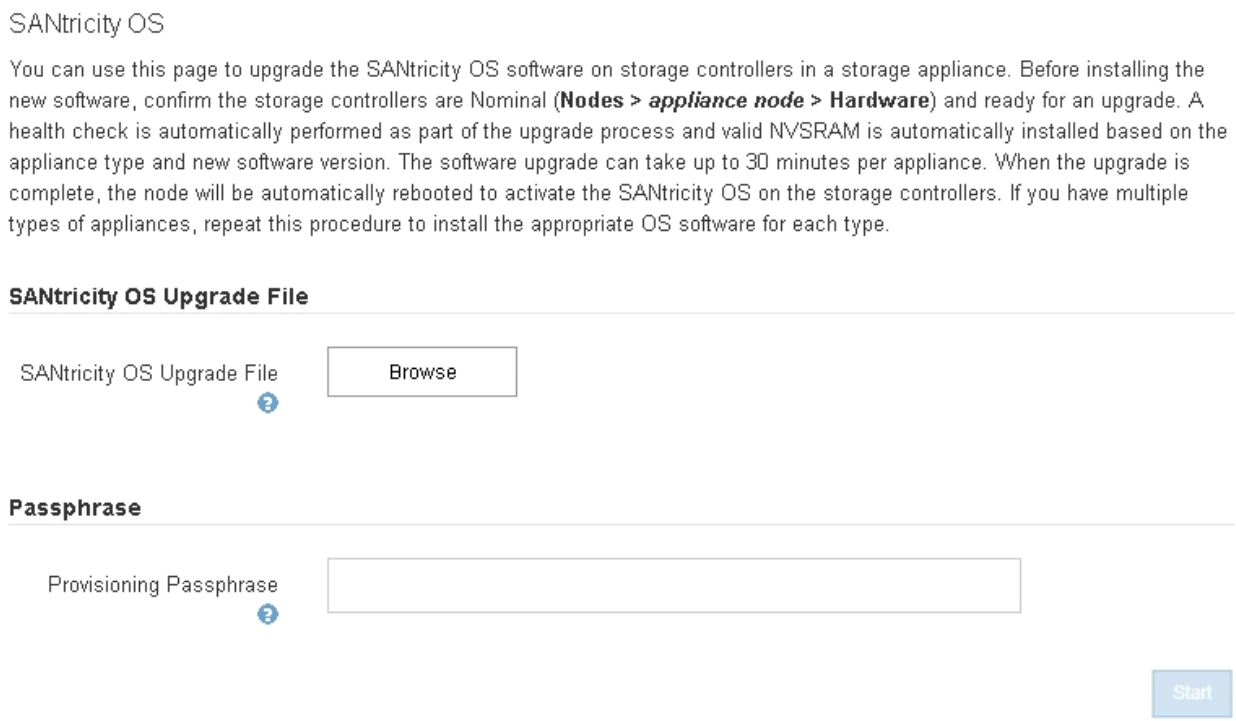
2. Faça login no Gerenciador de Grade usando um navegador compatível.
3. Selecione **Manutenção**. Em seguida, na seção sistema do menu, selecione **Atualização de software**.

   A página Atualização de software é exibida.



4. Clique em **SANtricity os**.

   A página do SANtricity os é exibida.



5. Selecione o arquivo de atualização do SANtricity os que você baixou no site de suporte do NetApp.

   a. Clique em **Procurar**.
   b. Localize e selecione o ficheiro.
   c. Clique em **abrir**.

      O arquivo é carregado e validado. Quando o processo de validação é concluído, o nome do arquivo é mostrado no campo Detalhes.

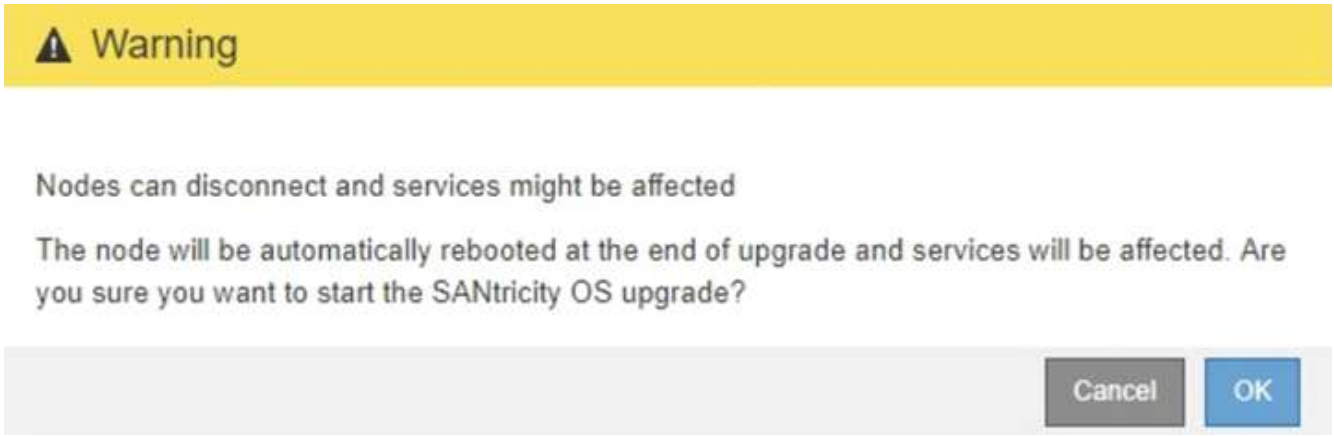
      Não altere o nome do arquivo, pois ele faz parte do processo de verificação.

6. Introduza a frase-passe de aprovisionamento.

   O botão **Start** está ativado.

7. Clique em **Iniciar**.

Uma caixa de aviso aparece informando que a conexão do seu navegador pode ser perdida temporariamente à medida que os serviços nos nós atualizados são reiniciados.



8. Clique em **OK** para colocar o arquivo de atualização do SANtricity os no nó de administração principal.

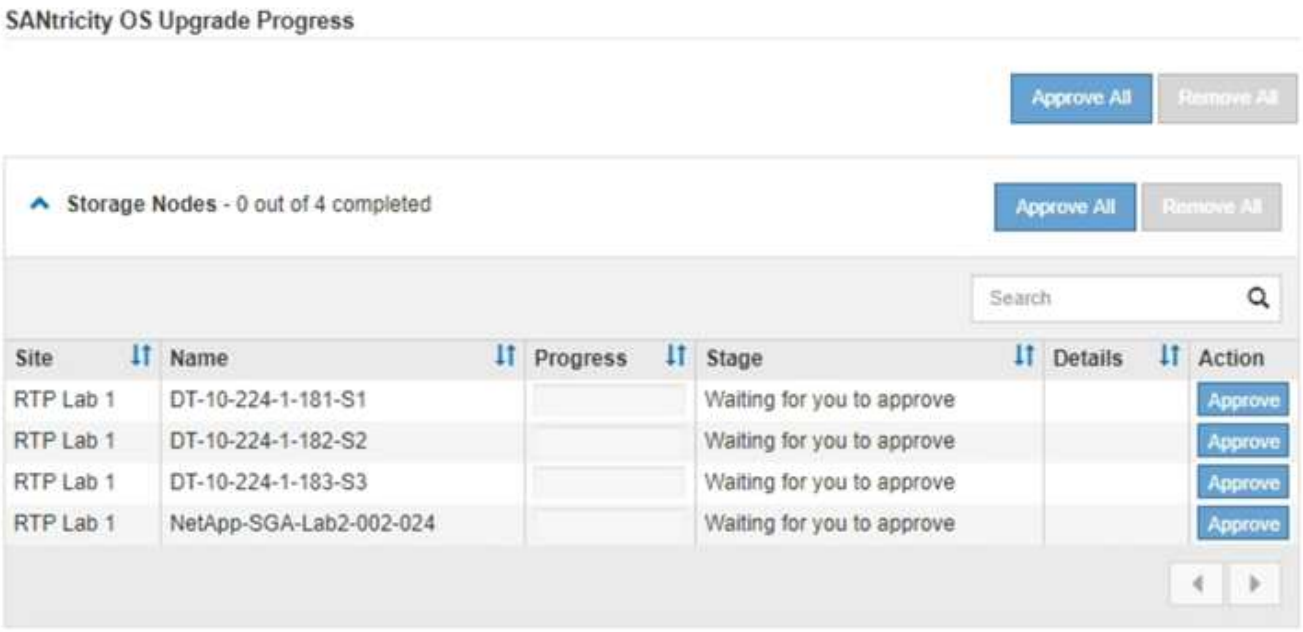
   Quando a atualização do SANtricity os é iniciada:

   a. A verificação de integridade é executada. Esse processo verifica se nenhum nó tem o status de precisa de atenção.

      Se algum erro for relatado, resolva-os e clique em **Start** novamente.

   b. A tabela de progresso da atualização do SANtricity os é exibida. Esta tabela mostra todos os nós de storage na grade e a etapa atual da atualização para cada nó.

      A tabela mostra todos os nós de storage, incluindo nós de storage baseados em software. Você precisa aprovar a atualização para todos os nós de storage, mesmo que uma atualização do SANtricity os não afete os nós de storage baseados em software. A mensagem de atualização retornada para nós de storage baseados em software é "a atualização do SANtricity os não se aplica a este nó."



9. Opcionalmente, classifique a lista de nós em ordem crescente ou decrescente por **Site**, **Nome**, **progresso**, **Estágio** ou **Detalhes**. Ou insira um termo na caixa **pesquisar** para pesquisar nós específicos.

   Você pode rolar pela lista de nós usando as setas esquerda e direita no canto inferior direito da seção.

10. Aprove os nós de grade que você está pronto para adicionar à fila de atualização. Nós aprovados do mesmo tipo são atualizados um de cada vez.

    > Não aprove a atualização do SANtricity os para um nó de armazenamento de dispositivo, a menos que você tenha certeza de que o nó está pronto para ser interrompido e reinicializado.quando a atualização do SANtricity os for aprovada em um nó, os serviços nesse nó são interrompidos. Mais tarde, quando o nó é atualizado, o nó do appliance é reinicializado. Essas operações podem causar interrupções de serviço para clientes que estão se comunicando com o nó.

    - Clique em um dos botões **Approve All** para adicionar todos os nós de armazenamento à fila de atualização do SANtricity os.

      > 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).

    - Clique em um ou mais botões **Approve** para adicionar um ou mais nós à fila de atualização do SANtricity os.

      > Você pode atrasar a aplicação de uma atualização do SANtricity os a um nó, mas o processo de atualização do SANtricity os não será concluído até que você aprove a atualização do SANtricity os em todos os nós de armazenamento listados.

      Depois de clicar em **Approve**, o processo de atualização determina se o nó pode ser atualizado. Se um nó puder ser atualizado, ele será adicionado à fila de atualização. E

      Para alguns nós, o arquivo de atualização selecionado não é aplicado intencionalmente e você pode concluir o processo de atualização sem atualizar esses nós específicos. Para nós intencionalmente não atualizados, o processo mostrará o estágio completo com uma das seguintes mensagens na coluna Detalhes

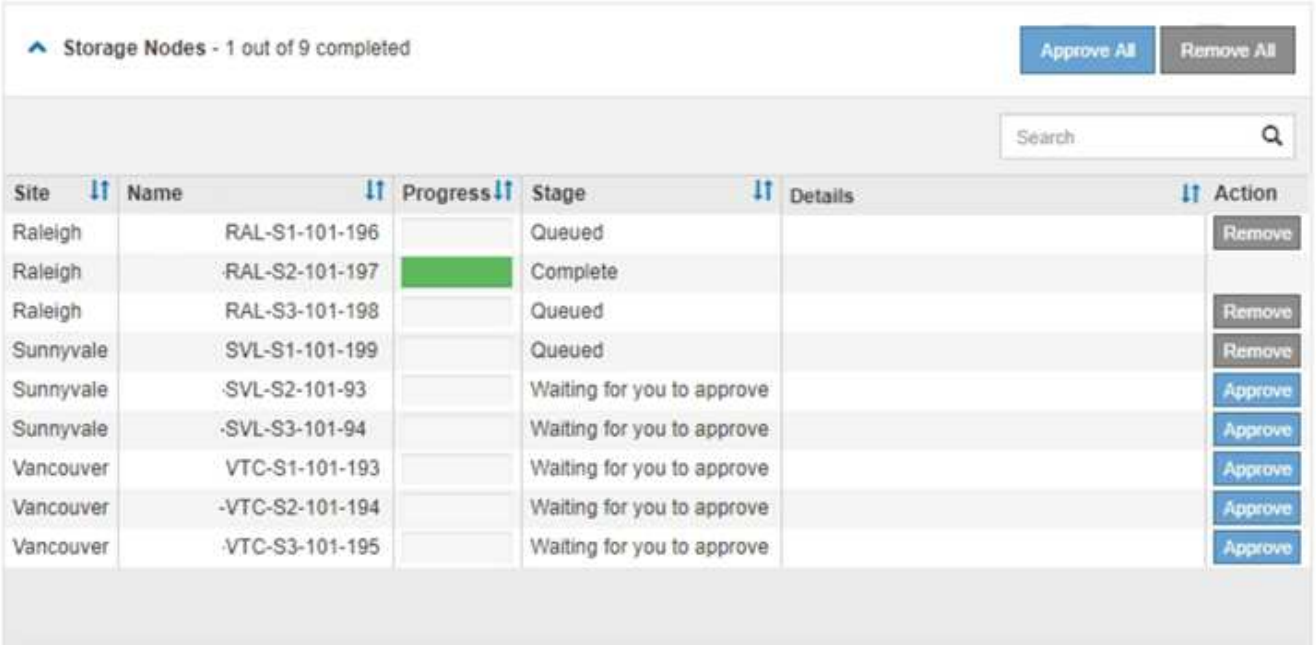
      - O nó de storage já foi atualizado.
      - A atualização do SANtricity os não é aplicável a este nó.
      - O ficheiro SANtricity os não é compatível com este nó.

    A mensagem "'SANtricity os upgrade não é aplicável a este nó'" indica que o nó não tem um controlador de armazenamento que pode ser gerenciado pelo sistema StorageGRID. Essa mensagem será exibida para nós de storage que não sejam do dispositivo. Você pode concluir o processo de atualização do SANtricity os sem atualizar o nó exibindo esta mensagem. A mensagem "'arquivo SANtricity os não é compatível com este nó'" indica que o nó requer um arquivo SANtricity os diferente daquele que o processo está tentando instalar. Depois de concluir a atualização atual do SANtricity os, baixe o SANtricity os apropriado para o nó e repita o processo de atualização.

11. Se você precisar remover um nó ou todos os nós da fila de atualização do SANtricity os, clique em **Remover** ou **Remover tudo**.

    Como mostrado no exemplo, quando o estágio avança além da fila, o botão **Remover** fica oculto e você

não pode mais remover o nó do processo de atualização do SANtricity os.



12. Aguarde enquanto a atualização do SANtricity os é aplicada a cada nó de grade aprovado.

> Se algum nó mostrar um estágio de erro enquanto a atualização do SANtricity os está sendo aplicada, a atualização falhou para esse nó. Pode ser necessário colocar o aparelho no modo de manutenção para recuperar da falha. Contacte o suporte técnico antes de continuar.

Se o firmware no nó é muito antigo para ser atualizado com o Gerenciador de Grade, o nó mostra um estágio de erro com os detalhes: "'você deve usar o modo de manutenção para atualizar o SANtricity os neste nó. Consulte as instruções de instalação e manutenção do seu aparelho. Após a atualização, você pode usar este utilitário para futuras atualizações." para resolver o erro, faça o seguinte:

a. Use o modo de manutenção para atualizar o SANtricity os no nó que mostra um estágio de erro.
b. Use o Gerenciador de Grade para reiniciar e concluir a atualização do SANtricity os.

   Quando a atualização do SANtricity os é concluída em todos os nós aprovados, a tabela de progresso da atualização do SANtricity os fecha e um banner verde mostra a data e a hora em que a atualização do SANtricity os foi concluída.

13. Repita este procedimento de atualização para todos os nós com um estágio de conclusão que exigem um

arquivo de atualização diferente do SANtricity os.

> Para todos os nós com um status de precisa de atenção, use o modo de manutenção para executar a atualização.

Informações relacionadas

"Atualizando o SANtricity os no controlador E2700 usando o modo de manutenção"

Atualizando o SANtricity os no controlador E2700 usando o modo de manutenção

Se você não conseguir atualizar o software SANtricity os usando o Gerenciador de Grade, use o procedimento de modo de manutenção para aplicar a atualização.

O que você vai precisar

- Você consultou a ferramenta de Matriz de interoperabilidade (IMT) do NetApp para confirmar que a versão do SANtricity os que você está usando para a atualização é compatível com o seu dispositivo.
- Você deve colocar o controlador E5600SG no modo de manutenção se não estiver usando o Gerenciador de Grade. Colocar o controlador no modo de manutenção interrompe a ligação ao controlador E2700. Antes de alterar a configuração da ligação, tem de colocar o controlador E5600SG no modo de manutenção. Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

  "Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Não atualize o SANtricity os ou a NVSRAM na controladora e-Series em mais de um dispositivo StorageGRID de cada vez.

> A atualização de mais de um dispositivo StorageGRID por vez pode causar indisponibilidade de dados, dependendo do modelo de implantação e das políticas de ILM.

Passos

1. A partir de um laptop de serviço, acesse o SANtricity Storage Manager e entre.
2. Transfira o novo ficheiro de software SANtricity os e o ficheiro NVSRAM para o cliente de gestão.

   > A NVSRAM é específica do dispositivo StorageGRID. Não utilize a transferência NVSRAM padrão.

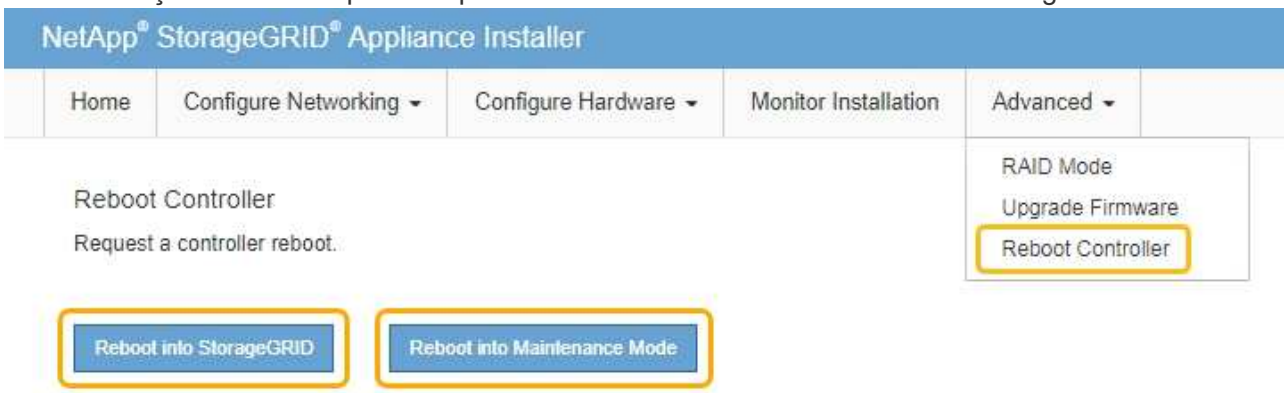
3. Siga as instruções nas instruções de atualização de software e firmware do SANtricity *E2700 e E5600* ou na ajuda on-line do SANtricity Storage Manager e atualize o firmware, NVSRAM ou ambos da controladora E2700.

   > Se você precisar atualizar a NVSRAM na controladora E2700, confirme se o arquivo SANtricity os baixado foi designado como compatível com os dispositivos StorageGRID.

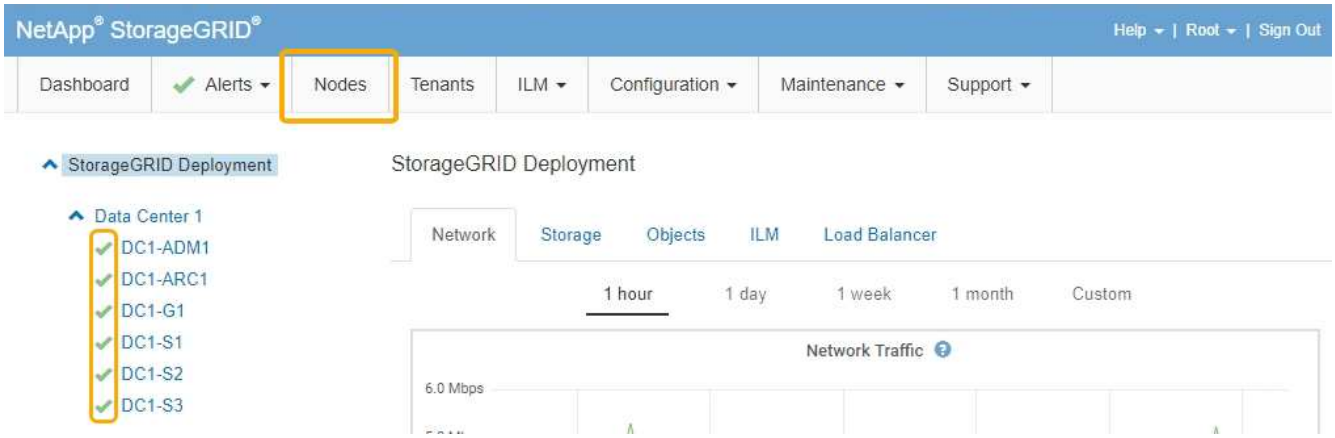
   > Ative os arquivos de atualização imediatamente. Não adiar a ativação.

4. Uma vez concluída a operação de atualização, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

- Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
- Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Atualizando o firmware da unidade usando o SANtricity Storage Manager

Você atualiza o firmware da sua unidade para garantir que você tenha todos os recursos mais recentes e correções de bugs.

O que você vai precisar

- O dispositivo de armazenamento tem um status ideal.
- Todas as unidades têm um status ideal.
- Você tem a versão mais recente do SANtricity Storage Manager instalada que é compatível com sua versão do StorageGRID.

"Atualizando o SANtricity os nos controladores de storage usando o Gerenciador de Grade"

"Atualizando o SANtricity os no controlador E2700 usando o modo de manutenção"

- Colocou o aparelho StorageGRID no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

> O modo de manutenção interrompe a conexão com o controlador de storage, interrompendo todas as atividades de e/S e colocando todas as unidades offline.

> Não atualize o firmware da unidade em mais de um dispositivo StorageGRID de cada vez. Isso pode causar indisponibilidade de dados, dependendo do modelo de implantação e das políticas de ILM.

Passos

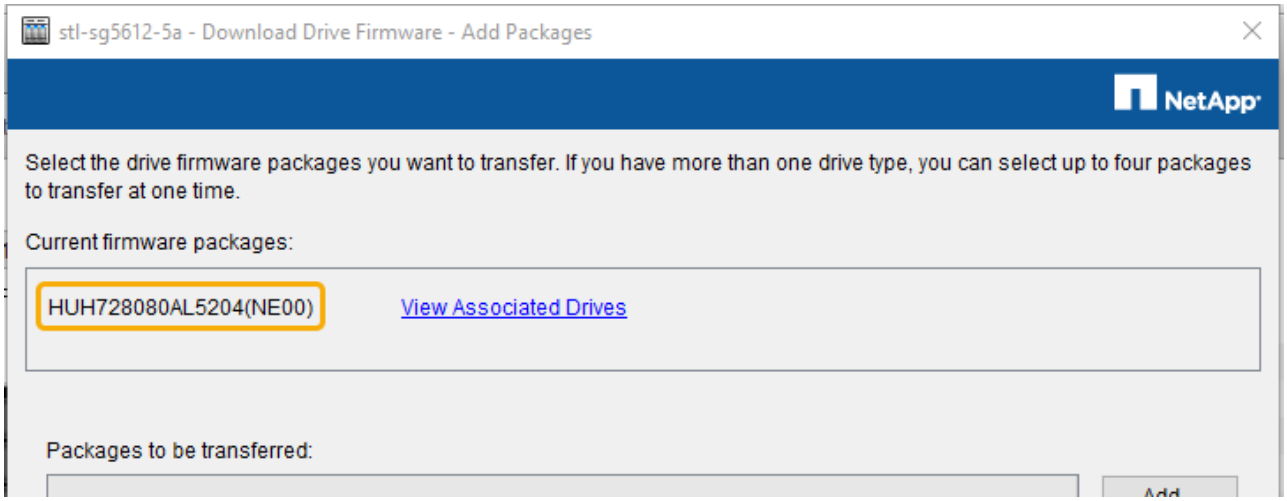
1. Abra um navegador da Web e insira o endereço IP como o URL do SANtricity Storage Manager
   `https://E2700_Controller_IP`
2. Introduza o nome de utilizador e a palavra-passe do administrador do SANtricity Storage Manager, se necessário.
3. No Gerenciamento Empresarial do SANtricity, selecione a guia **dispositivos**.

   A janela Gerenciamento de matrizes SANtricity é aberta.
4. No gerenciamento de storage SANtricity, clique duas vezes no storage array com as unidades a serem atualizadas.
5. Verifique se o storage de armazenamento e as unidades têm um status ideal.
6. Verifique a versão do firmware da unidade atualmente instalada no dispositivo de armazenamento:

   a. Em Gerenciamento Empresarial SANtricity, selecione **Upgrade Drive firmware**.

      A janela Download Drive firmware - Add Packages (Transferir firmware da unidade - Adicionar pacotes) apresenta os ficheiros de firmware da unidade atualmente em utilização.

   b. Observe as revisões atuais do firmware da unidade e identificadores de unidade nos pacotes de firmware atuais.



   Neste exemplo:

- A revisão do firmware da unidade é **NE00**.
- O identificador da unidade é **HUH728080AL5204**.

Selecione **Exibir unidades associadas** para exibir onde essas unidades estão instaladas no seu dispositivo de armazenamento.

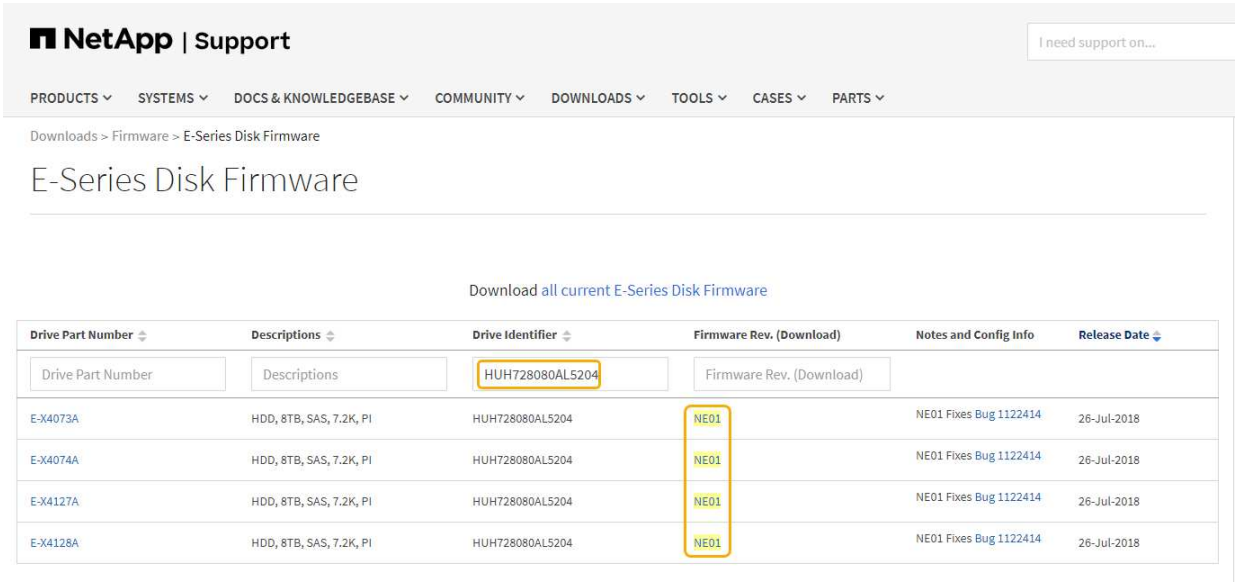
7. Transfira e prepare a atualização de firmware da unidade disponível:
   a. Abra seu navegador da Web, navegue até o site de suporte da NetApp e faça login usando sua ID e senha.

      "Suporte à NetApp"

   b. No site de suporte da NetApp, selecione a guia **Downloads** e, em seguida, selecione **firmware da unidade de disco da série e**.

      É apresentada a página firmware do disco e-Series.

   c. Procure cada **Drive Identifier** instalado no seu dispositivo de armazenamento e verifique se cada identificador de unidade tem a revisão de firmware mais recente.
      - Se a revisão do firmware não for um link, esse identificador de unidade terá a revisão de firmware mais recente.
      - Se um ou mais números de peça de unidade forem listados para um identificador de unidade, uma atualização de firmware estará disponível para essas unidades. Pode selecionar qualquer ligação para transferir o ficheiro de firmware.



   d. Se estiver listada uma revisão de firmware posterior, selecione o link na coluna firmware Rev. (Download) para baixar um `.zip` arquivo contendo o arquivo de firmware.

   e. Extraia (descompacte) os arquivos de arquivo de firmware da unidade que você baixou do site de suporte.

8. Instale a atualização do firmware da unidade:

   a. Na janela SANtricity Storage Manager Download Drive firmware - Add Packages (Baixar firmware da unidade - Adicionar pacotes), selecione **Add** (Adicionar).

   b. Navegue até o diretório que contém os arquivos de firmware e selecione até quatro arquivos de firmware.

Os arquivos de firmware da unidade têm um nome de arquivo semelhante a `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`

Selecionar mais de um ficheiro de firmware para atualizar o firmware da mesma unidade pode resultar num erro de conflito de ficheiros. Se ocorrer um erro de conflito de arquivo, uma caixa de diálogo de erro será exibida. Para resolver esse erro, selecione **OK** e remova todos os outros arquivos de firmware, exceto aquele que você deseja usar para atualizar o firmware da unidade. Para remover um arquivo de firmware, selecione o arquivo de firmware na área de informações Pacotes a serem transferidos e selecione **Remover**. Além disso, você só pode selecionar até quatro pacotes de firmware de unidade de uma só vez.

c. Selecione **OK**.

O sistema atualiza a área de informações Pacotes a serem transferidos com os arquivos de firmware selecionados.

d. Selecione **seguinte**.

Abre-se a janela Download Drive firmware - Select Drives (Transferir firmware da unidade - Selecionar unidades).

- Todas as unidades do dispositivo são digitalizadas para obter informações de configuração e elegibilidade de atualização.
- É-lhe apresentada uma seleção (dependendo da variedade de unidades que tem na matriz de armazenamento) de unidades compatíveis que podem ser atualizadas com o firmware selecionado. As unidades capazes de ser atualizadas como uma operação on-line são exibidas por padrão.
- O firmware selecionado para a unidade aparece na área de informações de firmware proposto. Se for necessário alterar o firmware, selecione **voltar** para retornar à caixa de diálogo anterior.

e. Na capacidade de atualização da unidade, selecione a operação de download **Parallel** ou **All**.

Você pode usar qualquer um desses métodos de atualização porque o dispositivo está no modo de manutenção, onde a atividade de e/S é interrompida para todas as unidades e todos os volumes.

f. Em unidades compatíveis, selecione as unidades para as quais pretende atualizar os ficheiros de firmware selecionados.

- Para uma ou mais unidades, selecione cada unidade que deseja atualizar.
- Para todas as unidades compatíveis, selecione **Selecionar tudo**.

  A prática recomendada é atualizar todas as unidades do mesmo modelo para a mesma revisão de firmware.

g. Selecione **Finish**; em seguida, digite `yes` e selecione **OK**.

- O download e a atualização do firmware da unidade começam, com Download Drive firmware - progresso indicando o status da transferência de firmware para todas as unidades.
- O status de cada unidade que participa da atualização é exibido na coluna progresso da transferência de dispositivos atualizados.

  Uma operação de atualização de firmware de unidade paralela pode levar até 90 segundos para ser concluída se todas as unidades forem atualizadas em um sistema de 24 unidades. Em um sistema maior, o tempo de execução é um pouco mais longo.

h. Durante o processo de atualização do firmware, você pode

- Selecione **Stop** para interromper a atualização de firmware em andamento. Qualquer atualização de firmware atualmente em curso está concluída. Quaisquer unidades que tenham tentado atualizar o firmware mostram seu status individual. Quaisquer unidades restantes são listadas com um estado de não tentativa.

> Parar a atualização do firmware da unidade em processo pode resultar em perda de dados ou unidades indisponíveis.

- Selecione **Save as** (Guardar como) para guardar um relatório de texto do resumo do progresso da atualização do firmware. O relatório é salvo com uma extensão de arquivo .log padrão. Se você quiser alterar a extensão ou diretório do arquivo, altere os parâmetros em Salvar Registro de download da unidade.

i. Use Download Drive firmware - Progress para monitorar o progresso das atualizações de firmware da unidade. A área unidades atualizadas contém uma lista de unidades agendadas para atualização de firmware e o status de transferência de cada unidade de download e atualização.

O progresso e o status de cada unidade que está participando da atualização são exibidos na coluna progresso da transferência. Tome a ação recomendada apropriada se ocorrerem erros durante a atualização.

- **Pendente**

Este estado é apresentado para uma operação de transferência de firmware online que foi agendada mas ainda não foi iniciada.

- **Em andamento**

O firmware está a ser transferido para a unidade.

- **Reconstrução em andamento**

Este estado é apresentado se ocorrer uma transferência de volume durante a reconstrução rápida de uma unidade. Isto é normalmente devido a uma reinicialização ou falha do controlador e o proprietário do controlador transfere o volume.

O sistema iniciará uma reconstrução completa da unidade.

◦ **Falhou - parcial**

O firmware só foi parcialmente transferido para a unidade antes de um problema impedir que o resto do arquivo fosse transferido.

◦ **Falhou - estado inválido**

O firmware não é válido.

◦ **Falhou - outro**

O firmware não pôde ser baixado, possivelmente por causa de um problema físico com a unidade.

◦ * Não tentou*

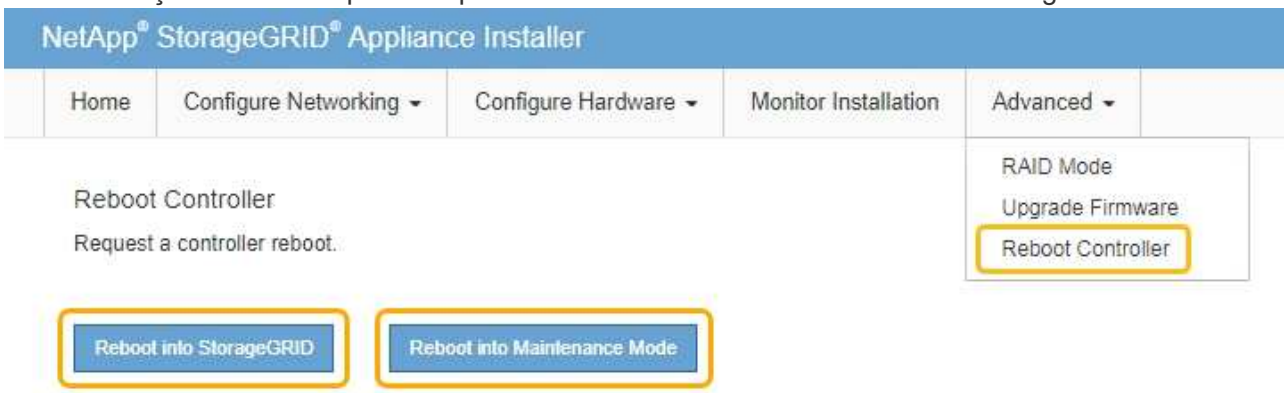
O firmware não foi baixado, o que pode ser devido a vários motivos diferentes, como o download foi

interrompido antes que ele pudesse ocorrer, ou a unidade não se qualificou para a atualização, ou o download não pôde ocorrer devido a um erro.

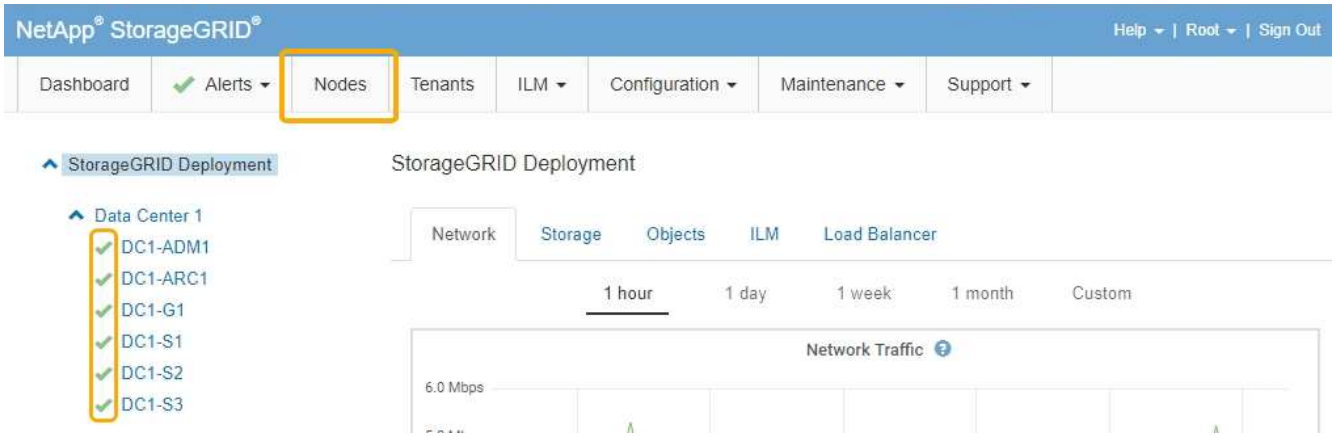
- * Bem-sucedido *

  O firmware foi transferido com sucesso.

9. Após a conclusão da atualização do firmware da unidade:
   - Para fechar o Assistente de transferência do firmware da unidade, selecione **Fechar**.
   - Para iniciar o assistente novamente, selecione **Transferir mais**.
10. Quando a operação de atualização estiver concluída, reinicie o aparelho. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:
    - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
    - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Substituição do controlador E2700

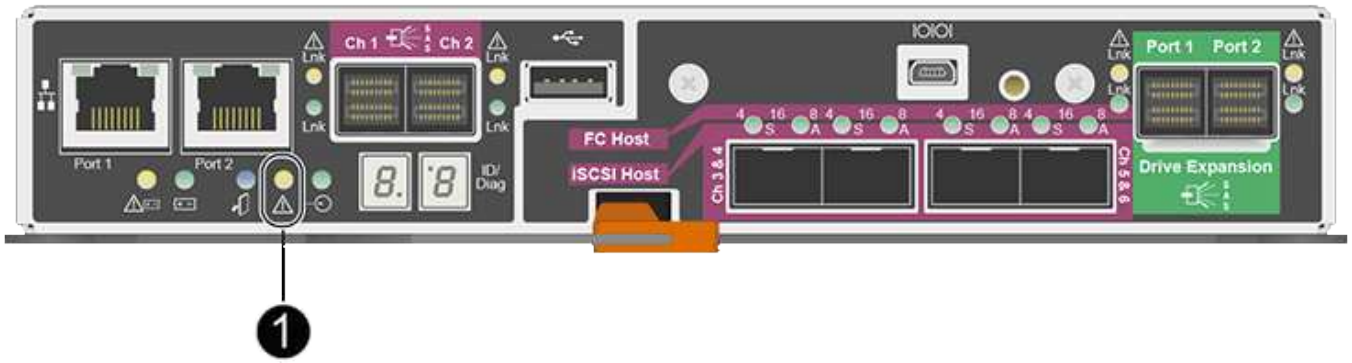
Talvez seja necessário substituir o controlador E2700 se ele não estiver funcionando de forma ideal ou se ele tiver falhado.

O que você vai precisar

- Você tem um controlador de substituição com o mesmo número de peça do controlador que está substituindo.
- Você tem etiquetas para identificar cada cabo conetado ao controlador.
- Você tem proteção antiestática.
- Tem de ter a permissão Manutenção ou Acesso root. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

Sobre esta tarefa

Pode determinar se tem um controlador com falha verificando o LED âmbar Ação de Serviço necessária no controlador (apresentado como 1 na ilustração). Se este LED estiver ligado, o controlador deve ser substituído.



O nó de storage do dispositivo não estará acessível quando você substituir o controlador. Se o controlador E2700 estiver a funcionar o suficiente, pode colocar o controlador E5600SG no modo de manutenção.

Quando substituir um controlador, tem de remover a bateria do controlador original e instalá-la no controlador de substituição.

Passos

1. Prepare-se para remover o controlador.

   Você usa o SANtricity Storage Manager para executar estas etapas.

   a. Anote qual versão do software SANtricity os está atualmente instalada no controlador.
   b. Anote qual versão do NVSRAM está instalada atualmente.
   c. Se o recurso Segurança da unidade estiver ativado, verifique se existe uma chave salva e se você sabe a frase-passe necessária para instalá-la.

   Possível perda de acesso a dados -- se todas as unidades do dispositivo estiverem habilitadas para segurança, o novo controlador não poderá acessar o dispositivo até que você desbloqueie as unidades protegidas usando a janela Gerenciamento Empresarial no SANtricity Storage Manager.

d. Faça uma cópia de segurança da base de dados de configuração.

   Se ocorrer um problema ao remover um controlador, pode utilizar o ficheiro guardado para restaurar a configuração.

e. Colete dados de suporte para o dispositivo.

   > A coleta de dados de suporte antes e depois da substituição de um componente garante que você possa enviar um conjunto completo de logs para o suporte técnico caso a substituição não resolva o problema.

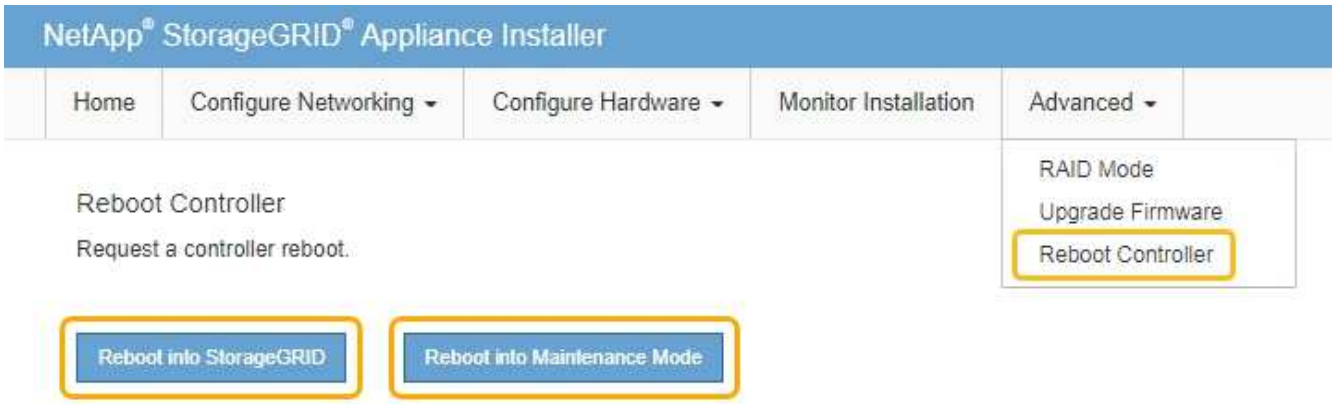
2. Se o dispositivo StorageGRID estiver a funcionar num sistema StorageGRID, coloque o controlador E5600SG no modo de manutenção.

   "Colocar um aparelho no modo de manutenção"

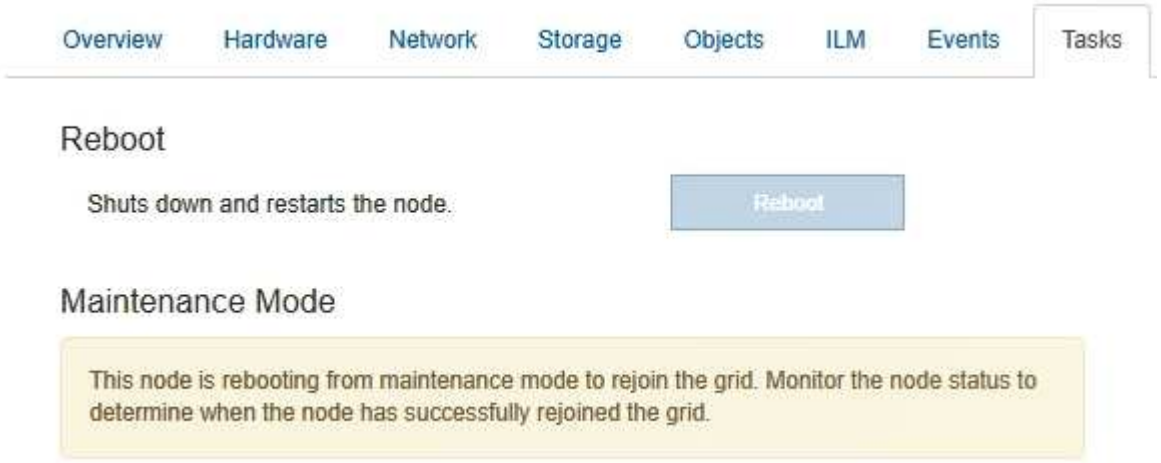
3. Se o controlador E2700 estiver a funcionar o suficiente para permitir um encerramento controlado, confirme que todas as operações foram concluídas.
   a. Na barra de título da janela Gerenciamento de matrizes, selecione **Monitor relatórios operações em andamento**.
   b. Confirme se todas as operações foram concluídas.
4. Siga as instruções no procedimento de substituição de um controlador simplex E2700 para concluir estes passos:
   a. Identifique os cabos e, em seguida, desligue os cabos.

      > Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos.

   b. Retire o controlador com falha do aparelho.
   c. Retire a tampa do controlador.
   d. Desaperte o parafuso de aperto manual e retire a bateria do controlador avariado.
   e. Instale a bateria no controlador de substituição e volte a colocar a tampa do controlador.
   f. Instale o controlador de substituição no aparelho.
   g. Volte a colocar os cabos.
   h. Aguarde até que o controlador E2700 seja reiniciado. Verifique se o visor de sete segmentos mostra um estado `99` de .
5. Se o dispositivo utilizar unidades seguras, importe a chave de segurança da unidade.
6. Volte a colocar o aparelho no modo de funcionamento normal. No Instalador de dispositivos StorageGRID, selecione **Avançado controlador de reinicialização** e, em seguida, selecione **Reiniciar no StorageGRID**.

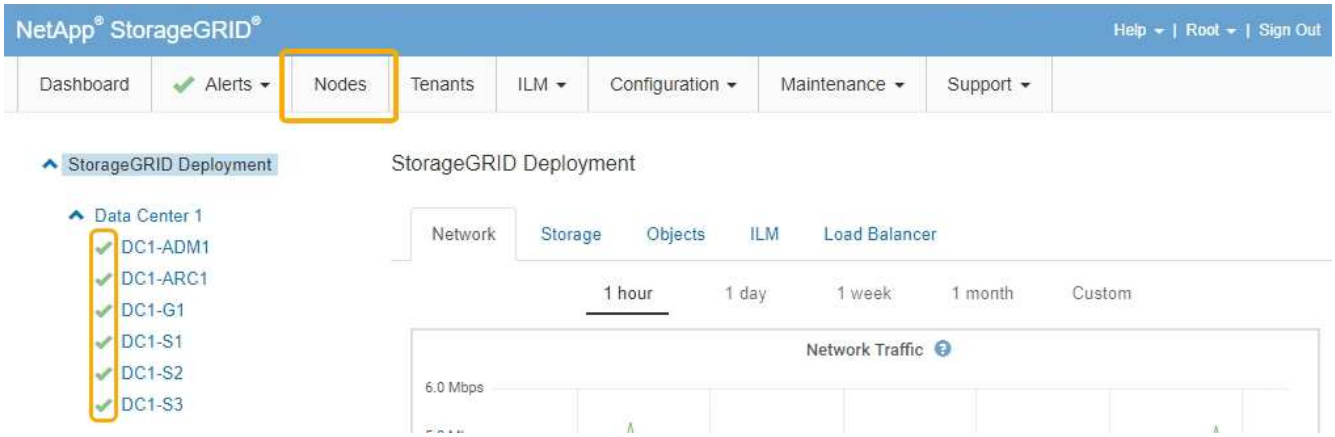


Durante a reinicialização, é apresentado o seguinte ecrã:



O aparelho reinicia e regozija-se com a grelha. Este processo pode demorar até 20 minutos.

7. Confirme se a reinicialização está concluída e se o nó voltou a ingressar na grade. No Gerenciador de Grade, verifique se a guia **nós** exibe um status normal ✔para o nó do dispositivo, indicando que nenhum alerta está ativo e o nó está conetado à grade.



8. Na SANtricity Storage Manager, confirme se o novo controlador é ideal e colete dados de suporte.

Informações relacionadas

"Procedimentos de substituição de hardware do NetApp e-Series e EF-Series"

"Documentação do NetApp: Série E2700"

Substituição do controlador E5600SG

Talvez seja necessário substituir o controlador E5600SG.

O que você vai precisar

Você deve ter acesso aos seguintes recursos:

- Informações de substituição de hardware do e-Series no site de suporte da NetApp em mais "mysupport.NetApp.com"
- E5600 documentação no site de suporte
- O aparelho foi colocado no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Se ambos os controladores estiverem funcionando o suficiente para permitir um desligamento controlado, você poderá desligar o controlador E5600SG primeiro para interromper a conetividade com o controlador E2700.

> Se você estiver substituindo o controlador antes de instalar o software StorageGRID, talvez você não consiga acessar o instalador do StorageGRID Appliance imediatamente após concluir este procedimento. Embora você possa acessar o Instalador de dispositivos StorageGRID de outros hosts na mesma sub-rede que o appliance, você não pode acessá-lo de hosts em outras sub-redes. Esta condição deve resolver-se dentro de 15 minutos (quando qualquer entrada de cache ARP para o tempo limite do controlador original), ou você pode limpar a condição imediatamente, limpando quaisquer entradas de cache ARP antigas manualmente do roteador ou gateway local.

Passos

1. Use proteção antiestática.
2. Identifique cada cabo conetado ao controlador E5600SG para que você possa reconetar os cabos corretamente.

   > Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos. Não dobre os cabos com mais firmeza do que um raio de 5 cm (2 pol.).

3. Quando o aparelho tiver sido colocado no modo de manutenção, desligue o controlador E5600SG.
   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. Desligue o controlador E5600SG
`shutdown -h now`

4. Desligue a alimentação do compartimento e aguarde até que todas as atividades de exibição de LED e sete segmentos na parte traseira do controlador tenham parado.
5. Retire os cabos.
6. Remova o controlador, conforme descrito na documentação do controlador E5600SG.
7. Insira o novo controlador, conforme descrito na documentação do controlador E5600SG.
8. Substitua todos os cabos.
9. Volte a ligar a alimentação ao compartimento.
10. Monitorize os códigos de sete segmentos.
    - Controlador E2700:

      O estado final do LED é `99`.

    - Controlador E5600SG:

      O estado final do LED é `HA`.

11. Monitore o status do nó de armazenamento do dispositivo no Gerenciador de Grade.

    Verifique se os nós de storage do dispositivo retornam ao status esperado.

Informações relacionadas

"Procedimentos de substituição de hardware do NetApp e-Series e EF-Series"

"Documentação do NetApp: Série E5600"

Substituição de outros componentes de hardware

Pode ser necessário substituir uma unidade, ventoinha, fonte de alimentação ou bateria no aparelho StorageGRID.

O que você vai precisar

- Você tem o procedimento de substituição de hardware do e-Series.
- O aparelho foi colocado no modo de manutenção se o procedimento de substituição de componentes exigir que desligue o aparelho.

  "Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Para substituir uma unidade, um recipiente do ventilador de alimentação, um recipiente do ventilador, um recipiente de alimentação, uma bateria ou uma gaveta de unidade, consulte os procedimentos padrão para os storages de armazenamento E2700 e E5600. Concentre-se nas instruções passo a passo para remover e substituir o hardware em si; muitos dos procedimentos do SANtricity Storage Manager não se aplicam a um dispositivo.

SG5612 instruções de substituição de componentes

FRU	Consulte
Condução	Siga as etapas nas instruções do e-Series para substituir uma unidade nas bandejas de E2600, E2700, E5400, E5500, E5600 ou 12 unidades ou 24 unidades.
Depósito da ventoinha de alimentação	Siga as etapas nas instruções do e-Series para substituir um recipiente do ventilador de energia com falha na bandeja de unidades e controlador E5612 ou E5624
Bateria no controlador E2700 (requer a remoção do controlador)	Siga as etapas em "Substituição do controlador E2700", mas instale a nova bateria no controlador existente.

SG5660 instruções de substituição de componentes

FRU	Consulte
Condução	Siga as etapas nas instruções do e-Series para substituir uma unidade nas bandejas E2660, E2760, E5460, E5560 ou E5660.
Depósito de alimentação	Siga as etapas nas instruções do e-Series para substituir um recipiente de alimentação com falha na bandeja de unidades e controlador E5660
Recipiente da ventoinha	Siga as etapas nas instruções do e-Series para substituir um recipiente de ventilador com falha na bandeja de unidades e controlador E5660
Bateria no controlador E2700 (requer a remoção do controlador)	Siga as etapas em "Substituição do controlador E2700", mas instale a nova bateria no controlador existente.

Informações relacionadas

"Procedimentos de substituição de hardware do NetApp e-Series e EF-Series"

"Documentação do NetApp: Série E2700"

"Documentação do NetApp: Série E5600"

Alterar a configuração do link do controlador E5600SG

Pode alterar a configuração da ligação Ethernet do controlador E5600SG. Pode alterar o modo de ligação de porta, o modo de ligação de rede e a velocidade de ligação.

O que você vai precisar

- Tem de colocar o controlador E5600SG no modo de manutenção. Colocar o controlador no modo de manutenção interrompe a ligação ao controlador E2700. Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

  "Colocar um aparelho no modo de manutenção"

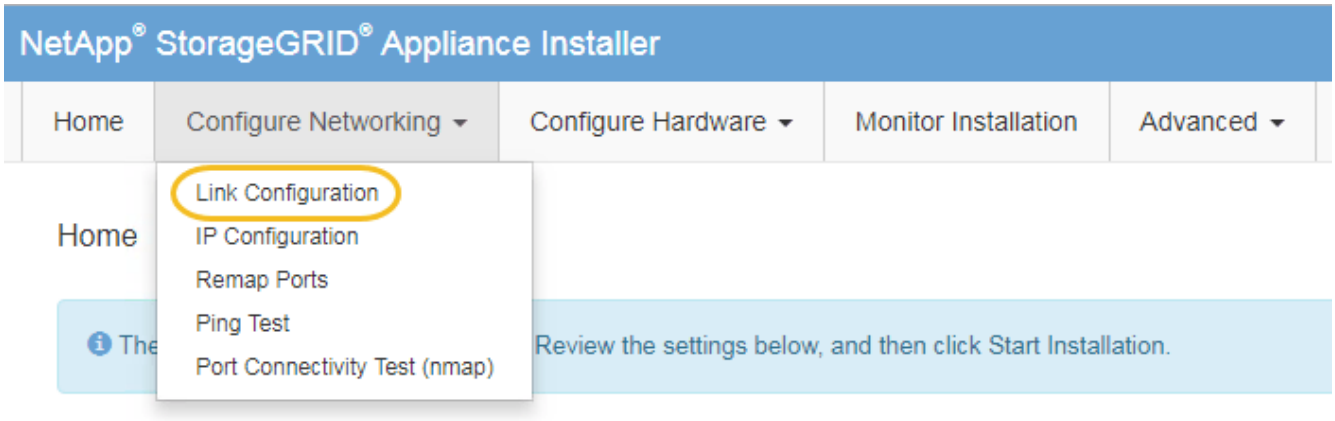
Sobre esta tarefa

As opções para alterar a configuração do link Ethernet do controlador E5600SG incluem:

- Alterar o modo **Port bond** de fixo para agregado, ou de agregado para fixo
- Alteração do **modo de ligação de rede** de ative-Backup para LACP ou de LACP para ative-Backup
- Ativar ou desativar a marcação de VLAN ou alterar o valor de uma tag VLAN
- Alteração da velocidade do link de 10 GbE para 25 GbE ou de 25 GbE para 10 GbE

Passos

1. Selecione **Configurar rede Configuração de ligação** no menu.



1. Faça as alterações desejadas na configuração do link.

   Para obter mais informações sobre as opções, consulte ""Configurando links de rede".

2. Quando estiver satisfeito com suas seleções, clique em **Salvar**.

   Poderá perder a ligação se tiver efetuado alterações à rede ou à ligação através da qual está ligado. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do Instalador de appliance StorageGRID usando um dos outros endereços IP atribuídos ao appliance
   `https://E5600SG_Controller_IP:8443`

   Se você fez alterações nas configurações de VLAN, a sub-rede do dispositivo pode ter sido alterada. Se você precisar alterar os endereços IP do dispositivo, siga as instruções para configurar endereços IP.

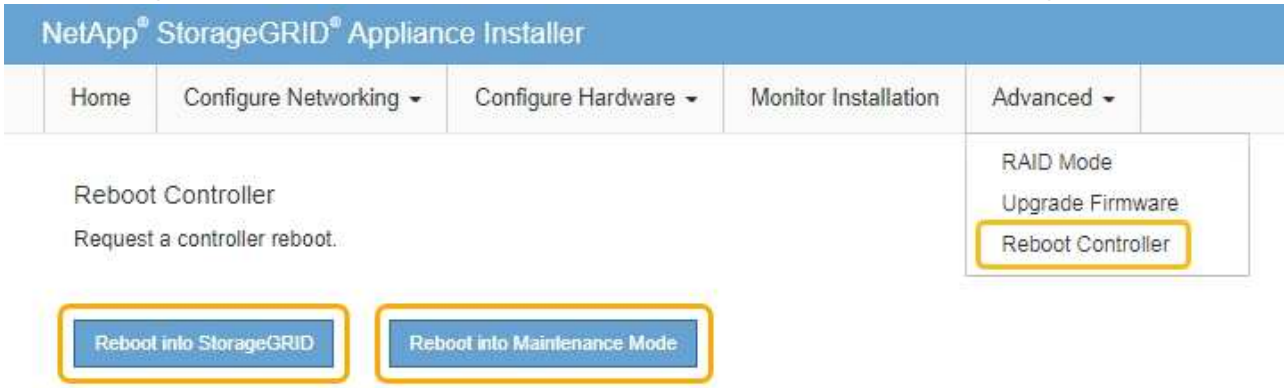
   "Definir a configuração IP"

3. No Instalador do StorageGRID Appliance, selecione **Configurar rede Teste de ping**.
4. Use a ferramenta Teste de ping para verificar a conetividade com endereços IP em qualquer rede que possa ter sido afetada pelas alterações de configuração de link feitas na Alterar a configuração do link etapa.

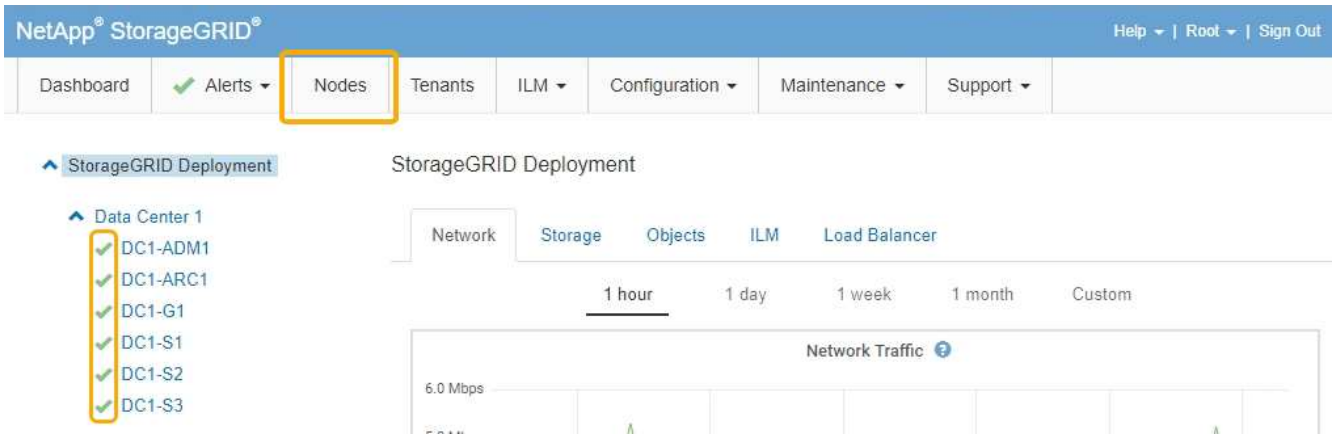
Além de quaisquer outros testes que você escolher executar, confirme que você pode fazer ping no endereço IP da grade do nó Admin principal e no endereço IP da grade de pelo menos um outro nó de armazenamento. Se necessário, corrija quaisquer problemas de configuração do link.

5. Uma vez que você estiver satisfeito que as alterações de configuração do link estão funcionando, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



   Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Configurando links de rede (SG5600)"

Alterar a definição MTU

Você pode alterar a configuração MTU atribuída quando configurou endereços IP para o nó do dispositivo.

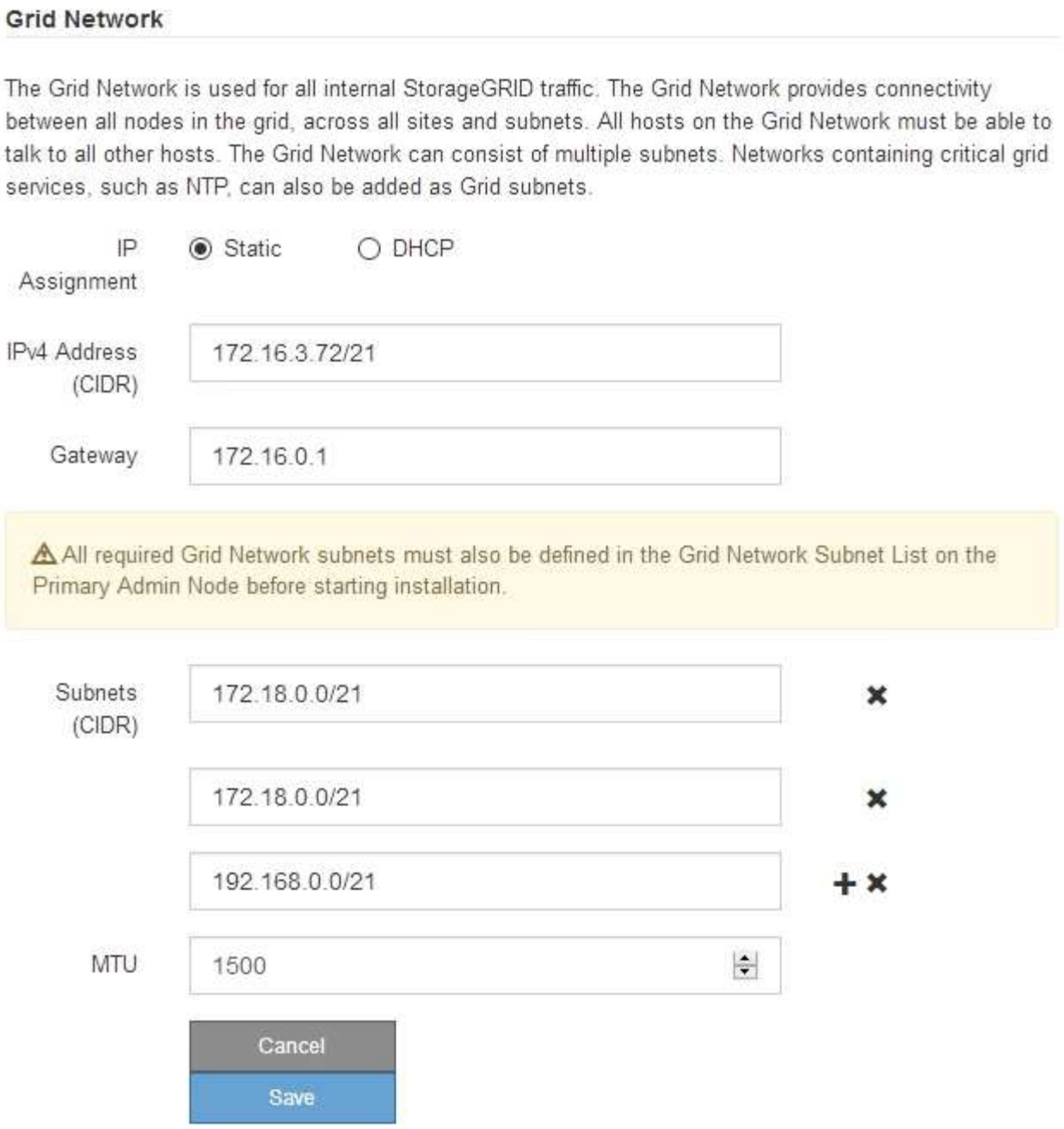
O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração IP**.
2. Faça as alterações desejadas nas configurações de MTU para rede de Grade, rede de Admin e rede de cliente.



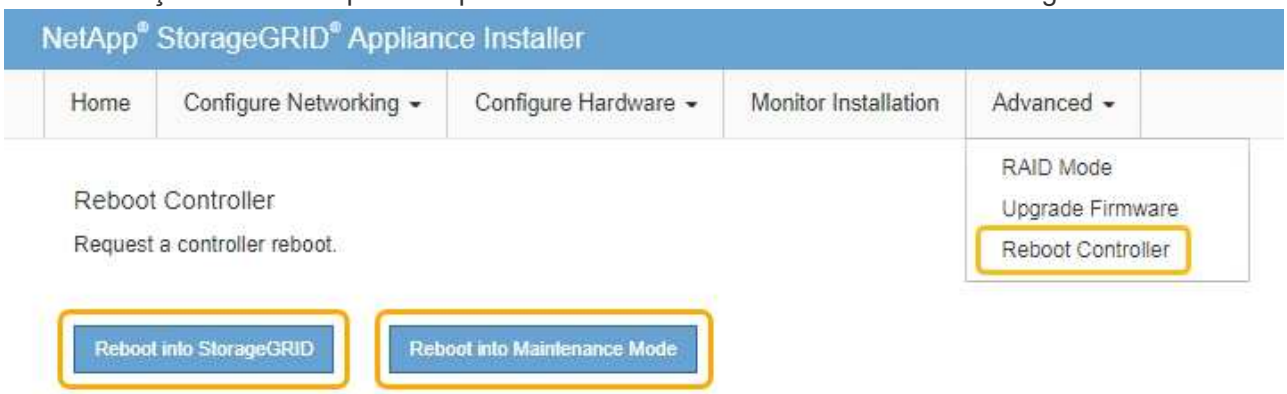
O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

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.

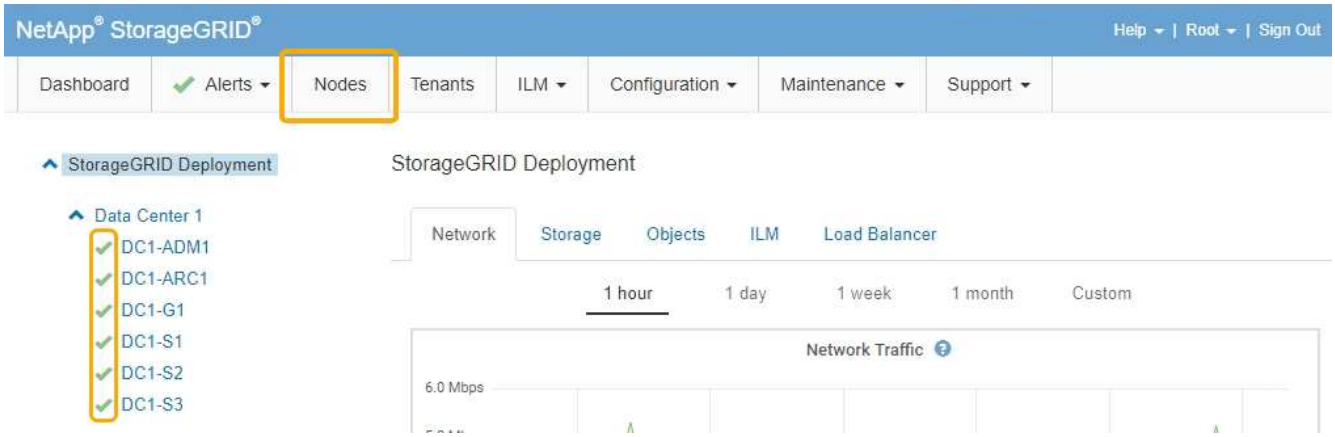
3. Quando estiver satisfeito com as definições, selecione **Guardar**.
4. Reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de**

reinicialização e, em seguida, selecione uma destas opções:

- Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
- Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Administrar o StorageGRID"

Verificar a configuração do servidor DNS

Você pode verificar e alterar temporariamente os servidores DNS (sistema de nomes de domínio) que estão atualmente em uso por este nó de appliance.

O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Talvez seja necessário alterar as configurações do servidor DNS se um dispositivo criptografado não puder se conetar ao servidor de gerenciamento de chaves (KMS) ou ao cluster KMS porque o nome do host para o KMS foi especificado como um nome de domínio em vez de um endereço IP. Quaisquer alterações efetuadas nas definições de DNS do dispositivo são temporárias e perdem-se quando sai do modo de manutenção. Para tornar essas alterações permanentes, especifique os servidores DNS no Gerenciador de Grade (**Manutenção rede servidores DNS**).

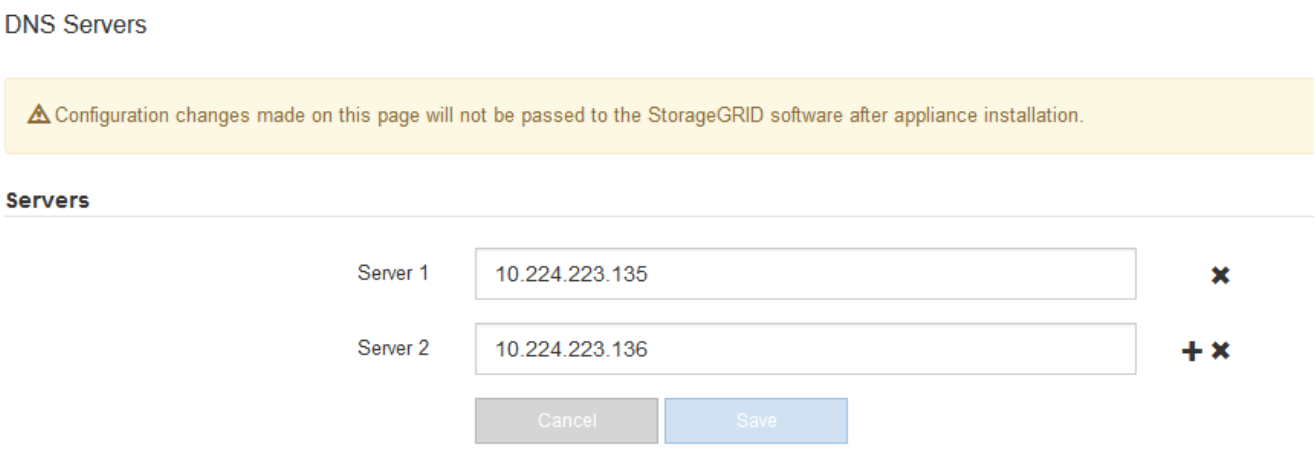
- As alterações temporárias na configuração DNS são necessárias apenas para dispositivos encriptados por nó onde o servidor KMS é definido utilizando um nome de domínio totalmente qualificado, em vez de um endereço IP, para o nome de anfitrião.
- Quando um dispositivo criptografado por nó se coneta a um KMS usando um nome de domínio, ele deve se conetar a um dos servidores DNS definidos para a grade. Um desses servidores DNS converte o nome de domínio em um endereço IP.
- Se o nó não conseguir alcançar um servidor DNS para a grade, ou se você alterou as configurações de DNS em toda a grade quando um nó de dispositivo criptografado por nó estava off-line, o nó não consegue se conetar ao KMS. Os dados criptografados no dispositivo não podem ser descriptografados até que o problema de DNS seja resolvido.

Para resolver um problema de DNS que impede a ligação KMS, especifique o endereço IP de um ou mais servidores DNS no Instalador de aplicações StorageGRID. Essas configurações de DNS temporárias permitem que o dispositivo se conete ao KMS e descriptografar dados no nó.

Por exemplo, se o servidor DNS para a grade mudar enquanto um nó criptografado estava off-line, o nó não será capaz de alcançar o KMS quando ele voltar on-line, uma vez que ainda está usando os valores DNS anteriores. A introdução do novo endereço IP do servidor DNS no Instalador de aplicações StorageGRID permite que uma ligação KMS temporária desencripte os dados do nó.

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração de DNS**.
2. Verifique se os servidores DNS especificados estão corretos.



3. Se necessário, altere os servidores DNS.

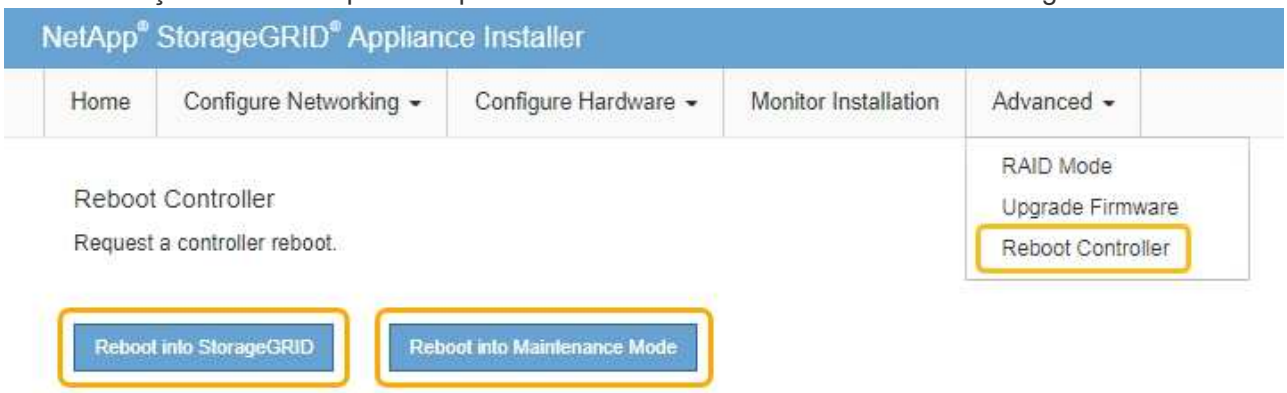
As alterações efetuadas nas definições de DNS são temporárias e perdem-se quando sai do modo de manutenção.

4. Quando estiver satisfeito com as definições de DNS temporárias, selecione **Guardar**.

   O nó usa as configurações do servidor DNS especificadas nesta página para se reconetar ao KMS, permitindo que os dados no nó sejam descriptografados.

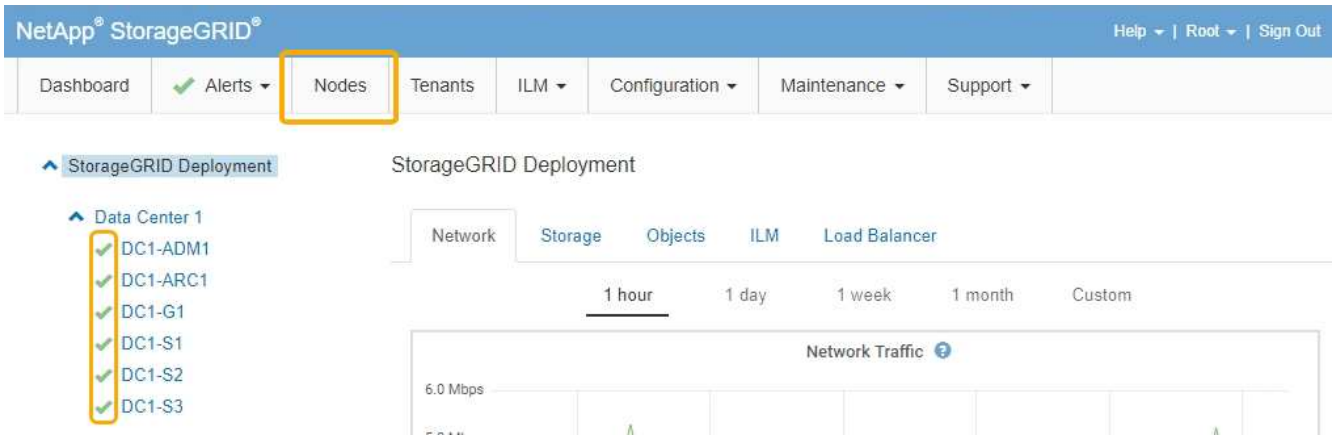
5. Depois que os dados do nó forem descriptografados, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Quando o nó reinicializa e realegra a grade, ele usa os servidores DNS de todo o sistema listados no Gerenciador de Grade. Depois de reingressar na grade, o dispositivo não usará mais os servidores DNS temporários especificados no Instalador de dispositivos StorageGRID enquanto o dispositivo estava no modo de manutenção.

Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Monitorização da encriptação do nó no modo de manutenção

Se você ativou a criptografia de nó para o dispositivo durante a instalação, poderá monitorar o status de criptografia de nó de cada nó do dispositivo, incluindo os detalhes do estado de criptografia de nó e do servidor de gerenciamento de chaves (KMS).

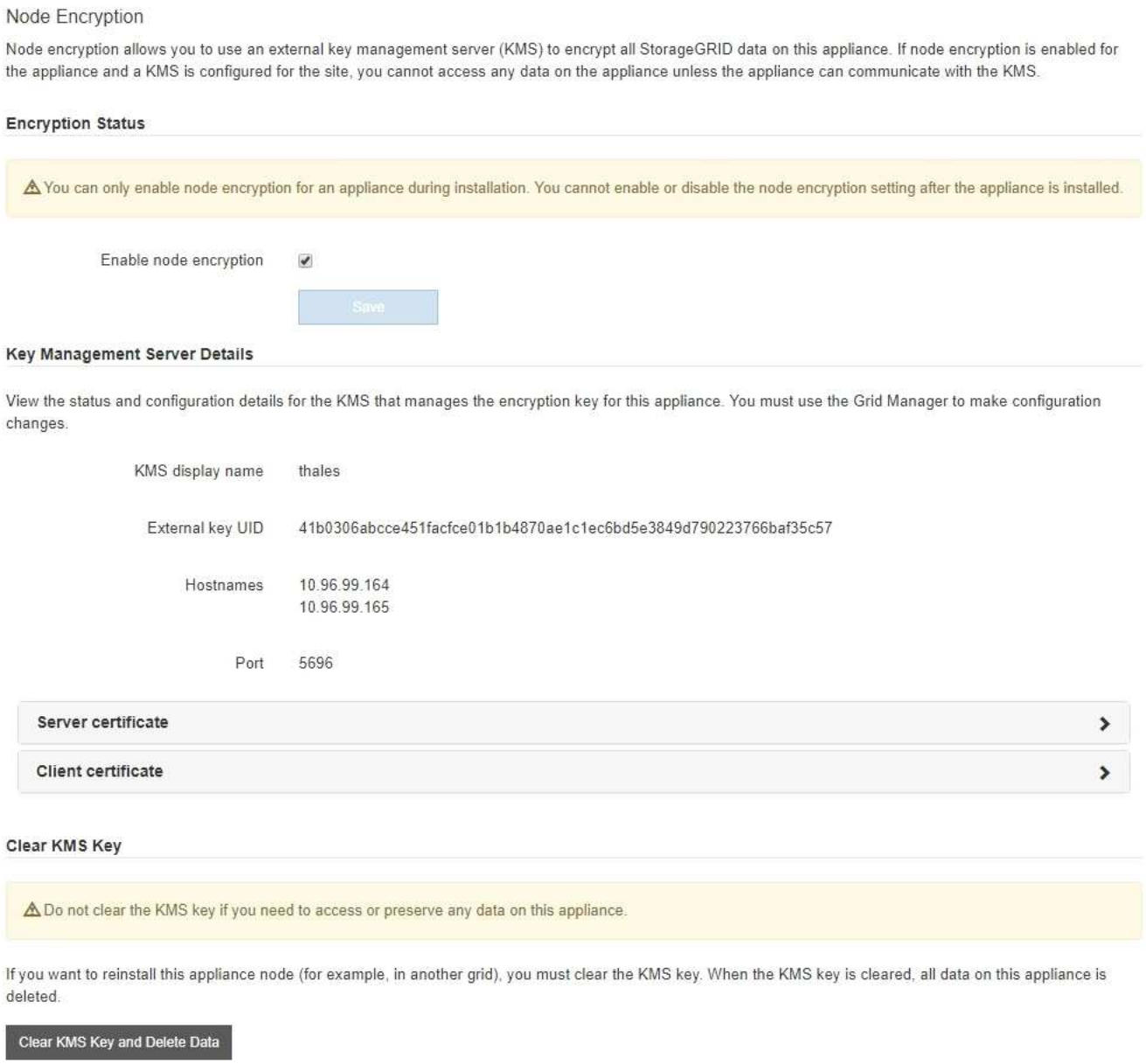
O que você vai precisar

- A criptografia do nó deve ter sido ativada para o dispositivo durante a instalação. Não é possível ativar a criptografia de nó depois que o dispositivo estiver instalado.
- O aparelho foi colocado no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Configurar hardware criptografia de nó**.



A página criptografia do nó inclui estas três seções:

- O estado de encriptação mostra se a encriptação do nó está ativada ou desativada para o dispositivo.
- Detalhes do servidor de gerenciamento de chaves mostra informações sobre o KMS sendo usado para criptografar o dispositivo. Você pode expandir as seções de certificado de servidor e cliente para exibir detalhes e status do certificado.
  - Para resolver problemas com os próprios certificados, como a renovação de certificados expirados, consulte as informações sobre o KMS nas instruções de administração do StorageGRID.
  - Se houver problemas inesperados ao se conetar aos hosts KMS, verifique se os servidores DNS (sistema de nomes de domínio) estão corretos e se a rede do appliance está configurada corretamente.

    "Verificar a configuração do servidor DNS"

  - Se você não conseguir resolver os problemas do certificado, entre em Contato com o suporte técnico.

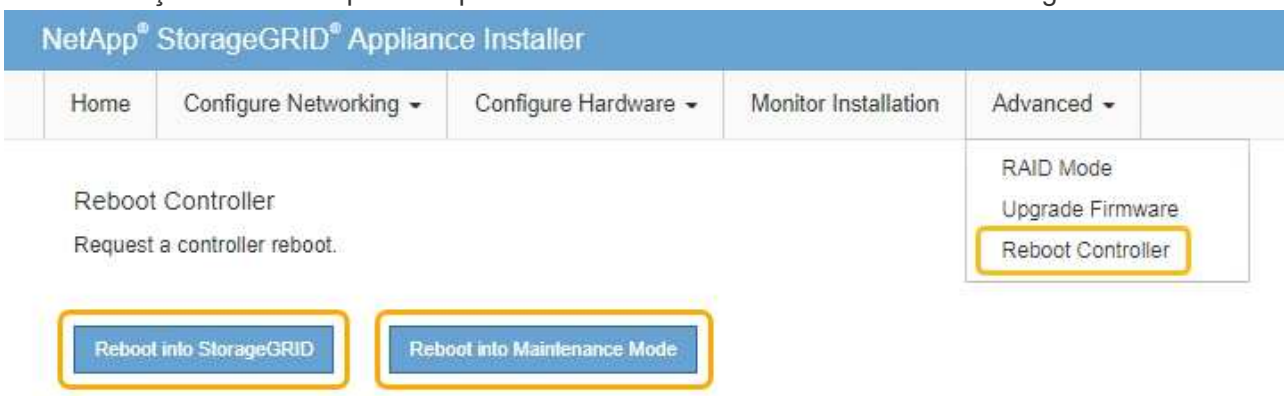
- Limpar chave KMS desativa a criptografia de nó para o dispositivo, remove a associação entre o dispositivo e o servidor de gerenciamento de chaves que foi configurado para o site StorageGRID e exclui todos os dados do dispositivo. Tem de limpar a chave KMS antes de poder instalar o aparelho noutro sistema StorageGRID.

  "Limpando a configuração do servidor de gerenciamento de chaves"

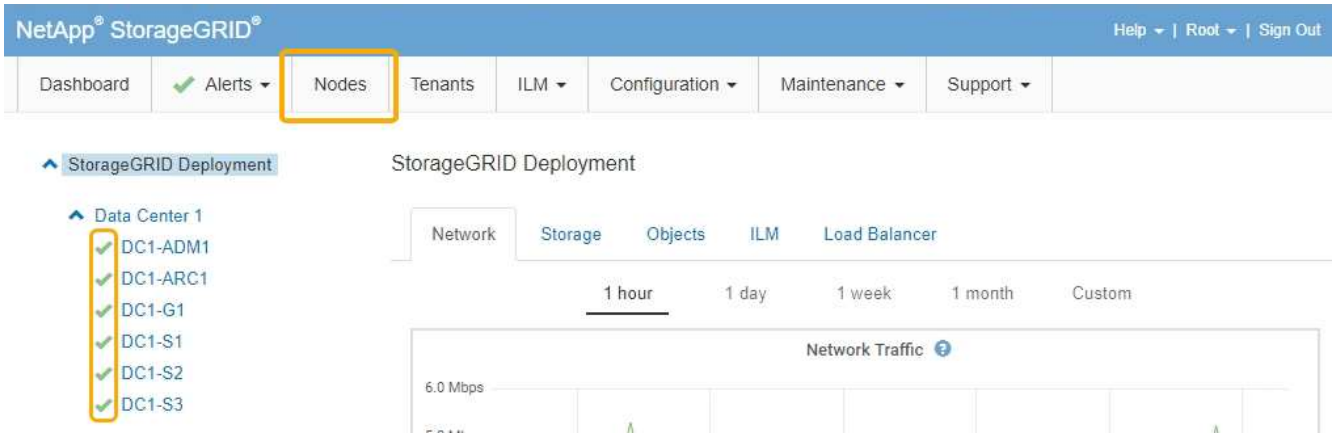
  Limpar a configuração do KMS exclui os dados do dispositivo, tornando-os permanentemente inacessíveis. Estes dados não são recuperáveis.

2. Quando terminar de verificar o estado da encriptação do nó, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Administrar o StorageGRID"

Limpando a configuração do servidor de gerenciamento de chaves

Limpar a configuração do servidor de gerenciamento de chaves (KMS) desativa a criptografia de nó no seu dispositivo. Depois de limpar a configuração do KMS, os dados do seu aparelho são excluídos permanentemente e não são mais acessíveis. Estes dados não são recuperáveis.

O que você vai precisar

Se você precisar preservar dados no dispositivo, você deve executar um procedimento de desativação de nós antes de limpar a configuração do KMS.

> Quando o KMS é eliminado, os dados no aparelho serão eliminados permanentemente e deixarão de estar acessíveis. Estes dados não são recuperáveis.

Desative o nó para mover quaisquer dados que ele contenha para outros nós no StorageGRID. Consulte as instruções de recuperação e manutenção para a desativação do nó da grade.

Sobre esta tarefa

A limpeza da configuração do KMS do appliance desativa a criptografia do nó, removendo a associação entre o nó do appliance e a configuração do KMS para o site do StorageGRID. Os dados no dispositivo são então excluídos e o dispositivo é deixado em um estado de pré-instalação. Este processo não pode ser revertido.

Você deve limpar a configuração do KMS:

- Antes de instalar o aparelho em outro sistema StorageGRID, isso não usa um KMS ou que usa um KMS diferente.

  > Não limpe a configuração do KMS se você planeja reinstalar um nó de dispositivo em um sistema StorageGRID que usa a mesma chave KMS.

- Antes de poder recuperar e reinstalar um nó onde a configuração do KMS foi perdida e a chave KMS não é recuperável.
- Antes de devolver qualquer aparelho que estava anteriormente em uso em seu site.
- Após a desativação de um dispositivo que tinha a criptografia de nó ativada.

> Desative o dispositivo antes de limpar o KMS para mover seus dados para outros nós em seu sistema StorageGRID. Limpar o KMS antes de desativar o aparelho resultará em perda de dados e pode tornar o aparelho inoperável.

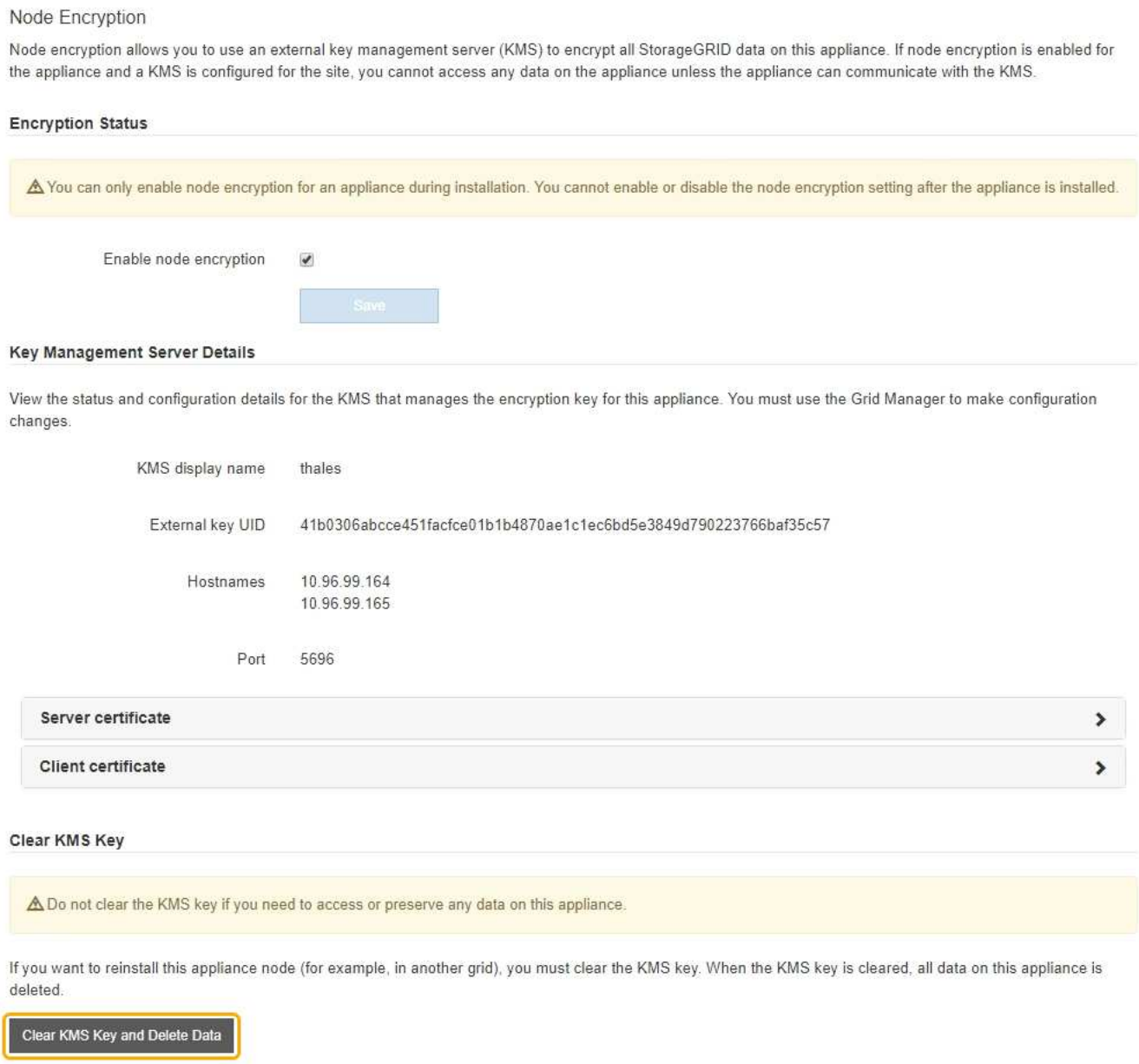
Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

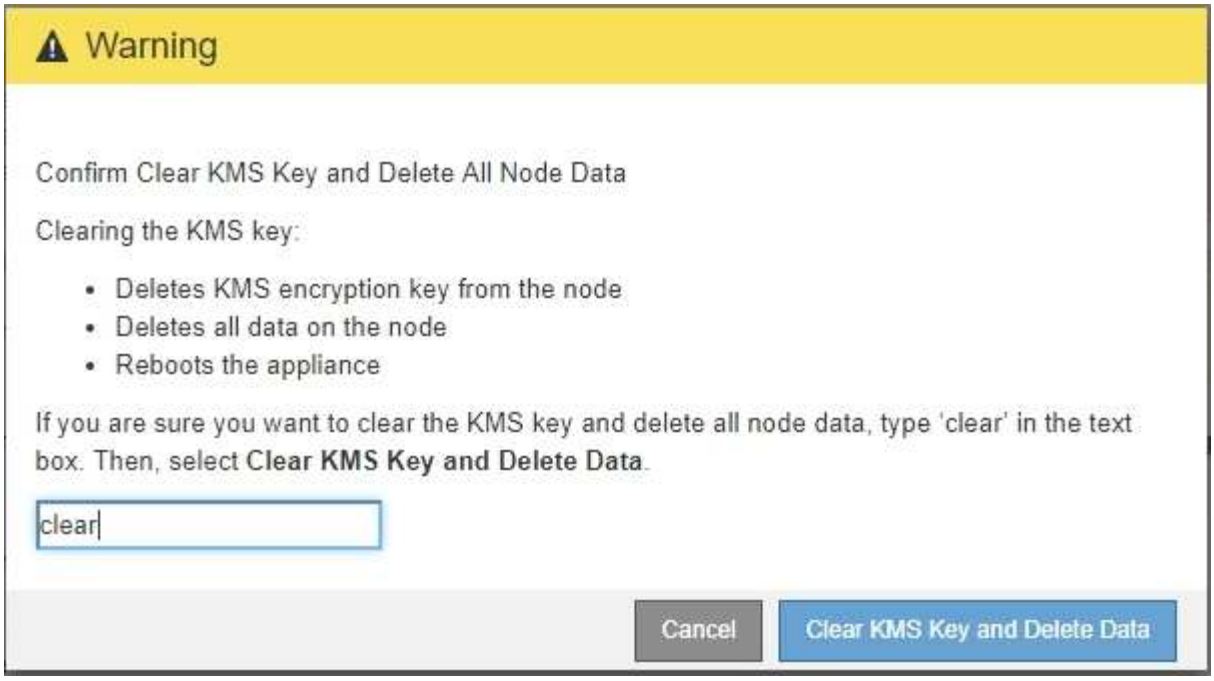
   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configure hardware Node Encryption**.



> Se a configuração do KMS for limpa, os dados no dispositivo serão excluídos permanentemente. Estes dados não são recuperáveis.

3. Na parte inferior da janela, selecione **Limpar chave KMS e Excluir dados**.
4. Se você tem certeza de que deseja limpar a configuração do KMS, digite `clear` e selecione **Limpar chave KMS e Excluir dados**.



A chave de criptografia KMS e todos os dados são excluídos do nó e o dispositivo é reinicializado. Isso pode levar até 20 minutos.

5. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E **`https://Controller_IP:8443`**

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

6. Selecione **Configure hardware Node Encryption**.
7. Verifique se a criptografia do nó está desativada e se as informações de chave e certificado em **Key Management Server Details** e **Clear KMS Key e Delete Data** control são removidas da janela.

   A criptografia do nó não pode ser reativada no dispositivo até que seja reinstalada em uma grade.

Depois de terminar

Depois de o aparelho reiniciar e verificar se o KMS foi limpo e se o aparelho está num estado de pré-instalação, pode remover fisicamente o aparelho do sistema StorageGRID. Consulte as instruções de recuperação e manutenção para obter informações sobre como preparar um aparelho para reinstalação.

Informações relacionadas

"Administrar o StorageGRID"

"Manter recuperar"

Aparelhos de serviços SG100 SG1000

Saiba como instalar e manter os dispositivos StorageGRID SG100 e SG1000.

- "Visão geral dos aparelhos SG100 e SG1000"

- "Aplicações SG100 e SG1000"
- "Visão geral da instalação e implantação"
- "Preparando-se para a instalação"
- "Instalar o hardware"
- "Configurando conexões StorageGRID"
- "Configurando a interface BMC"
- "Opcional: Habilitando a criptografia de nó"
- "Implantando um nó de dispositivo de serviços"
- "Solução de problemas da instalação do hardware"
- "Manutenção do aparelho"

Visão geral dos aparelhos SG100 e SG1000

O dispositivo de serviços StorageGRID SG100 e o dispositivo de serviços SG1000 podem operar como um nó de gateway e como um nó de administrador para fornecer serviços de balanceamento de carga de alta disponibilidade em um sistema StorageGRID. Ambos os dispositivos podem operar como nós de gateway e nós de administração (primários ou não primários) ao mesmo tempo.

Caraterísticas do aparelho

Ambos os modelos do dispositivo de serviços fornecem os seguintes recursos:

- Funções de nó de gateway ou nó de administrador para um sistema StorageGRID.
- O instalador do dispositivo StorageGRID para simplificar a implantação e a configuração de nós.
- Quando implantado, pode acessar o software StorageGRID de um nó de administrador existente ou de software baixado para uma unidade local. Para simplificar ainda mais o processo de implementação, uma versão recente do software é pré-carregada no dispositivo durante o fabrico.
- Um controlador de gerenciamento de placa base (BMC) para monitorar e diagnosticar alguns dos hardwares do dispositivo.
- A capacidade de se conetar a todas as três redes StorageGRID, incluindo a rede de Grade, a rede de Administração e a rede de Cliente:
  - O SG100 suporta até quatro conexões de 10 ou 25 GbE à rede de Grade e à rede do cliente.
  - O SG1000 suporta até quatro conexões de 10, 25, 40 ou 100 GbE à rede de Grade e à rede de Cliente.

Diagramas SG100D e SG1000D.

Esta figura mostra a parte frontal do SG100 e do SG1000 com a moldura removida.

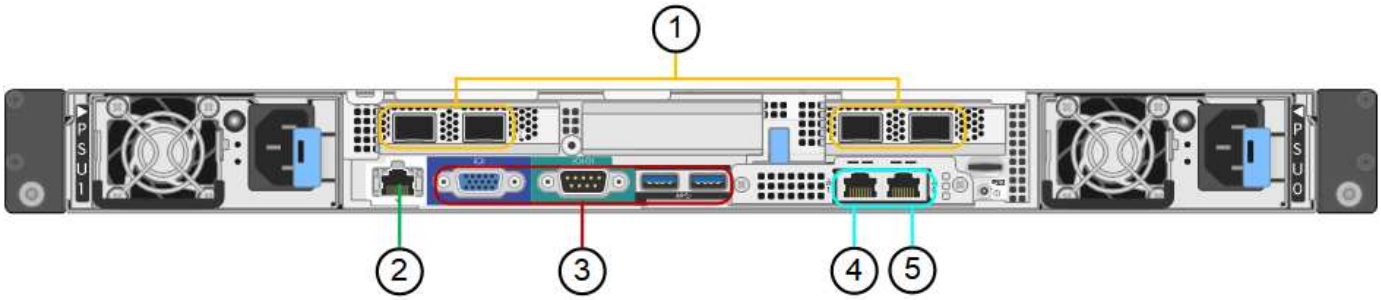
Pela frente, os dois aparelhos são idênticos, exceto o nome do produto na moldura.

As duas unidades de estado sólido (SSDs), indicadas pelo contorno laranja, são usadas para armazenar o sistema operacional StorageGRID e são espelhadas usando RAID1 para redundância. Quando o dispositivo de serviços SG100 ou SG1000 é configurado como um nó Admin, essas unidades são usadas para armazenar logs de auditoria, métricas e tabelas de banco de dados.

Os restantes slots de unidade estão em branco.

Conetores na parte traseira do SG100

Esta figura mostra os conetores na parte de trás do SG100.

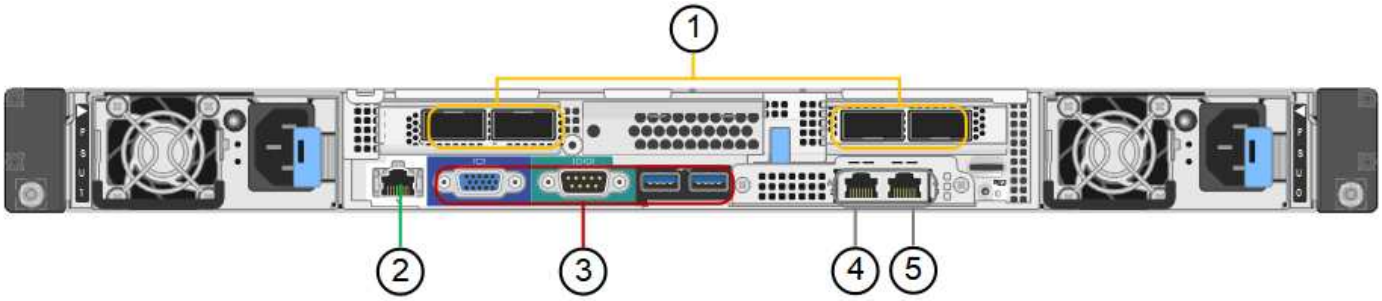


	Porta	Tipo	Utilização
1	Portas de rede 1-4	10/25-GbE, com base no tipo de transcetor de cabo ou SFP (os módulos SFP28 e SFP mais são suportados), velocidade do switch e velocidade do link configurada	Conete-se à rede de grade e à rede de cliente para StorageGRID.
2	Porta de gerenciamento de BMC	1 GbE (RJ-45)	Ligue ao controlador de gestão da placa de base do aparelho.
3	Portas de diagnóstico e suporte	• VGA • Série, 115200 8-N-1 • USB	Reservado para uso de suporte técnico.
4	Admin Network port 1	1 GbE (RJ-45)	Ligue o dispositivo à rede de administração para StorageGRID.

	Porta	Tipo	Utilização
5	Admin Network port 2	1 GbE (RJ-45)	Opções: • Vincular com a porta de gerenciamento 1 para uma conexão redundante com a rede de administração para StorageGRID. • Deixe desconetado e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, utilize a porta 2 para a configuração IP se os endereços IP atribuídos pelo DHCP não estiverem disponíveis.

Conetores na parte traseira do SG1000

Esta figura mostra os conetores na parte de trás do SG1000.



	Porta	Tipo	Utilização
1	Portas de rede 1-4	10/25/40/100-GbE, com base no tipo de cabo ou transcetor, velocidade do switch e velocidade do link configurada. Os transcetores QSFP28 e QSFP (40/100GbE) são suportados nativamente e os transcetores SFP28/SFP podem ser usados com um QSA (vendido separadamente) para usar velocidades 10/25GbE.	Conete-se à rede de grade e à rede de cliente para StorageGRID.
2	Porta de gerenciamento de BMC	1 GbE (RJ-45)	Ligue ao controlador de gestão da placa de base do aparelho.

	Porta	Tipo	Utilização
3	Portas de diagnóstico e suporte	• VGA • Série, 115200 8-N-1 • USB	Reservado para uso de suporte técnico.
4	Admin Network port 1	1 GbE (RJ-45)	Ligue o dispositivo à rede de administração para StorageGRID.
5	Admin Network port 2	1 GbE (RJ-45)	Opções: • Vincular com a porta de gerenciamento 1 para uma conexão redundante com a rede de administração para StorageGRID. • Deixe desconetado e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, utilize a porta 2 para a configuração IP se os endereços IP atribuídos pelo DHCP não estiverem disponíveis.

Aplicações SG100 e SG1000

Você pode configurar os dispositivos de serviços StorageGRID de várias maneiras para fornecer serviços de gateway, bem como redundância de alguns serviços de administração de grade.

Os dispositivos podem ser implantados das seguintes maneiras:

- Adicionar a uma grade nova ou existente como um nó de gateway
- Adicione a uma nova grade como um nó de administração primário ou não primário ou a uma grade existente como um nó de administração não primário
- Opere como um nó de gateway e um nó de administrador (primário ou não primário) ao mesmo tempo

O dispositivo facilita o uso de grupos de alta disponibilidade (HA) e balanceamento de carga inteligente para conexões de caminho de dados S3 ou Swift.

Os exemplos a seguir descrevem como você pode maximizar os recursos do dispositivo:

- Use dois dispositivos SG100 ou dois SG1000 para fornecer serviços de gateway configurando-os como nós de gateway.

> Não implante os dispositivos de serviço SG100 e SG1000 no mesmo local. Pode resultar em performance imprevisível.

- Use dois dispositivos SG100 ou dois SG1000 para fornecer redundância de alguns serviços de

administração de rede. Faça isso configurando cada dispositivo como nós de administração.

- Use dois dispositivos SG100 ou dois SG1000 para fornecer serviços de balanceamento de carga e modelagem de tráfego altamente disponíveis acessados por meio de um ou mais endereços IP virtuais. Faça isso configurando os dispositivos como qualquer combinação de nós de administrador ou nós de gateway e adicionando ambos os nós ao mesmo grupo de HA.

> Se você usar nós de administrador e nós de gateway no mesmo grupo de HA, as portas CLB (Connection Load Balancer) e as portas somente para nó de administrador não farão failover. Para obter instruções para configurar grupos de HA, consulte as instruções de administração do StorageGRID.

> O serviço CLB está obsoleto.

Quando usados com dispositivos de storage do StorageGRID, os dispositivos de serviços SG100 e SG1000 permitem a implantação de grades somente de dispositivos sem dependências em hipervisores externos ou hardware de computação.

Informações relacionadas

"Administrar o StorageGRID"

Visão geral da instalação e implantação

Você pode instalar um ou mais dispositivos de serviços do StorageGRID quando implantar o StorageGRID pela primeira vez ou adicionar nós de dispositivos de serviços posteriormente como parte de uma expansão.

O que você vai precisar

O seu sistema StorageGRID está a utilizar a versão necessária do software StorageGRID.

Aparelho	Versão StorageGRID necessária
SG100	11,4 ou posterior (correção mais recente recomendada)
SG1000	11,3 ou posterior (correção mais recente recomendada)

Tarefas de instalação e implantação

Preparar e adicionar um dispositivo StorageGRID à grade inclui quatro etapas principais:

1. Preparação para a instalação:
   - Preparar o local de instalação
   - Desembalar as caixas e verificar o conteúdo
   - Obtenção de equipamentos e ferramentas adicionais
   - Verificando a configuração da rede
   - Opcional: Configurando um servidor de gerenciamento de chaves externo (KMS) se você planeja criptografar todos os dados do dispositivo. Consulte detalhes sobre o gerenciamento de chaves

externas nas instruções de administração do StorageGRID.

2. Instalar o hardware:
   - Registar o hardware
   - Instalar o aparelho num armário ou num rack
   - Fazer o cabeamento do dispositivo
   - Ligar o cabo de alimentação e ligar a alimentação
   - Exibindo códigos de status de inicialização
3. Configurar o hardware:
   - Acessando o Instalador do StorageGRID Appliance e configurando as configurações de IP de rede e link necessárias para se conetar a redes StorageGRID
   - Acesso à interface do controlador de gerenciamento de placa base (BMC) no dispositivo.
   - Opcional: Habilitando a criptografia de nó se você planeja usar um KMS externo para criptografar dados do dispositivo.
4. Implantando um Gateway de dispositivo ou nó de administrador

   Depois que o hardware do dispositivo tiver sido instalado e configurado, você pode implantar o dispositivo como um nó de gateway e um nó de administrador em um sistema StorageGRID. Os dispositivos SG100 e SG1000 podem operar como nós de gateway e nós de administração (primários e não primários) ao mesmo tempo.

Tarefa	Instruções
Implantação de um Gateway de dispositivo ou nó de administrador em um novo sistema StorageGRID	"Implantando um nó de dispositivo de serviços"
Adicionar um Gateway de dispositivo ou nó de administrador a um sistema StorageGRID existente	"Instruções para expandir um sistema StorageGRID"
Implantação de um Gateway de dispositivo ou nó de administrador como parte de uma operação de recuperação de nó	"Instruções para recuperação e manutenção"

Informações relacionadas

"Preparando-se para a instalação"

"Instalar o hardware"

"Configurando conexões StorageGRID"

"Expanda sua grade"

"Manter recuperar"

"Administrar o StorageGRID"

Preparando-se para a instalação

Preparar a instalação de um dispositivo StorageGRID implica preparar o local e obter todo o hardware, cabos e ferramentas necessários. Você também deve coletar endereços IP e informações de rede.

Passos

- "Preparação do local (SG100 e SG1000)"
- "Desembalar as caixas (SG100 e SG1000)"
- "Obtenção de equipamentos e ferramentas adicionais (SG100 e SG1000)"
- "Requisitos do navegador da Web"
- "Rever as ligações de rede do dispositivo"
- "Recolha de informações de instalação (SG100 e SG1000)"

Preparação do local (SG100 e SG1000)

Antes de instalar o aparelho, certifique-se de que o local e o gabinete ou rack que pretende utilizar cumprem as especificações de um dispositivo StorageGRID.

Passos

1. Confirme se o local atende aos requisitos de temperatura, umidade, faixa de altitude, fluxo de ar, dissipação de calor, fiação, energia e aterramento. Consulte o NetApp Hardware Universe para obter mais informações.
2. Confirme se a sua localização fornece a tensão correta da alimentação CA (na faixa de 120 a 240 volts AC).
3. Obtenha um gabinete ou rack de 19 polegadas (48,3 cm) para encaixar prateleiras deste tamanho (sem cabos):

Altura	Largura	Profundidade	Peso máximo
1,70 pol. (4,32 cm)	17,32 pol. (44,0 cm)	32,0 pol. (81,3 cm)	13 39 lb. (17,7 kg)

4. Decida onde vai instalar o aparelho.

Informações relacionadas

"NetApp Hardware Universe"

"Ferramenta de Matriz de interoperabilidade do NetApp"

Desembalar as caixas (SG100 e SG1000)

Antes de instalar o dispositivo StorageGRID, desembale todas as caixas e compare o conteúdo com os itens no saco de embalagem.

Hardware do dispositivo

- **SG100 ou SG1000**

- **Kit de trilho com instruções**

Cabos de energia

O envio para o dispositivo StorageGRID inclui os seguintes cabos de alimentação:

- * Dois cabos de alimentação para o seu país*

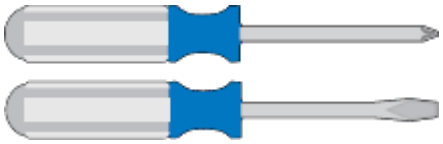
  O gabinete pode ter cabos de alimentação especiais que você usa em vez dos cabos de alimentação fornecidos com o aparelho.

Obtenção de equipamentos e ferramentas adicionais (SG100 e SG1000)

Antes de instalar o dispositivo StorageGRID, confirme se tem todo o equipamento e ferramentas adicionais de que necessita.

Você precisa do seguinte equipamento adicional para instalar e configurar o hardware:

- **Chaves de fenda**

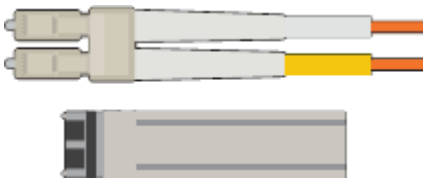


  Chave de fendas Phillips n.o 2

  Chave de parafusos plana média

- * Pulseira antiestática*

- * Cabos óticos e transcetores*



  - Cabo
    - Twinax/cobre (1 a 4)

      ou

    - Fibra/ótica (1 a 4)
  - 1 a 4 de cada um desses transcetores/adaptadores baseados na velocidade do link (velocidades mistas não são suportadas)
    - SG100:

Velocidade da ligação (GbE)	Equipamento necessário
10	Transceptor SFP
25	Transcetor SFP28

    - SG1000:

Velocidade da ligação (GbE)	Equipamento necessário
10	Adaptador QSFP-para-SFP (QSA) e transcetor SFP
25	Adaptador QSFP-para-SFP (QSA) e transcetor SFP28
40	Transceptor QSFP
100	Transcetor QFSP28

- **Cabos Ethernet RJ-45 (Cat5/Cat5e/Cat6/Cat6a)**

- * Serviço de laptop*

Navegador da Web suportado

Porta de 1 GbE (RJ-45)

Algumas portas podem não suportar velocidades Ethernet de 10/100Mbps.

- **Ferramentas opcionais**

Broca elétrica com ponta Phillips

Lanterna

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Rever as ligações de rede do dispositivo

Antes de instalar o dispositivo StorageGRID, você deve entender quais redes podem ser conetadas ao dispositivo.

Ao implantar um dispositivo StorageGRID como nó em um sistema StorageGRID, você pode conectá-lo às seguintes redes:

- **Rede de grade para StorageGRID**: A rede de grade é usada para todo o tráfego interno de StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes. A rede de Grade é necessária.
- **Rede de administração para StorageGRID**: A rede de administração é uma rede fechada usada para administração e manutenção do sistema. A rede Admin é normalmente uma rede privada e não precisa ser roteável entre sites. A rede de administração é opcional.
- **Rede de clientes para StorageGRID:** a rede de clientes é uma rede aberta usada para fornecer acesso a aplicativos clientes, incluindo S3 e Swift. A rede do cliente fornece acesso ao protocolo do cliente à grade, de modo que a rede da grade possa ser isolada e protegida. Você pode configurar a rede do cliente para que o dispositivo possa ser acessado por essa rede usando apenas as portas que você escolher abrir. A rede do cliente é opcional.
- **Rede de gerenciamento BMC para o utilitário de serviços:** esta rede fornece acesso ao controlador de gerenciamento de placa base nos SG100 e SG1000, dispositivos que permitem monitorar e gerenciar os componentes de hardware no dispositivo. Essa rede de gerenciamento pode ser a mesma rede de administração para StorageGRID ou pode ser uma rede de gerenciamento independente.

Informações relacionadas

"Recolha de informações de instalação (SG100 e SG1000)"

"Cabeamento do dispositivo SG100 e SG1000)"

"Diretrizes de rede"

"Primário de grelha"

Modos de ligação de porta para os aparelhos SG100 e SG1000

Ao configurar links de rede para os dispositivos SG100 e SG1000, você pode usar a ligação de portas para as portas que se conetam à rede de Grade e à rede cliente opcional e as portas de gerenciamento de 1 GbE que se conetam à rede de administração opcional. A ligação de portas ajuda a proteger os seus dados fornecendo caminhos redundantes entre as redes StorageGRID e o dispositivo.

Modos de ligação de rede

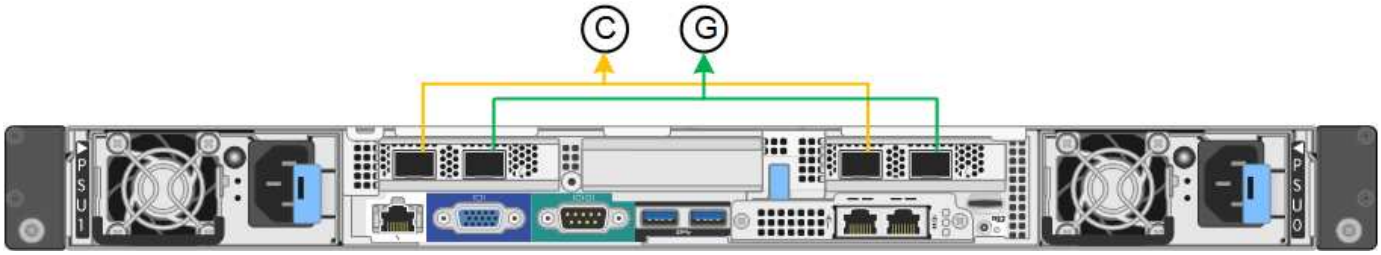
As portas de rede no dispositivo de serviços suportam o modo de ligação de porta fixa ou

o modo de ligação de porta agregada para as conexões de rede de Grade e rede de cliente.

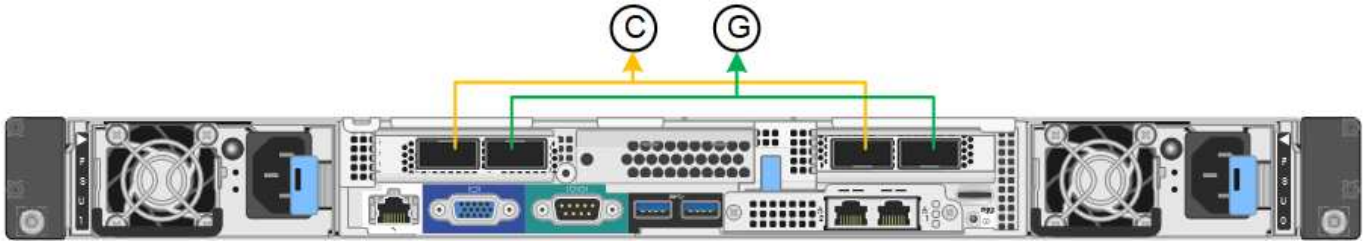
Modo de ligação de porta fixa

O modo de ligação de porta fixa é a configuração padrão para as portas de rede.

SG100 modo de ligação de porta fixa



SG1000 modo de ligação de porta fixa



	Quais portas estão coladas
C	As portas 1 e 3 são Unidas para a rede do cliente, se esta rede for utilizada.
G	As portas 2 e 4 são Unidas para a rede de Grade.

Ao usar o modo de ligação de porta fixa, as portas podem ser coladas usando o modo de backup ativo ou o modo de protocolo de controle de agregação de link (LACP 802,3ad).

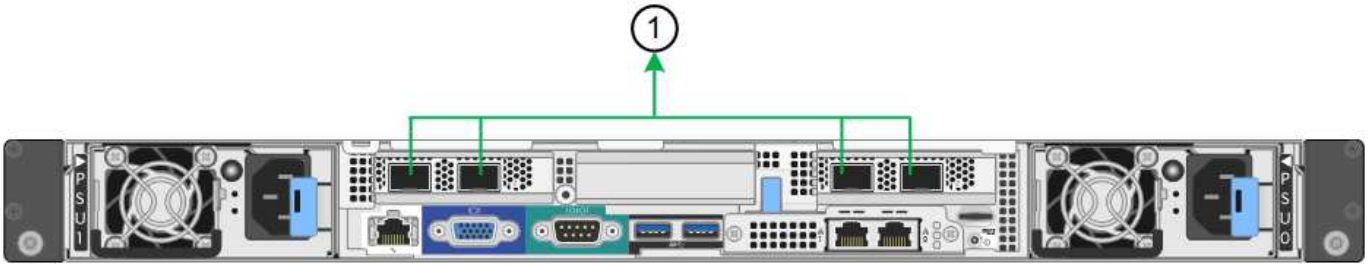
- No modo de backup ativo (padrão), apenas uma porta está ativa por vez. Se a porta ativa falhar, sua porta de backup fornecerá automaticamente uma conexão de failover. A porta 4 fornece um caminho de backup para a porta 2 (rede de Grade) e a porta 3 fornece um caminho de backup para a porta 1 (rede de cliente).
- No modo LACP, cada par de portas forma um canal lógico entre o dispositivo de serviços e a rede, permitindo uma maior taxa de transferência. Se uma porta falhar, a outra continua a fornecer o canal. A taxa de transferência é reduzida, mas a conetividade não é afetada.

> Se não precisar de ligações redundantes, pode utilizar apenas uma porta para cada rede. No entanto, esteja ciente de que o alerta **Assistente de Serviços para baixo** pode ser acionado no Gerenciador de Grade após a instalação do StorageGRID, indicando que um cabo está desconetado. Você pode desativar esta regra de alerta com segurança.

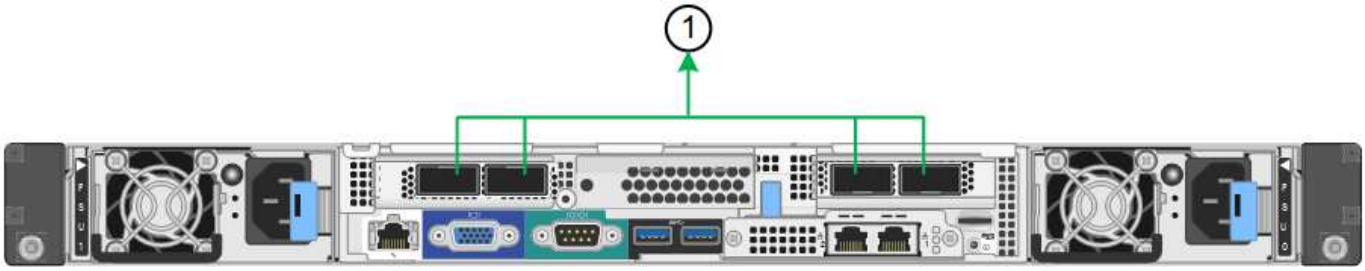
Modo de ligação de porta agregada

O modo de ligação de porta agregada aumenta significativamente a taxa de transferência para cada rede StorageGRID e fornece caminhos de failover adicionais.

SG100 modo de ligação de porta agregada



SG1000 modo de ligação de porta agregada



	Quais portas estão coladas
1	Todas as portas conetadas são agrupadas em uma única ligação LACP, permitindo que todas as portas sejam usadas para o tráfego de rede de Grade e rede de Cliente.

Se você planeja usar o modo de ligação de porta agregada:

- Você deve usar o modo de ligação de rede LACP.
- Você deve especificar uma tag VLAN exclusiva para cada rede. Essa tag VLAN será adicionada a cada pacote de rede para garantir que o tráfego de rede seja roteado para a rede correta.
- As portas devem ser conetadas a switches que possam suportar VLAN e LACP. Se vários switches estiverem participando da ligação LACP, os switches devem suportar grupos de agregação de links de vários gabinetes (MLAG) ou equivalente.
- Você deve entender como configurar os switches para usar VLAN, LACP e MLAG, ou equivalente.

Se você não quiser usar todas as quatro portas, você pode usar uma, duas ou três portas. O uso de mais de uma porta maximiza a chance de que alguma conetividade de rede permaneça disponível se uma das portas falhar.

> Se você optar por usar menos de quatro portas de rede, esteja ciente de que um alerta de link do dispositivo de serviços desativado* pode ser acionado no Gerenciador de Grade depois que o nó do dispositivo for instalado, indicando que um cabo está desconetado. Pode desativar esta regra de alerta com segurança para o alerta acionado.

Modos de ligação de rede para as portas de gestão

Para as duas portas de gerenciamento de 1 GbE no dispositivo de serviços, você pode escolher o modo de ligação de rede independente ou o modo de ligação de rede ative-Backup para se conetar à rede Admin opcional.

SG100 portas de gerenciamento de rede

SG1000 portas de gerenciamento de rede

No modo independente, apenas a porta de gerenciamento à esquerda está conetada à rede de administração. Este modo não fornece um caminho redundante. A porta de gerenciamento à direita está desconetada e disponível para conexões locais temporárias (usa o endereço IP 169.254.0.1)

No modo ative-Backup, ambas as portas de gerenciamento estão conetadas à rede Admin. Apenas uma porta está ativa de cada vez. Se a porta ativa falhar, sua porta de backup fornecerá automaticamente uma conexão de failover. A ligação dessas duas portas físicas em uma porta de gerenciamento lógico fornece um caminho redundante para a rede de administração.

> Se você precisar fazer uma conexão local temporária com o dispositivo de serviços quando as portas de gerenciamento de 1 GbE estiverem configuradas para o modo ative-Backup, remova os cabos de ambas as portas de gerenciamento, conete o cabo temporário à porta de gerenciamento à direita e acesse o dispositivo usando o endereço IP 169.254.0.1.

	Modo de ligação de rede
A	Modo ative-Backup (cópia de segurança ativa). Ambas as portas de gerenciamento são ligadas a uma porta de gerenciamento lógico conetada à rede de administração.
I	Modo independente. A porta à esquerda está ligada à rede de administração. A porta à direita está disponível para conexões locais temporárias (endereço IP 169.254.0.1).

Recolha de informações de instalação (SG100 e SG1000)

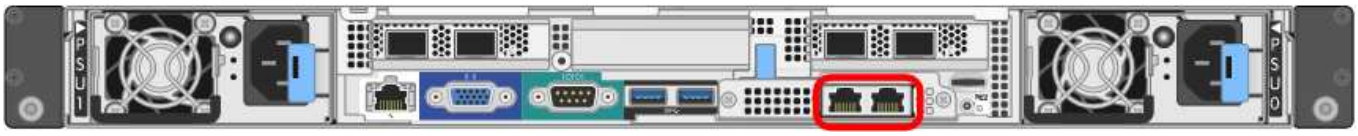
À medida que você instala e configura o dispositivo StorageGRID, você deve tomar decisões e coletar informações sobre portas de switch Ethernet, endereços IP e modos de ligação de porta e rede. Registe as informações necessárias para cada rede que ligar ao aparelho. Esses valores são necessários para instalar e configurar o hardware.

Portas de administração e manutenção

A rede de administração para StorageGRID é uma rede opcional, usada para administração e manutenção do

sistema. O dispositivo se coneta à rede Admin usando as seguintes portas de gerenciamento de 1 GbE no dispositivo.

SG100 portas RJ-45



SG1000 portas RJ-45

Conexões de administração e manutenção

Informações necessárias	O seu valor
Rede de administração ativada	Escolha uma: • Não • Sim (predefinição)
Modo de ligação de rede	Escolha uma: • Independente (predefinição) • Ative-Backup
Porta do switch para a porta esquerda circulada no diagrama (porta ativa padrão para o modo de ligação de rede independente)	
Porta do switch para a porta direita circulada no diagrama (apenas modo de ligação de rede ative-Backup)	

Informações necessárias	O seu valor
Endereço MAC para a porta Admin Network **Nota:** a etiqueta de endereço MAC na parte frontal do dispositivo lista o endereço MAC da porta de gerenciamento BMC. Para determinar o endereço MAC da porta Admin Network, você deve adicionar **2** ao número hexadecimal na etiqueta. Por exemplo, se o endereço MAC na etiqueta terminar em **09**, o endereço MAC da porta Admin terminaria em **0B**. Se o endereço MAC na etiqueta terminar em **(*y*)FF**, o endereço MAC da porta Admin terminaria em **(*y*(1)01**. Você pode facilmente fazer esse cálculo abrindo o Calculator no Windows, definindo-o para o modo Programador, selecionando Hex, digitando o endereço MAC e, em seguida, digitando * 2 *.	
Endereço IP atribuído pelo DHCP para a porta Admin Network, se disponível após a ativação **Observação:** você pode determinar o endereço IP atribuído pelo DHCP usando o endereço MAC para procurar o IP atribuído.	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de dispositivo na rede Admin **Nota:** se a rede não tiver um gateway, especifique o mesmo endereço IPv4 estático para o gateway.	• Endereço IPv4 (CIDR): • Gateway:
Sub-redes de rede Admin (CIDR)	

Portas de rede

As quatro portas de rede no dispositivo se conetam à rede de grade StorageGRID e à rede de cliente opcional.

- Conexões de rede*

Informações necessárias	O seu valor
Velocidade da ligação	Para o SG100, escolha uma das seguintes opções: • Auto (predefinição) • 10 GbE • 25 GbE Para o SG1000, escolha uma das seguintes opções: • Auto (predefinição) • 10 GbE • 25 GbE • 40 GbE • 100 GbE **Nota:** para as velocidades de SG1000, 10 e 25 GbE requerem o uso de adaptadores QSA.
Modo de ligação da porta	Escolha uma: • Fixo (padrão) • Agregado
Porta do switch para a porta 1 (rede do cliente para o modo fixo)	
Porta do switch para a porta 2 (rede de grade para modo fixo)	
Porta do switch para a porta 3 (rede do cliente para o modo fixo)	
Porta do switch para a porta 4 (rede de grade para modo fixo)	

Portas de rede de grade

A rede de Grade para StorageGRID é uma rede necessária, usada para todo o tráfego interno de StorageGRID. O dispositivo se coneta à rede de grade usando as quatro portas de rede.

- Conexões de rede de grade*

Informações necessárias	O seu valor
Modo de ligação de rede	Escolha uma: • Ative-Backup (padrão) • Bola de Futsal (802,3ad)
Marcação de VLAN ativada	Escolha uma: • Não (predefinição) • Sim
Tag VLAN (se a marcação VLAN estiver ativada)	Introduza um valor entre 0 e 4095:
Endereço IP atribuído pelo DHCP para a rede de Grade, se disponível após a ativação	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de dispositivo na rede de grelha **Nota:** se a rede não tiver um gateway, especifique o mesmo endereço IPv4 estático para o gateway.	• Endereço IPv4 (CIDR): • Gateway:
Sub-redes de rede de rede (CIDR)	
Configuração da unidade de transmissão máxima (MTU) (opcional) você pode usar o valor padrão de 1500, ou definir a MTU para um valor adequado para quadros jumbo, como 9000.	

Portas de rede do cliente

A rede de cliente para StorageGRID é uma rede opcional, normalmente usada para fornecer acesso de protocolo de cliente à grade. O dispositivo se coneta à rede do cliente usando as quatro portas de rede.

Conexões de rede de clientes

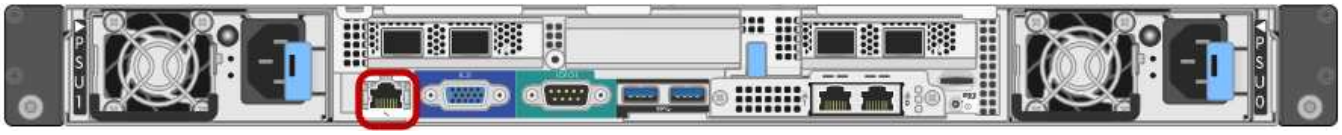
Informações necessárias	O seu valor
Rede cliente ativada	Escolha uma: • Não (predefinição) • Sim
Modo de ligação de rede	Escolha uma: • Ative-Backup (padrão) • Bola de Futsal (802,3ad)

Informações necessárias	O seu valor
Marcação de VLAN ativada	Escolha uma: • Não (predefinição) • Sim
Tag VLAN (se a marcação VLAN estiver ativada)	Introduza um valor entre 0 e 4095:
Endereço IP atribuído pelo DHCP para a rede do cliente, se disponível após a ligação	• Endereço IPv4 (CIDR): • Gateway:
Endereço IP estático que pretende utilizar para o nó de dispositivo na rede Cliente **Nota:** se a rede do cliente estiver ativada, a rota padrão no dispositivo usará o gateway especificado aqui.	• Endereço IPv4 (CIDR): • Gateway:

Portas de rede de gerenciamento BMC

Você pode acessar a interface BMC no utilitário de serviços usando a porta de gerenciamento de 1 GbE circulada no diagrama. Esta porta suporta a gestão remota do hardware do controlador através de Ethernet, utilizando a norma IPMI (Intelligent Platform Management Interface).

SG100 porta de gerenciamento BMC



SG1000 porta de gerenciamento BMC

Conexões de rede de gerenciamento BMC

Informações necessárias	O seu valor
Porta do switch Ethernet, você se conetará à porta de gerenciamento BMC (circulada no diagrama)	
Endereço IP atribuído por DHCP para a rede de gerenciamento BMC, se disponível após a inicialização	• Endereço IPv4 (CIDR): • Gateway:

Informações necessárias	O seu valor
Endereço IP estático que pretende utilizar para a porta de gestão BMC	• Endereço IPv4 (CIDR): • Gateway:

Informações relacionadas

"Visão geral dos aparelhos SG100 e SG1000"

"Cabeamento do dispositivo SG100 e SG1000)"

"Configurando endereços IP do StorageGRID"

Instalar o hardware

A instalação de hardware implica a instalação do aparelho em um gabinete ou rack, a conexão dos cabos e a aplicação de energia.

Passos

- "Registar o hardware"
- "Instalar o aparelho em um gabinete ou rack (SG100 e SG1000)"
- "Cabeamento do dispositivo SG100 e SG1000)"
- "Conexão dos cabos de alimentação e alimentação (SG100 e SG1000)"
- "Visualização de indicadores de status nos aparelhos SG100 e SG1000"

Registar o hardware

Registrar o hardware do aparelho fornece benefícios de suporte.

Passos

1. Localize o número de série do chassis do aparelho.

   Pode encontrar o número no folheto de embalagem, no seu e-mail de confirmação ou no aparelho depois de o desembalar.

2. Vá para o site de suporte da NetApp em "mysupport.NetApp.com".
3. Determine se você precisa Registrar o hardware:

Se você é um…	Siga estes passos…
Cliente NetApp existente	a. Inicie sessão com o seu nome de utilizador e palavra-passe. b. Selecione **Produtos Meus Produtos**. c. Confirme se o novo número de série está listado. d. Se não estiver, siga as instruções para novos clientes NetApp.
Novo cliente da NetApp	a. Clique em **Registe-se agora** e crie uma conta. b. Selecione **Produtos Registe produtos**. c. Insira o número de série do produto e os detalhes solicitados. Após a aprovação do seu registo, pode transferir qualquer software necessário. O processo de aprovação pode demorar até 24 horas.

Instalar o aparelho em um gabinete ou rack (SG100 e SG1000)

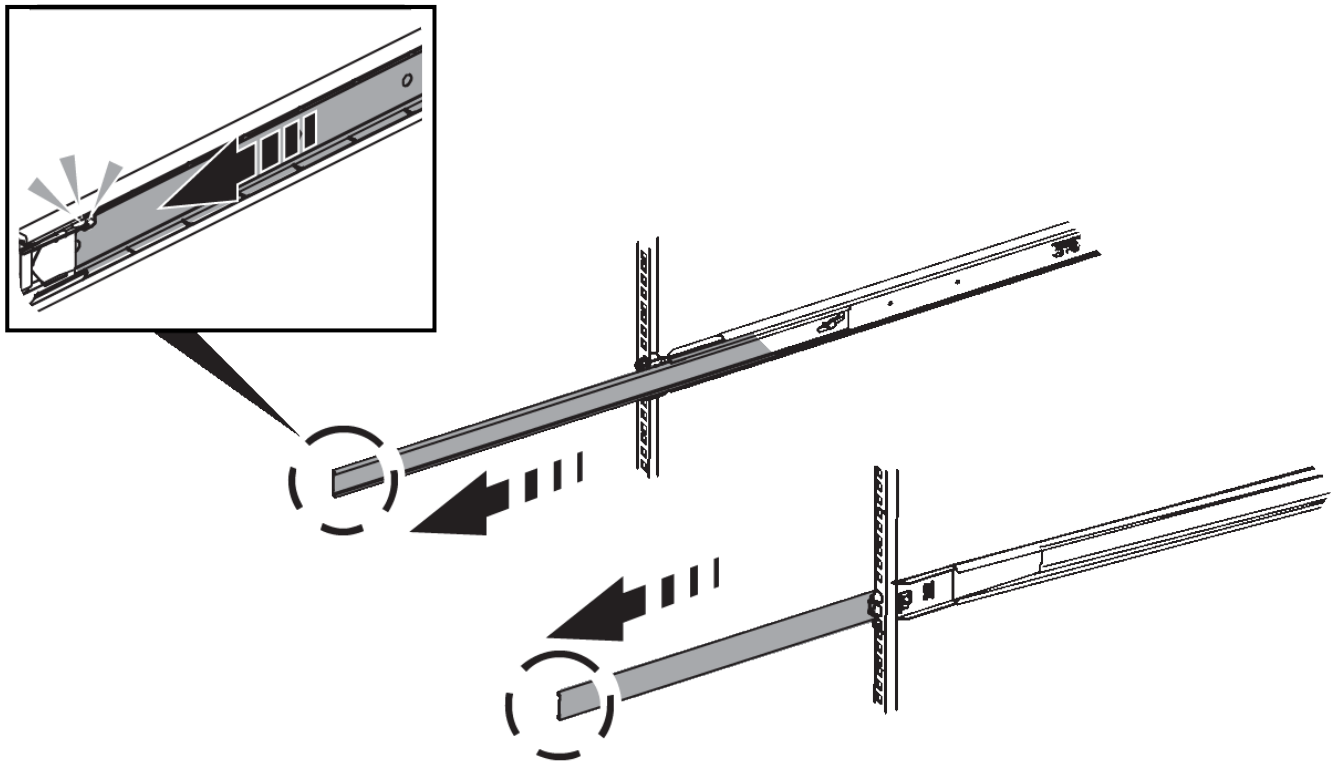
Tem de instalar um conjunto de calhas para o aparelho no seu armário ou rack e, em seguida, deslizar o aparelho para os trilhos.

O que você vai precisar

- Você revisou o documento de Avisos de segurança incluído na caixa e entendeu as precauções para mover e instalar hardware.
- Você tem as instruções fornecidas com o kit de trilho.

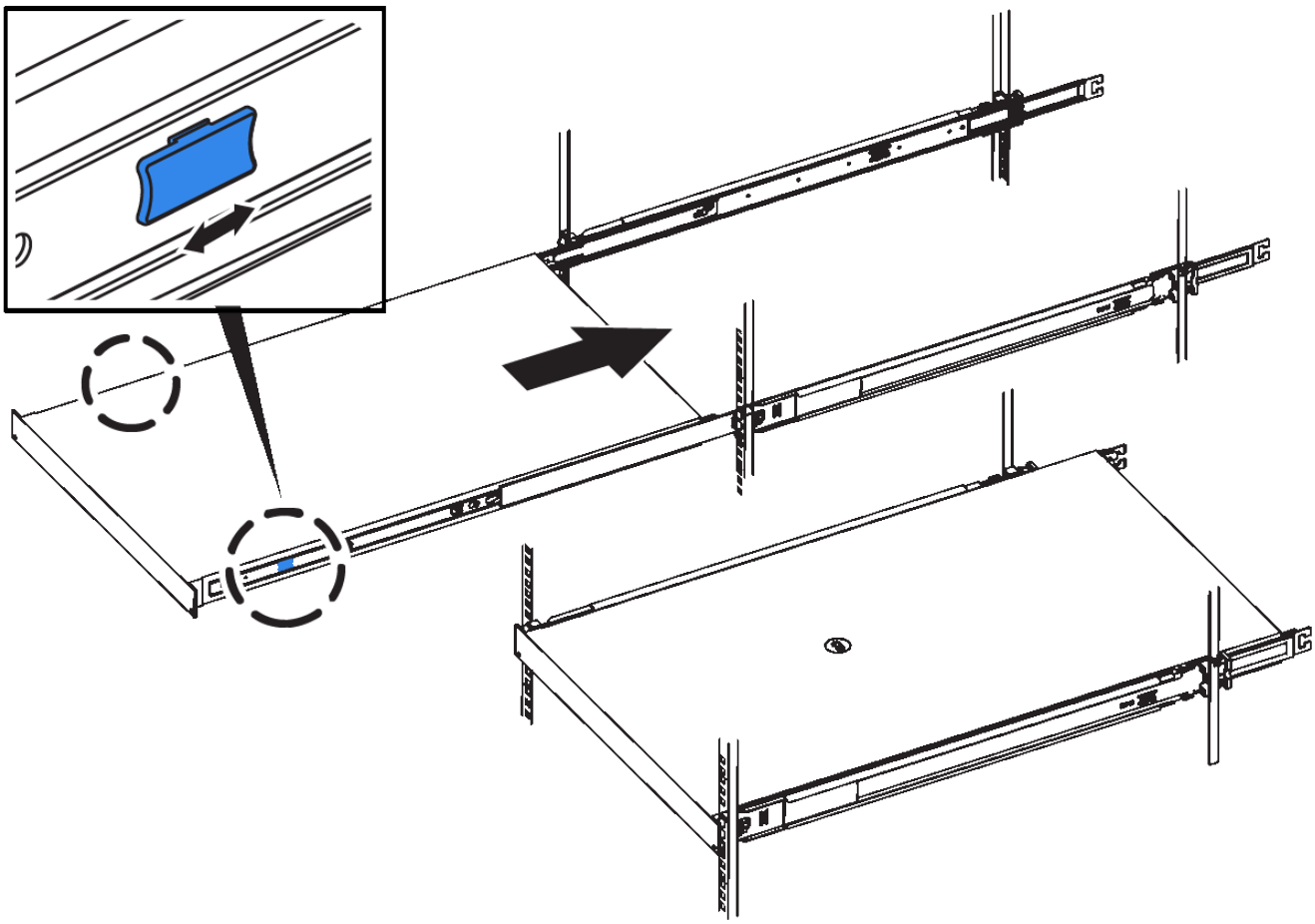
Passos

1. Siga cuidadosamente as instruções para o kit de trilho para instalar os trilhos em seu gabinete ou rack.
2. Nos dois trilhos instalados no gabinete ou rack, estenda as partes móveis dos trilhos até ouvir um clique.



3. Introduza o aparelho nas calhas.
4. Deslize o aparelho para dentro do gabinete ou rack.

   Quando não conseguir mover o aparelho mais, puxe os trincos azuis em ambos os lados do chassis para fazer deslizar o aparelho completamente para dentro.



Não ligue a moldura frontal até que o aparelho seja ligado.

Cabeamento do aparelho SG100 e SG1000

Você deve conetar a porta de gerenciamento do dispositivo ao laptop de serviço e conetar as portas de rede do dispositivo à rede de grade e à rede de cliente opcional para StorageGRID.

O que você vai precisar

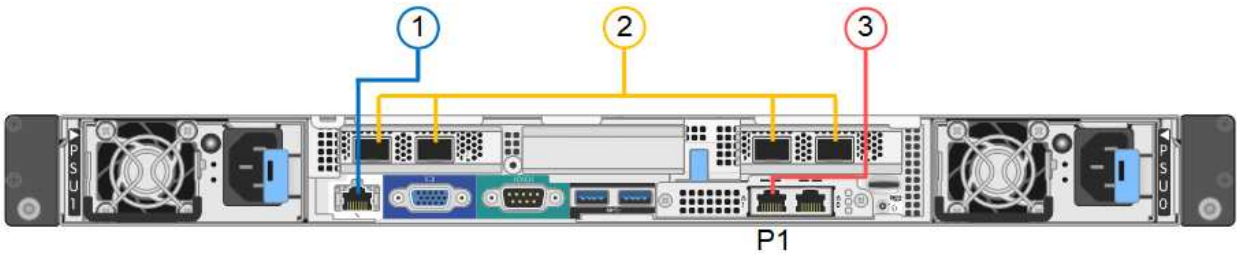
- Você tem um cabo Ethernet RJ-45 para conetar a porta de gerenciamento.
- Tem uma das seguintes opções para as portas de rede. Estes itens não são fornecidos com o aparelho.
  - Um a quatro cabos Twinax para ligar as quatro portas de rede.
  - Para o SG100, um a quatro transcetores SFP ou SFP28 se você planeja usar cabos óticos para as portas.
  - Para o SG1000, um a quatro transcetores QSFP ou QSFP28 se você planeja usar cabos óticos para as portas.

Risco de exposição à radiação laser — não desmonte nem remova qualquer parte de um transcetor SFP ou QSFP. Você pode estar exposto à radiação laser.

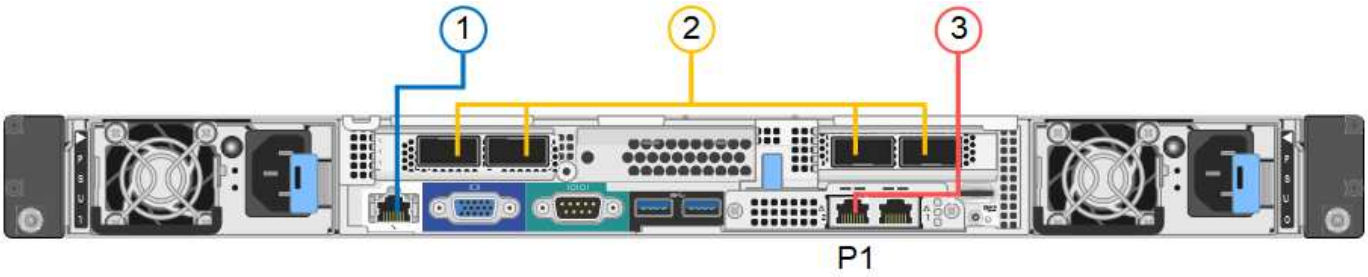
Sobre esta tarefa

As figuras a seguir mostram as portas na parte traseira do aparelho.

- SG100 conexões de porta*



- SG1000 conexões de porta*



	Porta	Tipo de porta	Função
1	Porta de gerenciamento BMC no dispositivo	1 GbE (RJ-45)	Liga-se à rede onde acede à interface BMC.
2	Quatro portas de rede no dispositivo	• Para o SG100: 10/25-GbE • Para o SG1000: 10/25/40/100-GbE	Conete-se à rede de grade e à rede de cliente para StorageGRID.
3	Porta de rede de administração no dispositivo (identificada como P1 nas figuras)	1 GbE (RJ-45) **Importante:** esta porta funciona apenas a 1000 BaseT/full e não suporta velocidades de 10 ou 100 megabits.	Liga o dispositivo à rede de administração para StorageGRID.
3	Porta RJ-45 mais à direita no aparelho	1 GbE (RJ-45) **Importante:** esta porta funciona apenas a 1000 BaseT/full e não suporta velocidades de 10 ou 100 megabits.	• Pode ser ligado com a porta de gerenciamento 1 se você quiser uma conexão redundante com a rede de administração. • Pode ser deixado desconetado e disponível para acesso local temporário (IP 169.254.0.1). • Durante a instalação, pode ser utilizado para ligar o dispositivo a um computador portátil de serviço se os endereços IP atribuídos por DHCP não estiverem disponíveis.

Passos

1. Conete a porta de gerenciamento BMC do dispositivo à rede de gerenciamento, usando um cabo Ethernet.

   Embora essa conexão seja opcional, recomenda-se facilitar o suporte.

2. Ligue as portas de rede do aparelho aos comutadores de rede adequados, utilizando cabos Twinax ou cabos óticos e transcetores.

   > As quatro portas de rede devem usar a mesma velocidade de link. Consulte as tabelas a seguir para saber o equipamento necessário com base no hardware e na velocidade da ligação.

Velocidade da ligação de SG100 (GbE)	Equipamento necessário
10	Transceptor SFP
25	Transcetor SFP28
Velocidade da ligação de SG1000 (GbE)	Equipamento necessário
10	Transceptor QSA e SFP
25	Transcetor QSA e SFP28
40	Transceptor QSFP
100	Transcetor QFSP28

   - Se você planeja usar o modo de ligação de porta fixa (padrão), conete as portas à rede StorageGRID e às redes de clientes, conforme mostrado na tabela.

Porta	Liga a…
Porta 1	Rede cliente (opcional)
Porta 2	Rede de rede
Porta 3	Rede cliente (opcional)
Porta 4	Rede de rede

   - Se você planeja usar o modo de ligação de porta agregada, conete uma ou mais portas de rede a um ou mais switches. Você deve conetar pelo menos duas das quatro portas para evitar ter um único ponto de falha. Se você usar mais de um switch para uma única ligação LACP, os switches devem suportar MLAG ou equivalente.

3. Se pretender utilizar a rede de administração para StorageGRID, ligue a porta de rede de administração do dispositivo à rede de administração, utilizando um cabo Ethernet.

Conexão dos cabos de alimentação e alimentação (SG100 e SG1000)

Depois de ligar os cabos de rede, está pronto para ligar a alimentação ao aparelho.

Passos

1. Ligue um cabo de alimentação a cada uma das duas fontes de alimentação do aparelho.
2. Conete esses dois cabos de alimentação a duas unidades de distribuição de energia (PDUs) diferentes no gabinete ou no rack.
3. Se o botão liga/desliga na parte frontal do aparelho não estiver aceso a azul, prima o botão para ligar o aparelho.

   Não volte a premir o botão de alimentação durante o processo de ativação.

4. Se ocorrerem erros, corrija quaisquer problemas.
5. Fixe a moldura frontal ao aparelho.

Informações relacionadas

"Visualização de indicadores de status nos aparelhos SG100 e SG1000"

Visualização de indicadores de status nos aparelhos SG100 e SG1000

O dispositivo inclui indicadores que o ajudam a determinar o status do controlador do dispositivo e dos dois SSDs.

Indicadores e botões do aparelho

	Visor	Estado
1	Botão de alimentação	• Azul: O aparelho está ligado. • Desligado: O aparelho está desligado.
2	Botão Reset (Repor)	Utilize este botão para executar uma reinicialização total do controlador.
3	Botão identificar	Este botão pode ser definido como intermitente, ligado (sólido) ou desligado. • Azul intermitente: Identifica o aparelho no gabinete ou rack. • Azul, sólido: Identifica o aparelho no gabinete ou rack. • Desligado: O aparelho não é visualmente identificável no gabinete ou no rack.

	Visor	Estado
4	LED de alarme	• Âmbar, sólido: Ocorreu um erro. **Nota:** para visualizar os códigos de inicialização e erro, você deve acessar a interface do BMC. • Desligado: Nenhum erro está presente.

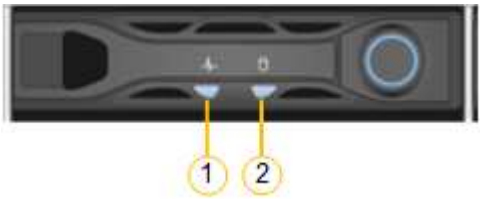
Códigos gerais de arranque

Durante a inicialização ou após uma reinicialização forçada do aparelho, ocorre o seguinte:

1. O controlador de gerenciamento de placa base (BMC) Registra códigos para a sequência de inicialização, incluindo quaisquer erros que ocorram.
2. O botão liga/desliga acende-se.
3. Se ocorrerem erros durante a inicialização, o LED de alarme acende-se.

   Para exibir os códigos de inicialização e erro, você deve acessar a interface do BMC.

Indicadores SSD



LED	Visor	Estado
1	Estado/avaria da transmissão	• Azul (sólido): A unidade está online • Âmbar (intermitente): Falha da unidade • Desligado: A ranhura está vazia
2	Condução ativa	Azul (intermitente): A unidade está a ser acedida

Informações relacionadas

"Solução de problemas da instalação do hardware"

"Configurando a interface BMC"

Configurando conexões StorageGRID

Antes de implantar o dispositivo de serviços como um nó em um sistema StorageGRID,

você deve configurar as conexões entre o dispositivo e as redes que você planeja usar. Você pode configurar a rede navegando até o Instalador de dispositivos StorageGRID, que está pré-instalado no utilitário de serviços.

Passos

- "Acessando o instalador do StorageGRID Appliance"
- "Verificando e atualizando a versão do Instalador de dispositivos StorageGRID"
- "Configuração de links de rede (SG100 e SG1000)"
- "Configurando endereços IP do StorageGRID"
- "Verificando conexões de rede"
- "Verificando conexões de rede no nível da porta"

Acessando o instalador do StorageGRID Appliance

Você deve acessar o Instalador do StorageGRID Appliance para configurar as conexões entre o appliance e as três redes StorageGRID: A rede de grade, a rede de administração (opcional) e a rede de cliente (opcional).

O que você vai precisar

- Você está usando qualquer cliente de gerenciamento que possa se conetar à rede de administração do StorageGRID.
- O cliente tem um navegador da Web suportado.
- O dispositivo de serviços está conetado a todas as redes StorageGRID que você planeja usar.
- Você sabe o endereço IP, o gateway e a sub-rede do utilitário de serviços nessas redes.
- Configurou os comutadores de rede que pretende utilizar.

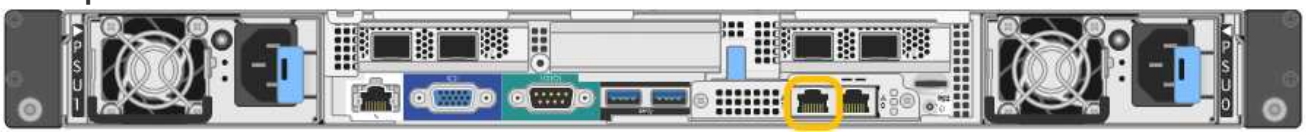
Sobre esta tarefa

Para acessar inicialmente o Instalador de dispositivos StorageGRID, você pode usar o endereço IP atribuído por DHCP para a porta de rede Admin no utilitário de serviços (supondo que ele esteja conetado à rede Admin), ou você pode conetar um laptop de serviço diretamente ao utilitário de serviços.

Passos

1. Se possível, use o endereço DHCP para a porta de rede de administrador no utilitário de serviços para acessar o instalador do dispositivo StorageGRID.

   SG100 porta de rede Admin

   SG1000 porta de rede Admin

   a. Localize a etiqueta de endereço MAC na parte frontal do dispositivo serrvices e determine o endereço

MAC da porta Admin Network.

O rótulo de endereço MAC lista o endereço MAC da porta de gerenciamento BMC.

Para determinar o endereço MAC da porta Admin Network, você deve adicionar **2** ao número hexadecimal na etiqueta. Por exemplo, se o endereço MAC na etiqueta terminar em **09**, o endereço MAC da porta Admin terminaria em **0B**. Se o endereço MAC na etiqueta terminar em **(*y*)FF**, o endereço MAC da porta Admin terminaria em **(*y*(1)01**. Você pode facilmente fazer esse cálculo abrindo o Calculator no Windows, definindo-o para o modo Programador, selecionando Hex, digitando o endereço MAC e, em seguida, digitando * 2 *.

b. Forneça o endereço MAC ao administrador da rede para que ele possa procurar o endereço DHCP do dispositivo na rede Admin.

c. No cliente, insira esta URL para o instalador do StorageGRID Appliance
`https://services-appliance_IP:8443`

Para *`services-appliance_IP`*, utilize o endereço DHCP.

d. Se for solicitado um alerta de segurança, exiba e instale o certificado usando o assistente de instalação do navegador.

O alerta não aparecerá na próxima vez que você acessar este URL.

A página inicial do instalador do dispositivo StorageGRID é exibida. As informações e as mensagens mostradas quando você acessa esta página pela primeira vez dependem de como o dispositivo está conetado atualmente às redes StorageGRID. Podem aparecer mensagens de erro que serão resolvidas em etapas posteriores.

2. Em alternativa, se não conseguir obter um endereço IP utilizando DHCP, utilize uma ligação local para aceder ao Instalador de aplicações StorageGRID.

a. Conete um laptop de serviço diretamente à porta RJ-45 mais à direita do dispositivo de serviços, usando um cabo Ethernet.

SG100 ligação local

SG1000 ligação local

b. Abra um navegador da Web.

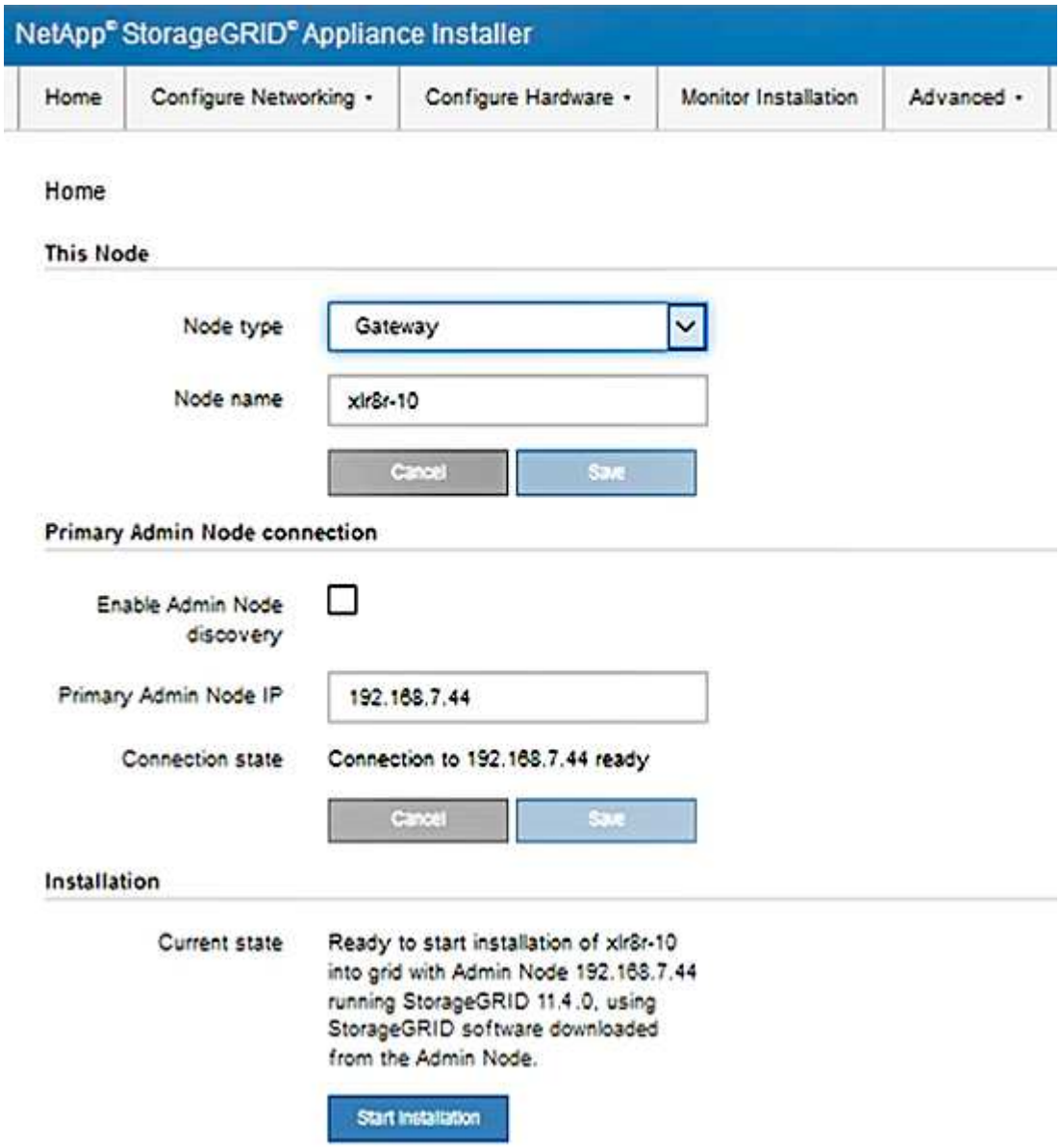
c. Digite este URL para o instalador do StorageGRID Appliance
`https://169.254.0.1:8443`

A página inicial do instalador do dispositivo StorageGRID é exibida. As informações e as mensagens mostradas quando você acessa esta página pela primeira vez dependem de como o dispositivo está conetado atualmente às redes StorageGRID. Podem aparecer mensagens de erro que serão

resolvidas em etapas posteriores.

> Se não conseguir aceder à página inicial através de uma ligação local, configure o endereço IP do computador portátil de serviço como `169.254.0.2`, e tente novamente.

3. Reveja as mensagens apresentadas na página inicial e configure a configuração da ligação e a configuração IP, conforme necessário.



Informações relacionadas

"Requisitos do navegador da Web"

Verificando e atualizando a versão do Instalador de dispositivos StorageGRID

A versão do Instalador de dispositivos StorageGRID no dispositivo deve corresponder à versão de software instalada no sistema StorageGRID para garantir que todos os recursos do StorageGRID sejam suportados.

O que você vai precisar

Você acessou o Instalador de dispositivos StorageGRID.

Sobre esta tarefa

Os dispositivos StorageGRID vêm da fábrica pré-instalados com o Instalador de dispositivos StorageGRID. Se você estiver adicionando um dispositivo a um sistema StorageGRID atualizado recentemente, talvez seja necessário atualizar manualmente o Instalador de dispositivos StorageGRID antes de instalar o dispositivo como um novo nó.

O Instalador de dispositivos StorageGRID é atualizado automaticamente quando você atualiza para uma nova versão do StorageGRID. Não é necessário atualizar o Instalador de dispositivos StorageGRID nos nós de dispositivos instalados. Este procedimento só é necessário quando estiver a instalar um dispositivo que contenha uma versão anterior do Instalador de dispositivos StorageGRID.

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Avançado Atualização de firmware**.
2. Compare a versão atual do firmware com a versão de software instalada no seu sistema StorageGRID (no Gerenciador de Grade, selecione **Ajuda sobre**).

   O segundo dígito nas duas versões deve corresponder. Por exemplo, se o seu sistema StorageGRID estiver executando a versão 11.**5**.*x*.*y*, a versão do Instalador de dispositivos StorageGRID deve ser 3.**5**.*z*.

3. Se o aparelho tiver uma versão de nível inferior do instalador do dispositivo StorageGRID, vá para a página de downloads do NetApp para StorageGRID.

   "NetApp Downloads: StorageGRID"

   Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.

4. Baixe a versão apropriada do arquivo **suporte para dispositivos StorageGRID** e o arquivo de checksum correspondente.

   O arquivo de suporte para dispositivos StorageGRID é um `.zip` arquivo que contém as versões de firmware atuais e anteriores para todos os modelos de dispositivos StorageGRID, em subdiretórios para cada tipo de controlador.

   Depois de baixar o arquivo de suporte para o arquivo de dispositivos StorageGRID, extraia o `.zip` arquivo e consulte o arquivo README para obter informações importantes sobre a instalação do Instalador de dispositivos StorageGRID.

5. Siga as instruções na página Atualizar firmware do Instalador de dispositivos StorageGRID para executar estas etapas:
   a. Carregue o ficheiro de suporte apropriado (imagem de firmware) para o seu tipo de controlador e o ficheiro de checksum.
   b. Atualize a partição inativa.
   c. Reinicie e troque partições.
   d. Atualize a segunda partição.

Informações relacionadas

"Acessando o instalador do StorageGRID Appliance"

Configuração de links de rede (SG100 e SG1000)

Você pode configurar links de rede para as portas usadas para conetar o dispositivo à rede de Grade, à rede de cliente e à rede de administração. Você pode definir a velocidade do link, bem como os modos de ligação de porta e rede.

O que você vai precisar

- Você obteve o equipamento adicional necessário para o seu tipo de cabo e velocidade de ligação.
- Você conetou as portas de rede a switches que suportam a velocidade escolhida.

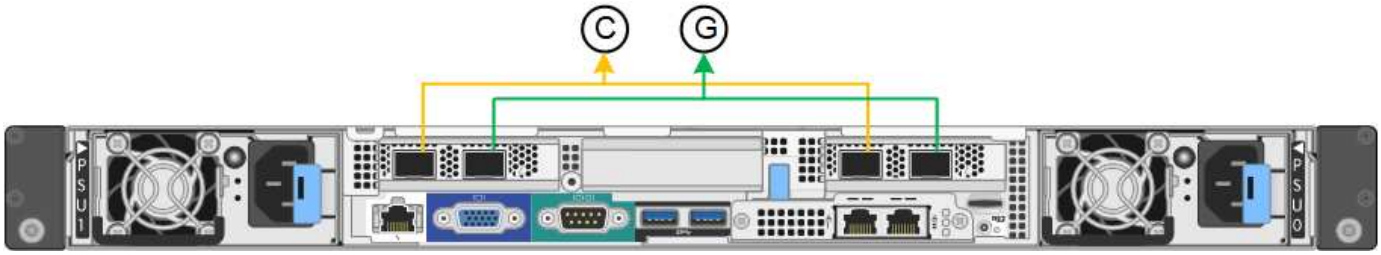
Se você planeja usar o modo de ligação de porta agregada, o modo de ligação de rede LACP ou a marcação de VLAN:

- Você conetou as portas de rede do dispositivo a switches que podem suportar VLAN e LACP.
- Se vários switches estiverem participando da ligação LACP, os switches suportam grupos de agregação de links de vários gabinetes (MLAG) ou equivalente.
- Você entende como configurar os switches para usar VLAN, LACP e MLAG ou equivalente.
- Você conhece a tag VLAN exclusiva a ser usada para cada rede. Essa tag VLAN será adicionada a cada pacote de rede para garantir que o tráfego de rede seja roteado para a rede correta.

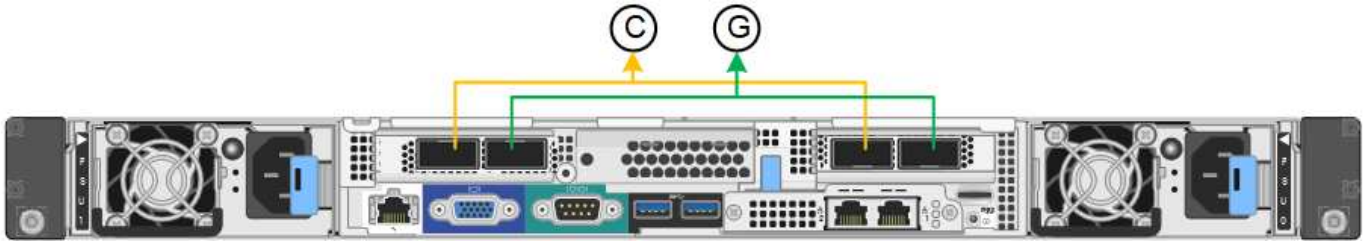
Sobre esta tarefa

As figuras mostram como as quatro portas de rede são ligadas no modo de ligação de porta fixa (configuração padrão).

SG100 modo de ligação de porta fixa



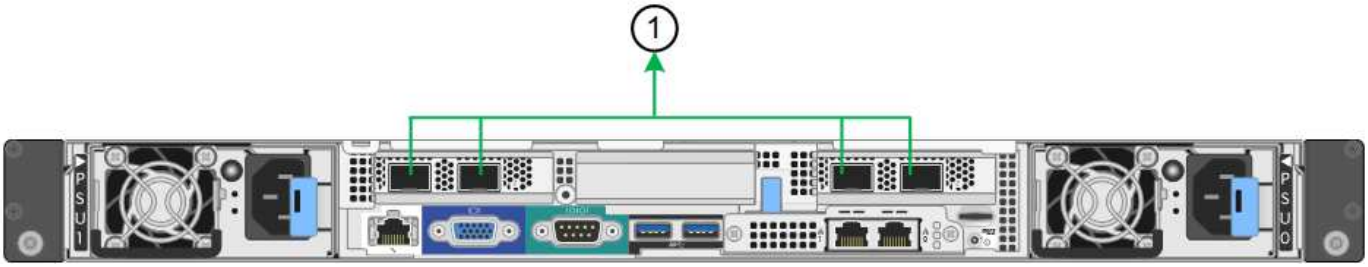
SG1000 modo de ligação de porta fixa



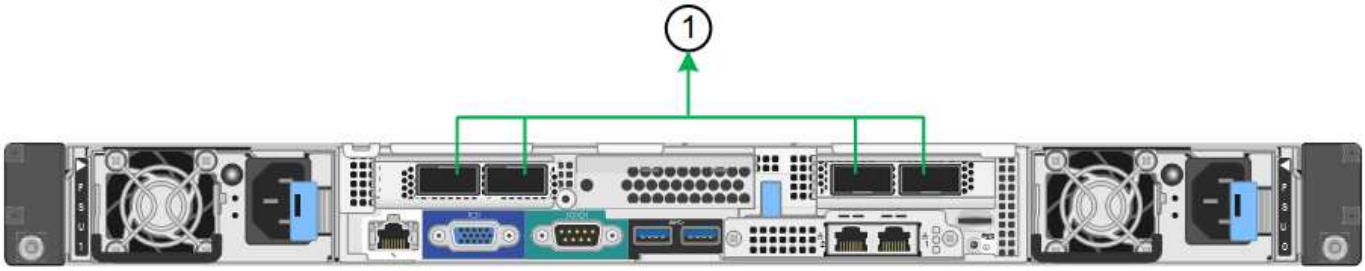
	Quais portas estão coladas
C	As portas 1 e 3 são Unidas para a rede do cliente, se esta rede for utilizada.
G	As portas 2 e 4 são Unidas para a rede de Grade.

Esta figura mostra como as quatro portas de rede são ligadas no modo de ligação de porta agregada.

SG100 modo de ligação de porta agregada



SG1000 modo de ligação de porta agregada



	Quais portas estão coladas
1	Todas as quatro portas são agrupadas em uma única ligação LACP, permitindo que todas as portas sejam usadas para o tráfego de rede de Grade e rede de Cliente.

A tabela resume as opções de configuração das quatro portas de rede. As predefinições são apresentadas a negrito. Só é necessário configurar as definições na página Configuração de ligação se pretender utilizar uma definição não predefinida.

> ⓘ A política de hash de transmissão LACP é padrão para o modo layer2-3. Se necessário, você pode usar a API de Gerenciamento de Grade para alterá-la para o modo layer3-4.

- **Modo de ligação de porta fixo (padrão)**

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Ative-Backup (padrão)	• As portas 2 e 4 usam uma ligação de backup ativo para a rede de Grade. • As portas 1 e 3 não são usadas. • Uma etiqueta VLAN é opcional.	• As portas 2 e 4 usam uma ligação de backup ativo para a rede de Grade. • As portas 1 e 3 usam uma ligação de backup ativo para a rede do cliente. • Tags VLAN podem ser especificadas para ambas as redes para a conveniência do administrador de rede.

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Bola de Futsal (802,3ad)	• As portas 2 e 4 usam uma ligação LACP para a rede de Grade. • As portas 1 e 3 não são usadas. • Uma etiqueta VLAN é opcional.	• As portas 2 e 4 usam uma ligação LACP para a rede de Grade. • As portas 1 e 3 usam uma ligação LACP para a rede de clientes. • Tags VLAN podem ser especificadas para ambas as redes para a conveniência do administrador de rede.

- **Modo de ligação de porta agregada**

Modo de ligação de rede	Rede cliente desativada (predefinição)	Rede cliente ativada
Apenas LACP (802,3ad)	• As portas 1-4 usam uma única ligação LACP para a rede de Grade. • Uma única etiqueta VLAN identifica pacotes de rede de Grade.	• As portas 1-4 usam uma única ligação LACP para a rede de Grade e a rede do Cliente. • Duas etiquetas VLAN permitem que os pacotes de rede de Grade sejam segregados dos pacotes de rede de Cliente.

Para obter detalhes adicionais, consulte o artigo sobre conexões de portas GbE para o utilitário de serviços.

Esta figura mostra como as duas portas de gerenciamento de 1 GbE no SG100 são ligadas no modo de ligação de rede do ative-Backup para a rede de administração.

Estas figuras mostram como as duas portas de gerenciamento de 1 GbE no dispositivo são ligadas no modo de ligação de rede ative-Backup para a rede Admin.

SG100 portas de rede Admin ligadas

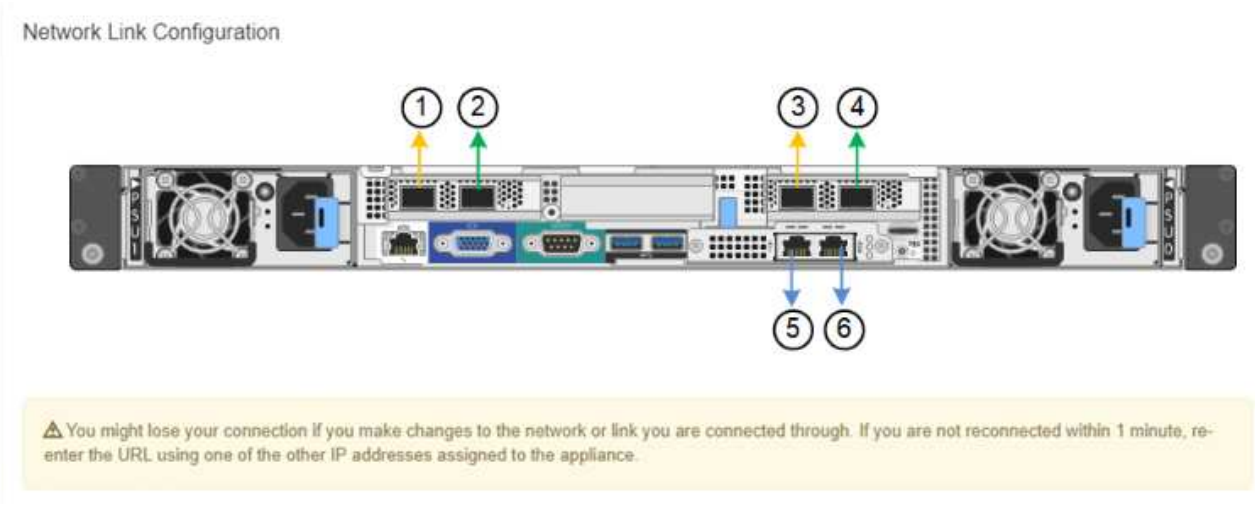
SG1000 portas de rede Admin ligadas

Passos

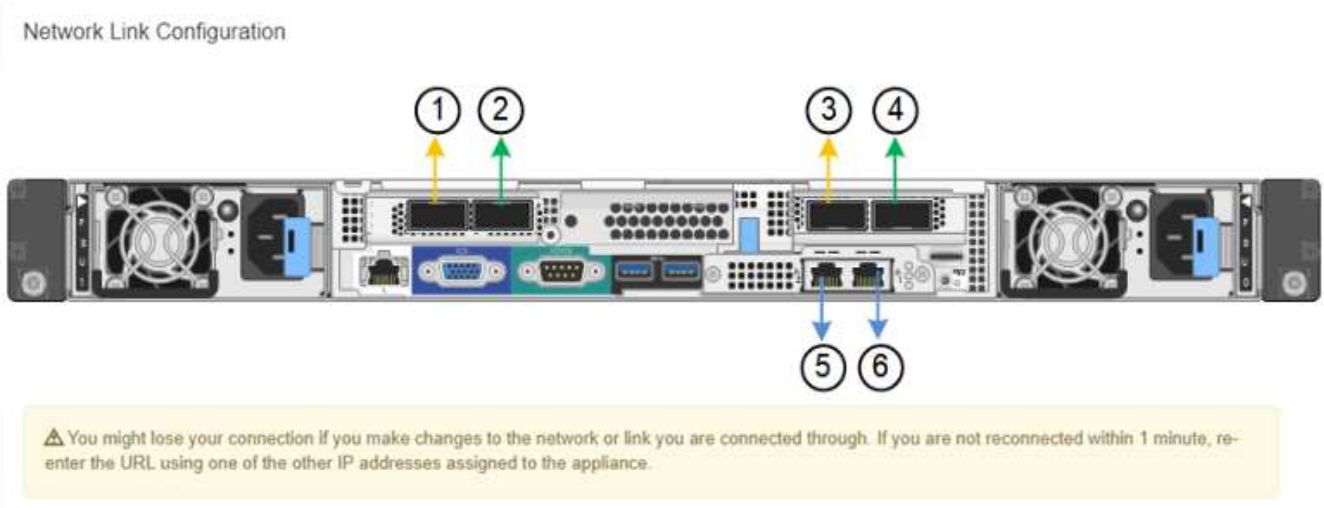
1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Configuração de ligação**.

   A página Network Link Configuration (Configuração da ligação de rede) apresenta um diagrama do seu dispositivo com as portas de rede e de gestão numeradas.

   SG100 portas



   SG1000 portas



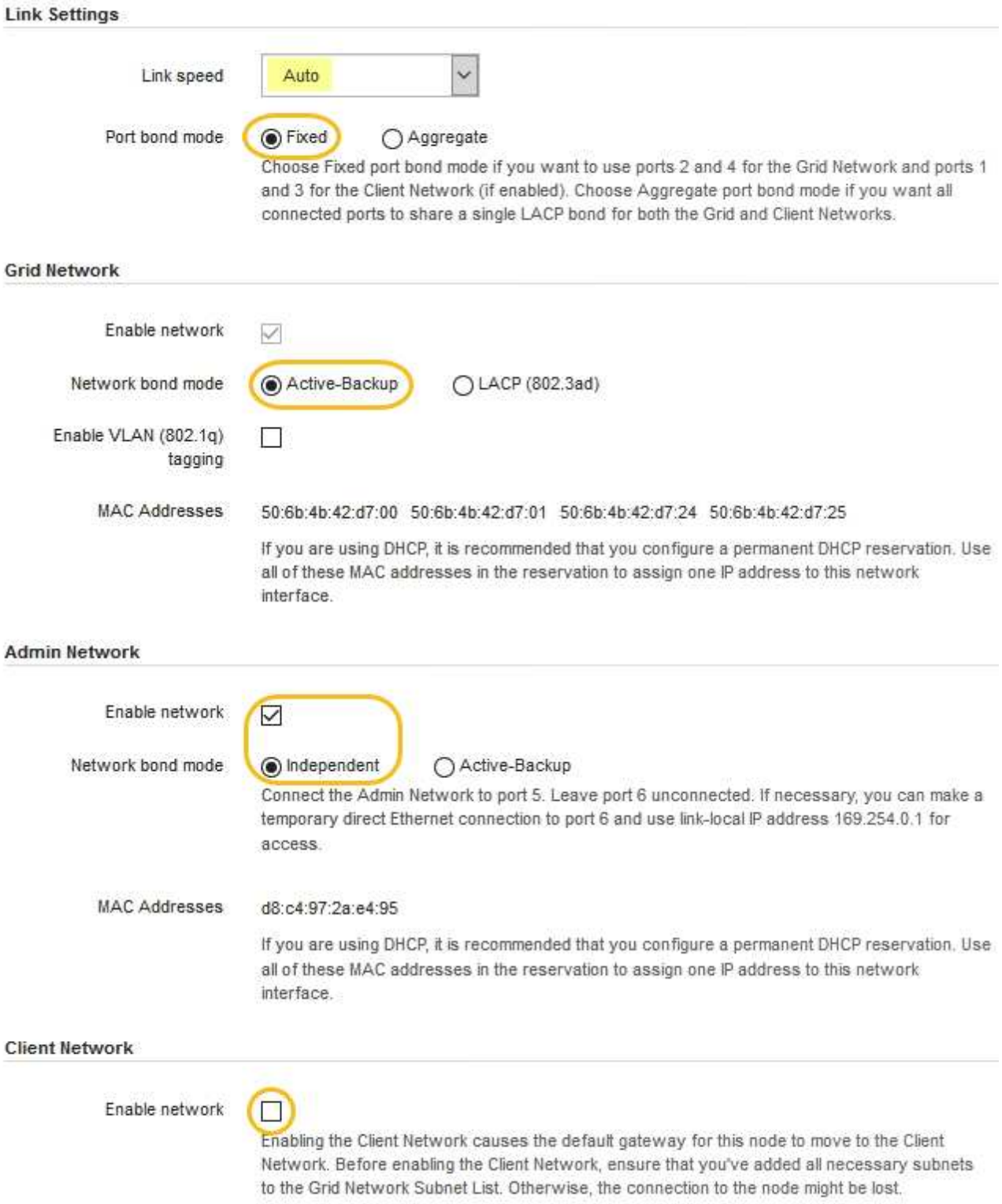
   A tabela Status do link lista o estado e a velocidade do link das portas numeradas (SG1000 mostradas).

Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Down	N/A
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

A primeira vez que aceder a esta página:

- **Link Speed** está definido para **Auto**.
- **Port bond mode** está definido como **Fixed**.
- **O modo de ligação de rede** está definido como **ative-Backup** para a rede de Grade.
- A **Admin Network** está ativada e o modo de ligação de rede está definido como **Independent**.
- A **rede do cliente** está desativada.



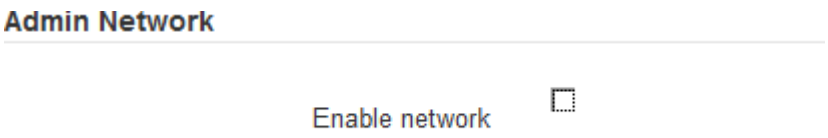
2. Selecione a velocidade da ligação para as portas de rede na lista pendente **Link speed** (velocidade da ligação).

   Os switches de rede que você está usando para a rede de Grade e a rede do cliente também devem suportar e ser configurados para essa velocidade. Você deve usar os adaptadores ou transcetores apropriados para a velocidade de link configurada. Utilize a velocidade de ligação automática quando possível, porque esta opção negocia tanto a velocidade de ligação como o modo de correção de erro de avanço (FEC) com o parceiro de ligação.

3. Ative ou desative as redes StorageGRID que pretende utilizar.

   A rede de Grade é necessária. Não é possível desativar esta rede.

   a. Se o dispositivo não estiver conetado à rede Admin, desmarque a caixa de seleção **Ativar rede** para a rede Admin.

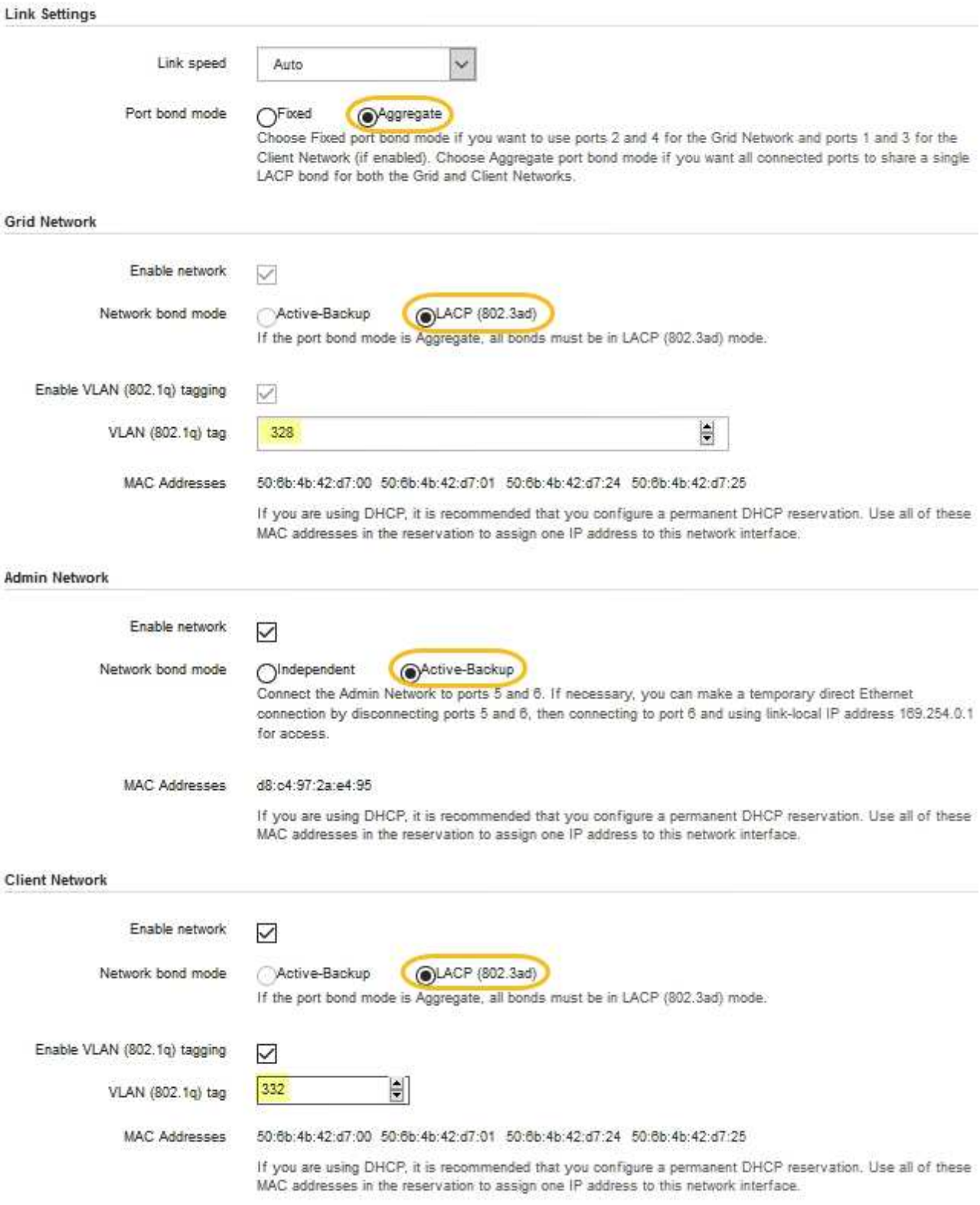
   b. Se o dispositivo estiver conetado à rede do cliente, marque a caixa de seleção **Ativar rede** para a rede do cliente.

      As configurações de rede do cliente para as portas NIC de dados são agora mostradas.

4. Consulte a tabela e configure o modo de ligação de porta e o modo de ligação de rede.

   Este exemplo mostra:

   - **Aggregate** e **LACP** selecionados para as redes Grid e Client. Você deve especificar uma tag VLAN exclusiva para cada rede. Pode selecionar valores entre 0 e 4095.
   - **Ative-Backup** selecionado para a rede Admin.



5. Quando estiver satisfeito com suas seleções, clique em **Salvar**.

Poderá perder a ligação se tiver efetuado alterações à rede ou à ligação através da qual está ligado. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do Instalador de appliance StorageGRID usando um dos outros endereços IP atribuídos ao appliance
`https://services_appliance_IP:8443`

Informações relacionadas

"Obtenção de equipamentos e ferramentas adicionais (SG100 e SG1000)"

Configurando endereços IP do StorageGRID

Você usa o Instalador do StorageGRID Appliance para configurar os endereços IP e as informações de roteamento usadas para o utilitário de serviços nas redes de Grade, Administrador e Cliente do StorageGRID.

Sobre esta tarefa

Você deve atribuir um IP estático para o dispositivo em cada rede conetada ou atribuir uma concessão permanente para o endereço no servidor DHCP.

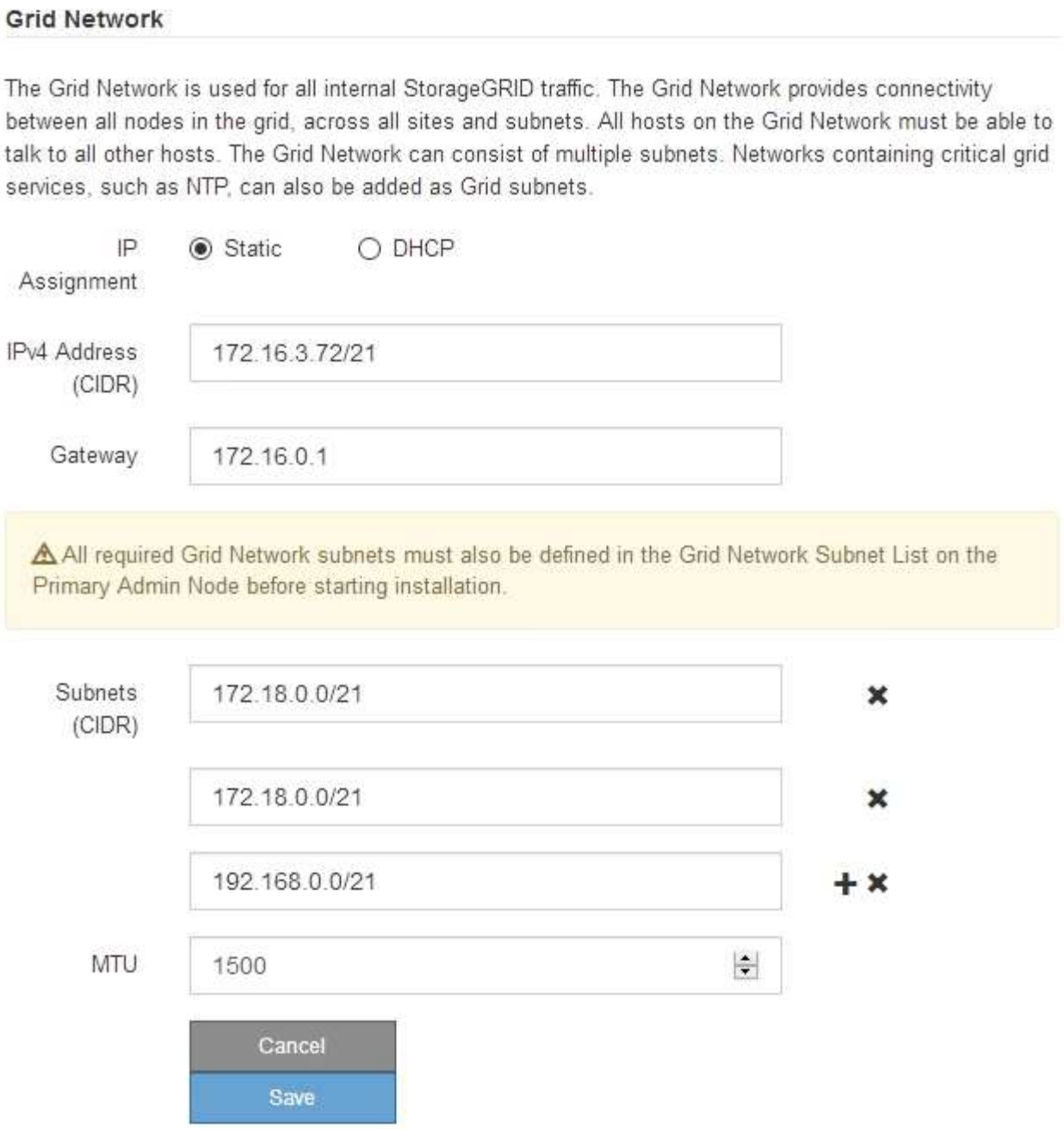
Se você quiser alterar a configuração do link, consulte as instruções para alterar a configuração do link do utilitário de serviços.

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração IP**.

   É apresentada a página Configuração IP.

2. Para configurar a rede de Grade, selecione **Static** ou **DHCP** na seção **Grid Network** da página.



3. Se você selecionou **Static**, siga estas etapas para configurar a rede de Grade:
   a. Insira o endereço IPv4 estático, usando a notação CIDR.
   b. Entre no gateway.

      Se a rede não tiver um gateway, insira novamente o mesmo endereço IPv4 estático.

   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

      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.

> 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.

d. Clique em **Salvar**.

   Quando você altera o endereço IP, o gateway e a lista de sub-redes também podem mudar.

   Se você perder a conexão com o Instalador do StorageGRID Appliance, insira novamente o URL usando o novo endereço IP estático que você acabou de atribuir. Por exemplo `https://services_appliance_IP:8443`

e. Confirme se a lista de sub-redes da rede de Grade está correta.

   Se você tiver 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. Essas sub-redes de rede de grade também devem ser definidas na lista de sub-redes de rede de grade no nó de administração principal quando você iniciar a instalação do StorageGRID.

   > A rota padrão não está listada. Se a rede do cliente não estiver ativada, a rota padrão usará o gateway de rede de grade.

   - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
   - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

f. Clique em **Salvar**.

4. Se você selecionou **DHCP**, siga estas etapas para configurar a rede de Grade:

   a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

      Os campos **IPv4 Address**, **Gateway** e **sub-redes** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

      O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

   b. Confirme se a lista de sub-redes da rede de Grade está correta.

      Se você tiver 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. Essas sub-redes de rede de grade também devem ser definidas na lista de sub-redes de rede de grade no nó de administração principal quando você iniciar a instalação do StorageGRID.

      > A rota padrão não está listada. Se a rede do cliente não estiver ativada, a rota padrão usará o gateway de rede de grade.

      - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
      - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros

jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

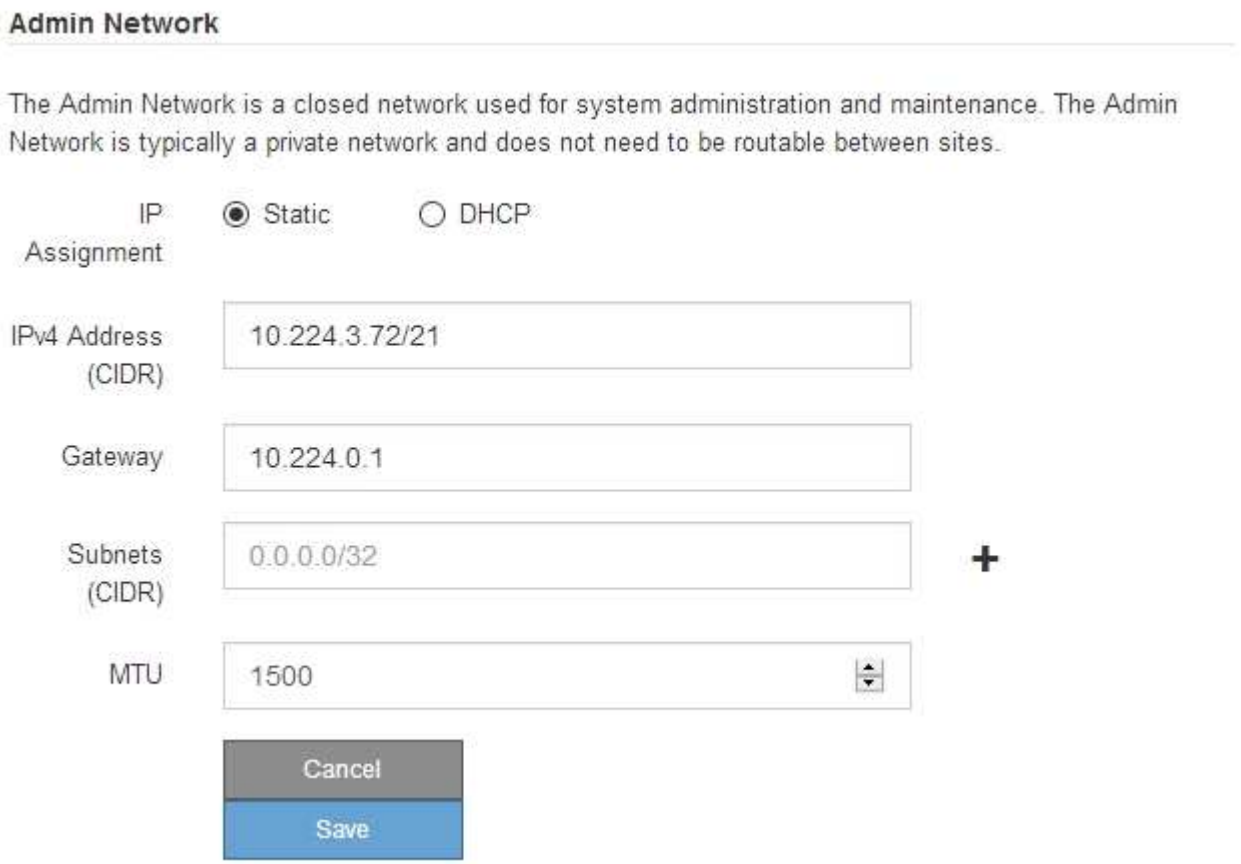
> O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

> 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.

a. Clique em **Salvar**.

5. Para configurar a rede Admin, selecione **Static** (estático) ou **DHCP** (DHCP) na secção Admin Network (rede Admin) da página.

> Para configurar a rede de administração, você deve ativar a rede de administração na página Configuração de ligação.



6. Se você selecionou **Static**, siga estas etapas para configurar a rede Admin:

a. Introduza o endereço IPv4 estático, utilizando a notação CIDR, para a porta de gestão 1 no dispositivo.

A porta de gerenciamento 1 fica à esquerda das duas portas RJ45 de 1 GbE na extremidade direita do dispositivo.

b. Entre no gateway.

   Se a rede não tiver um gateway, insira novamente o mesmo endereço IPv4 estático.

c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

   > 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.

d. Clique em **Salvar**.

   Quando você altera o endereço IP, o gateway e a lista de sub-redes também podem mudar.

   Se você perder a conexão com o Instalador do StorageGRID Appliance, insira novamente o URL usando o novo endereço IP estático que você acabou de atribuir. Por exemplo `https://services_appliance:8443`

e. Confirme se a lista de sub-redes Admin Network está correta.

   Você deve verificar se todas as sub-redes podem ser alcançadas usando o gateway fornecido.

   > A rota padrão não pode ser feita para usar o gateway de rede Admin.

   - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
   - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

f. Clique em **Salvar**.

7. Se você selecionou **DHCP**, siga estas etapas para configurar a rede Admin:

   a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

      Os campos **IPv4 Address**, **Gateway** e **sub-redes** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

      O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

   b. Confirme se a lista de sub-redes Admin Network está correta.

      Você deve verificar se todas as sub-redes podem ser alcançadas usando o gateway fornecido.

      > A rota padrão não pode ser feita para usar o gateway de rede Admin.

      - Para adicionar uma sub-rede, clique no ícone de inserção ➕à direita da última entrada.
      - Para remover uma sub-rede não utilizada, clique no ícone de eliminação ✖.

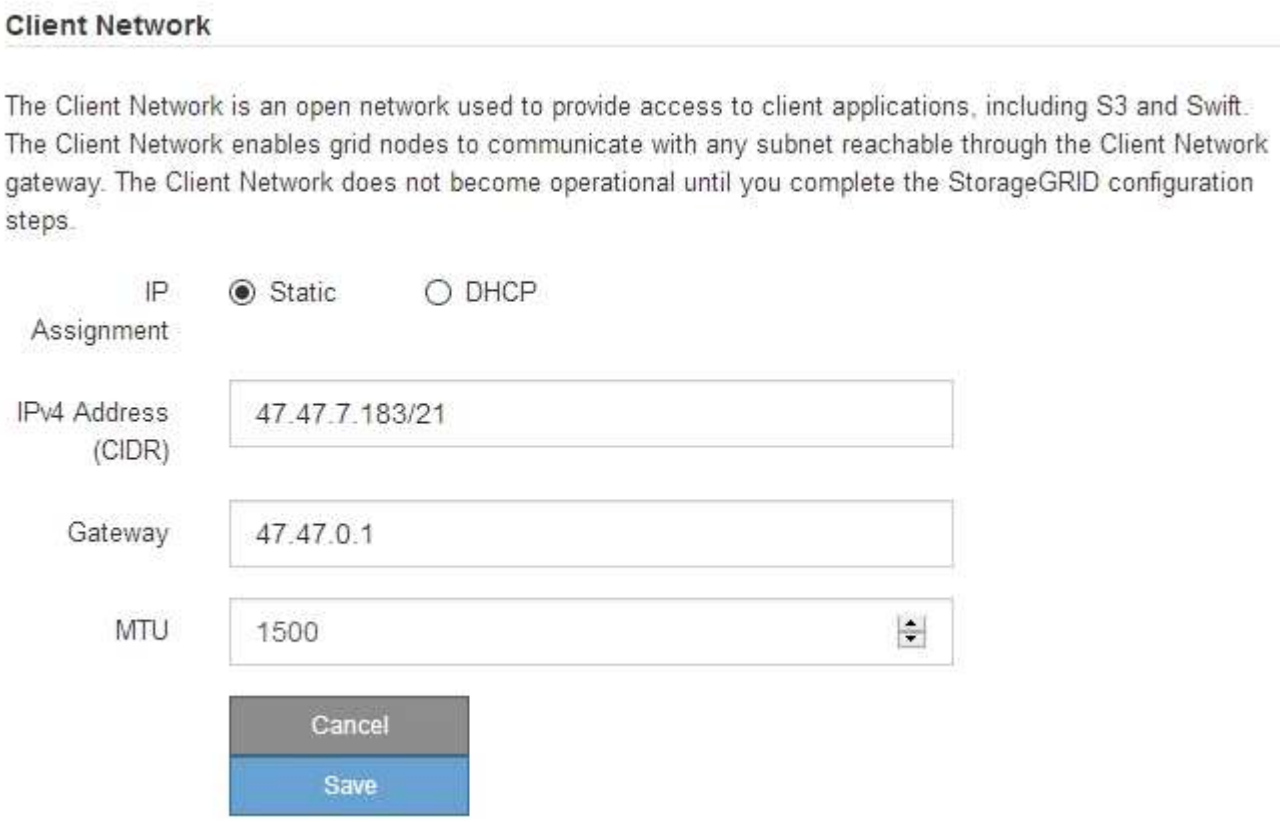
   c. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

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.

d. Clique em **Salvar**.

8. Para configurar a rede do cliente, selecione **estático** ou **DHCP** na seção **rede do cliente** da página.

Para configurar a rede do cliente, tem de ativar a rede do cliente na página Configuração da ligação.



9. Se você selecionou **Static**, siga estas etapas para configurar a rede do cliente:

a. Insira o endereço IPv4 estático, usando a notação CIDR.

b. Clique em **Salvar**.

c. Confirme se o endereço IP do gateway de rede do cliente está correto.

Se a rede do cliente estiver ativada, é apresentada a rota predefinida. A rota padrão usa o gateway de rede do cliente e não pode ser movida para outra interface enquanto a rede do cliente está ativada.

d. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

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.

e. Clique em **Salvar**.

10. Se você selecionou **DHCP**, siga estas etapas para configurar a rede do cliente:

    a. Depois de selecionar o botão de opção **DHCP**, clique em **Save** (Guardar).

       Os campos **IPv4 Address** e **Gateway** são preenchidos automaticamente. Se o servidor DHCP estiver configurado para atribuir um valor MTU, o campo **MTU** será preenchido com esse valor e o campo se tornará somente leitura.

    O navegador da Web é automaticamente redirecionado para o novo endereço IP do Instalador de dispositivos StorageGRID.

    a. Confirme se o gateway está correto.

       > Se a rede do cliente estiver ativada, é apresentada a rota predefinida. A rota padrão usa o gateway de rede do cliente e não pode ser movida para outra interface enquanto a rede do cliente está ativada.

    b. Se você quiser usar quadros jumbo, altere o campo MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão de 1500.

       > 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.

Informações relacionadas

"Alterar a configuração do link do dispositivo de serviços"

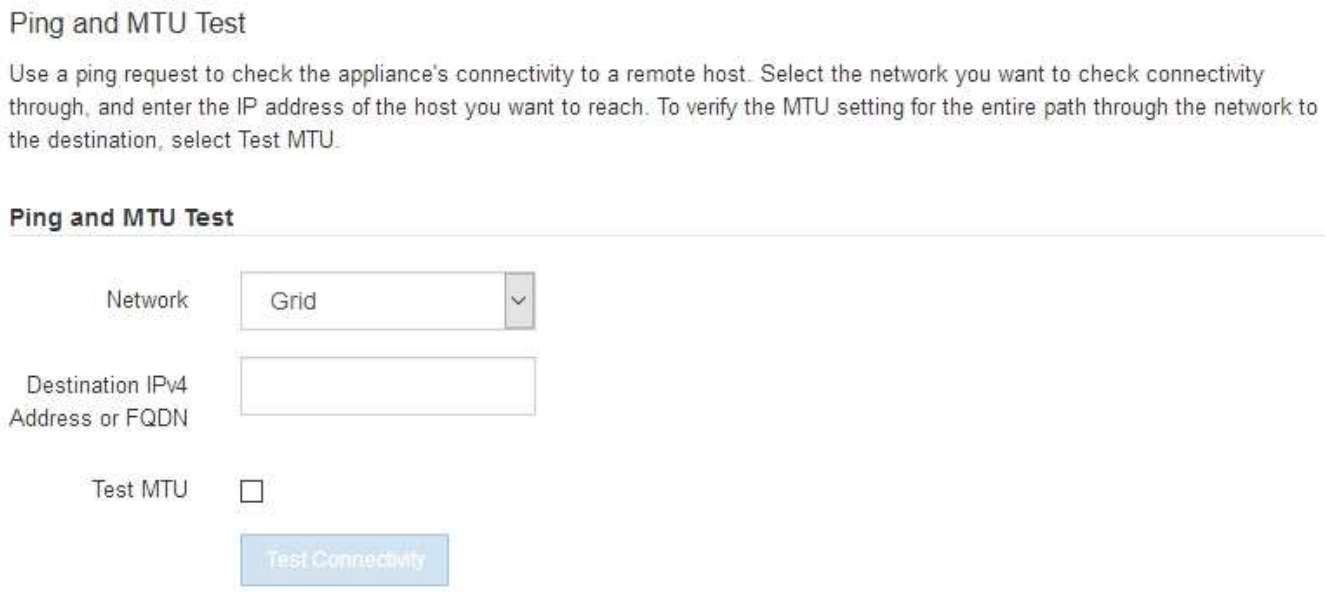
Verificando conexões de rede

Confirme que pode aceder às redes StorageGRID que está a utilizar a partir do dispositivo. Para validar o roteamento por meio de gateways de rede, você deve testar a conetividade entre o Instalador de dispositivos StorageGRID e endereços IP em diferentes sub-redes. Você também pode verificar a configuração MTU.

Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Configurar rede Teste de Ping e MTU**.

   A página Ping e MTU Test (Teste de Ping e MTU) é exibida.



2. Na caixa suspensa **rede**, selecione a rede que deseja testar: Grade, Admin ou Cliente.
3. Insira o endereço IPv4 ou o nome de domínio totalmente qualificado (FQDN) para um host nessa rede.

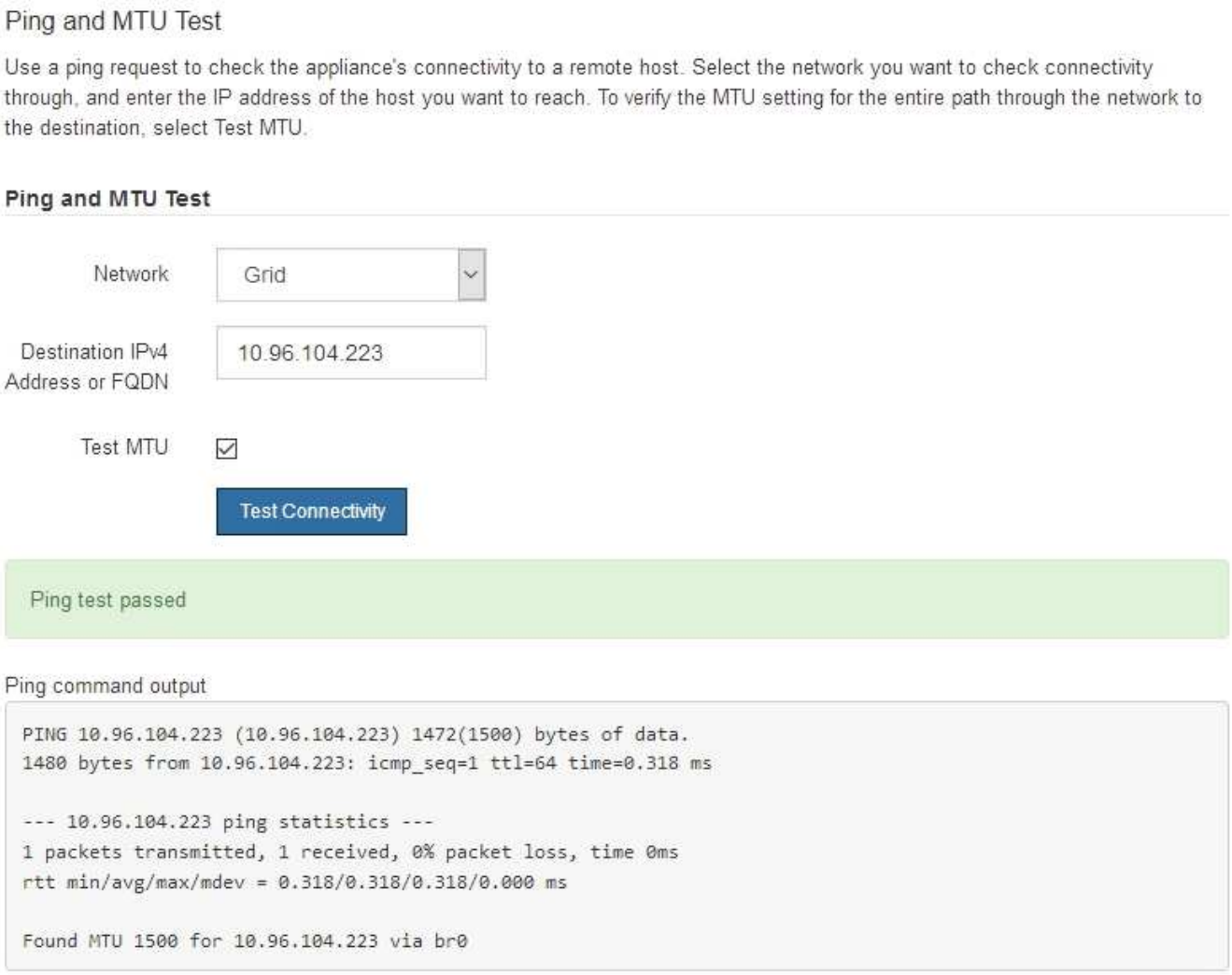
   Por exemplo, você pode querer fazer ping no gateway na rede ou no nó de administração principal.

4. Opcionalmente, marque a caixa de seleção **Test MTU** para verificar a configuração de MTU para todo o caminho através da rede até o destino.

   Por exemplo, você pode testar o caminho entre o nó do dispositivo e um nó em um local diferente.

5. Clique em **testar conetividade**.

   Se a conexão de rede for válida, a mensagem "Teste de ping aprovado" será exibida, com a saída do comando ping listada.



Informações relacionadas

"Configuração de links de rede (SG100 e SG1000)"

"Alterar a definição MTU"

Verificando conexões de rede no nível da porta

Para garantir que o acesso entre o Instalador de dispositivos StorageGRID e outros nós não esteja obstruído por firewalls, confirme se o Instalador de dispositivos StorageGRID pode se conetar a uma porta TCP específica ou conjunto de portas no endereço IP ou intervalo de endereços especificado.

Sobre esta tarefa

Usando a lista de portas fornecida no Instalador de dispositivos StorageGRID, você pode testar a conetividade entre o dispositivo e os outros nós da rede de Grade.

Além disso, você pode testar a conetividade nas redes Admin e Client e nas portas UDP, como as usadas para servidores NFS ou DNS externos. Para obter uma lista dessas portas, consulte a referência de porta nas diretrizes de rede do StorageGRID.

As portas de rede de grade listadas na tabela de conetividade de portas são válidas apenas para o StorageGRID versão 11,5.0. Para verificar quais portas estão corretas para cada tipo de nó, você deve sempre consultar as diretrizes de rede para sua versão do StorageGRID.

Passos

1. No Instalador de dispositivos StorageGRID, clique em **Configurar rede Teste de conetividade de porta (nmap)**.

   A página Teste de conetividade de porta é exibida.

   A tabela de conetividade de porta lista os tipos de nós que exigem conetividade TCP na rede de Grade. Para cada tipo de nó, a tabela lista as portas de rede de Grade que devem ser acessíveis ao seu dispositivo.

   The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

   Você pode testar a conetividade entre as portas do dispositivo listadas na tabela e os outros nós da rede de Grade.

2. Na lista suspensa **Network**, selecione a rede que deseja testar: **Grid**, **Admin** ou **Client**.
3. Especifique um intervalo de endereços IPv4 para os hosts nessa rede.

   Por exemplo, você pode querer pesquisar o gateway na rede ou no nó de administração principal.

   Especifique um intervalo usando um hífen, como mostrado no exemplo.

4. Insira um número de porta TCP, uma lista de portas separadas por vírgulas ou um intervalo de portas.

The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

Port Connectivity Test

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: TCP UDP

Test Connectivity

5. Clique em **testar conetividade**.

   - Se as conexões de rede no nível da porta selecionadas forem válidas, a mensagem ""Teste de conetividade de porta aprovado"" aparecerá em um banner verde. A saída do comando nmap está listada abaixo do banner.

     Port connectivity test passed

     Nmap command output. Note: Unreachable hosts will not appear in the output.

     ```
     # Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
     Nmap scan report for 10.224.6.160
     Host is up (0.00072s latency).

     PORT     STATE SERVICE
     22/tcp   open  ssh
     2022/tcp open  down

     Nmap scan report for 10.224.6.161
     Host is up (0.00060s latency).

     PORT     STATE SERVICE
     22/tcp   open  ssh
     2022/tcp open  down

     # Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
     ```

   - Se uma conexão de rede no nível da porta for feita ao host remoto, mas o host não estiver ouvindo em uma ou mais das portas selecionadas, a mensagem ""Falha no teste de conetividade da porta"" aparecerá em um banner amarelo. A saída do comando nmap está listada abaixo do banner.

     Qualquer porta remota que o host não esteja ouvindo tem um estado de "fechado". Por exemplo, você pode ver esse banner amarelo quando o nó ao qual você está tentando se conetar estiver em um estado pré-instalado e o serviço StorageGRID NMS ainda não estiver sendo executado nesse nó.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- Se uma conexão de rede no nível de porta não puder ser feita para uma ou mais portas selecionadas, a mensagem "Falha no teste de conetividade de porta" aparecerá em um banner vermelho. A saída do comando nmap está listada abaixo do banner.

  O banner vermelho indica que uma tentativa de conexão TCP para uma porta no host remoto foi feita, mas nada foi retornado ao remetente. Quando nenhuma resposta é retornada, a porta tem um estado de "filtrada" e é provavelmente bloqueada por um firewall.

  > Os portos com "fechado" também são listados.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

Informações relacionadas

"Diretrizes de rede"

Configurando a interface BMC

A interface do usuário do controlador de gerenciamento de placa base (BMC) no utilitário de serviços fornece informações de status sobre o hardware e permite que você configure as configurações SNMP e outras opções para o utilitário de serviços.

Passos

- "Alterar a senha raiz da interface BMC"
- "Definir o endereço IP da porta de gerenciamento do BMC"
- "Acessando a interface BMC"
- "Configurar definições SNMP para o utilitário de serviços"
- "Configurar notificações por e-mail para alertas"

Alterar a senha raiz da interface BMC

Para segurança, você deve alterar a senha do usuário raiz do BMC.

O que você vai precisar

O cliente de gerenciamento está usando um navegador da Web compatível.

Sobre esta tarefa

Quando você instala o dispositivo pela primeira vez, o BMC usa uma senha padrão para o usuário raiz (`root/calvin`). Você deve alterar a senha do usuário raiz para proteger seu sistema.

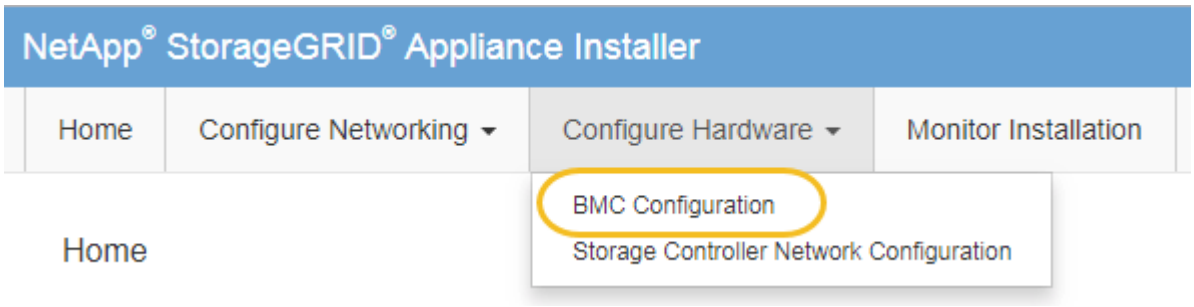
Passos

1. No cliente, insira o URL para o instalador do StorageGRID Appliance
   `https://services_appliance_IP:8443`

   Para `services_appliance_IP`, use o endereço IP do dispositivo em qualquer rede StorageGRID.

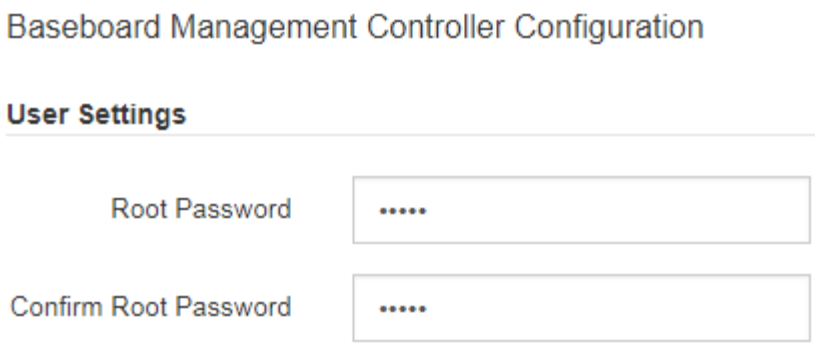
   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configurar hardware Configuração do BMC**.



   É apresentada a página Baseboard Management Controller Configuration (Configuração do controlador de gestão de base).

3. Insira uma nova senha para a conta root nos dois campos fornecidos.



4. Clique em **Salvar**.

Definir o endereço IP da porta de gerenciamento do BMC

Antes de poder aceder à interface BMC, tem de configurar o endereço IP para a porta de gestão BMC no dispositivo de serviços.

O que você vai precisar

- O cliente de gerenciamento está usando um navegador da Web compatível.
- Você está usando qualquer cliente de gerenciamento que possa se conetar a uma rede StorageGRID.
- A porta de gerenciamento do BMC está conetada à rede de gerenciamento que você planeja usar.

SG100 porta de gerenciamento BMC

SG1000 porta de gerenciamento BMC

Sobre esta tarefa

Para fins de suporte, a porta de gerenciamento do BMC permite acesso a hardware de baixo nível. Só deve ligar esta porta a uma rede de gestão interna segura, fidedigna. Se nenhuma rede estiver disponível, deixe a porta BMC desconetada ou bloqueada, a menos que uma conexão BMC seja solicitada pelo suporte técnico.

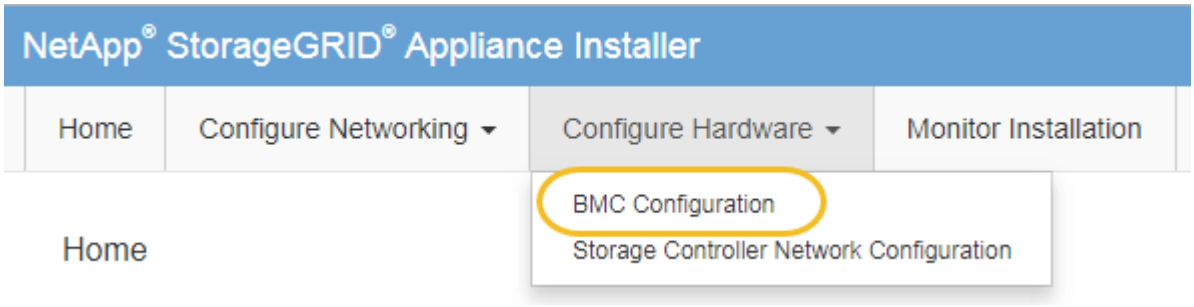
Passos

1. No cliente, insira o URL para o instalador do StorageGRID Appliance
   `https://services_appliance_IP:8443`

   Para *`services_appliance_IP`*, use o endereço IP do dispositivo em qualquer rede StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configurar hardware Configuração do BMC**.

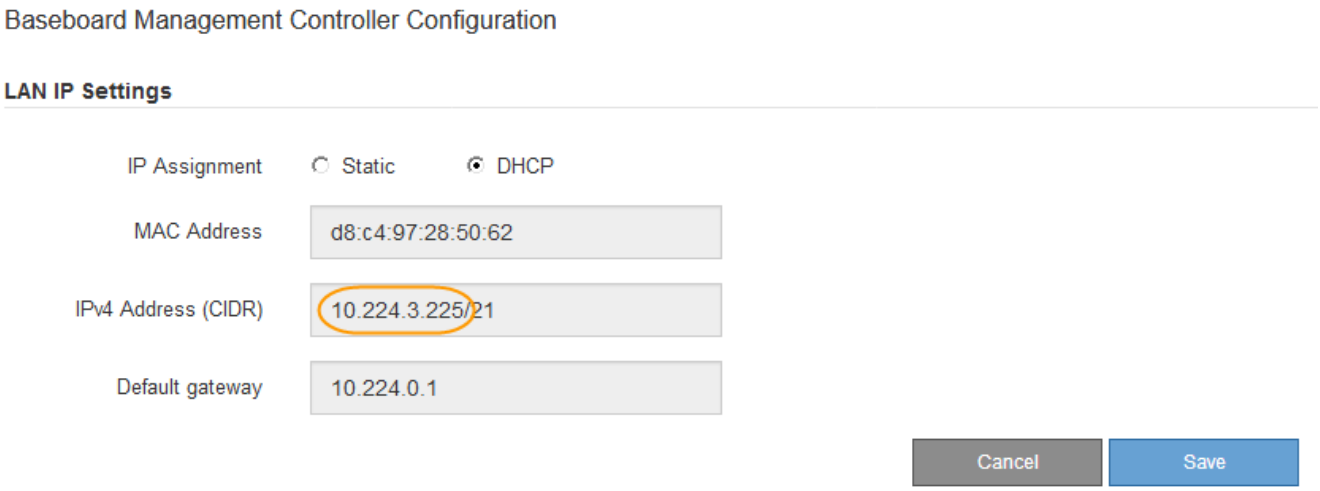


É apresentada a página Baseboard Management Controller Configuration (Configuração do controlador de gestão de base).

3. Anote o endereço IPv4 que é exibido automaticamente.

   DHCP é o método padrão para atribuir um endereço IP a esta porta.

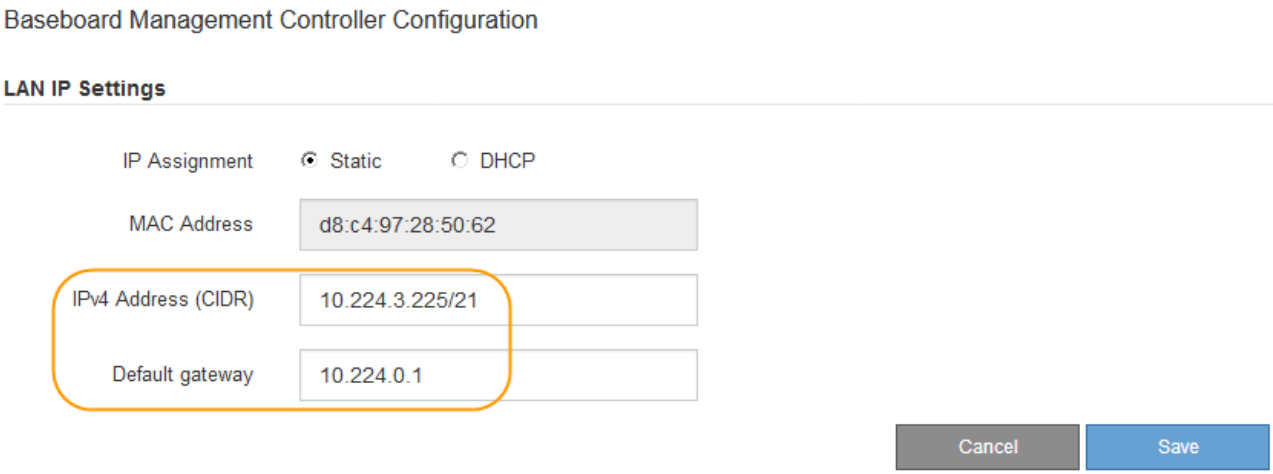
   Pode demorar alguns minutos para que os valores DHCP apareçam.



4. Opcionalmente, defina um endereço IP estático para a porta de gerenciamento BMC.

   Você deve atribuir um IP estático para a porta de gerenciamento do BMC ou atribuir uma concessão permanente para o endereço no servidor DHCP.

   a. Selecione **estático**.
   b. Introduza o endereço IPv4, utilizando a notação CIDR.
   c. Introduza o gateway predefinido.



d. Clique em **Salvar**.

Pode levar alguns minutos para que suas alterações sejam aplicadas.

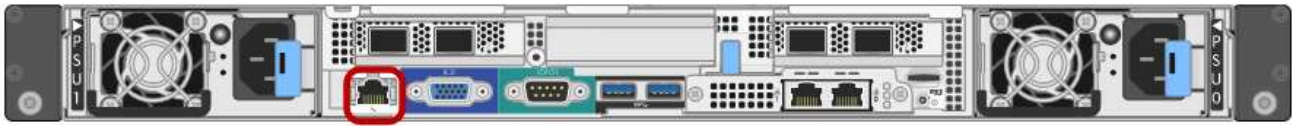
Acessando a interface BMC

Você pode acessar a interface BMC no utilitário de serviços usando o DHCP ou o endereço IP estático para a porta de gerenciamento BMC.

O que você vai precisar

- O cliente de gerenciamento está usando um navegador da Web compatível.
- A porta de gerenciamento do BMC no dispositivo de serviços está conetada à rede de gerenciamento que você planeja usar.

SG100 porta de gerenciamento BMC



SG1000 porta de gerenciamento BMC

Passos

1. Digite o URL para a interface do BMC
   `https://BMC_Port_IP`

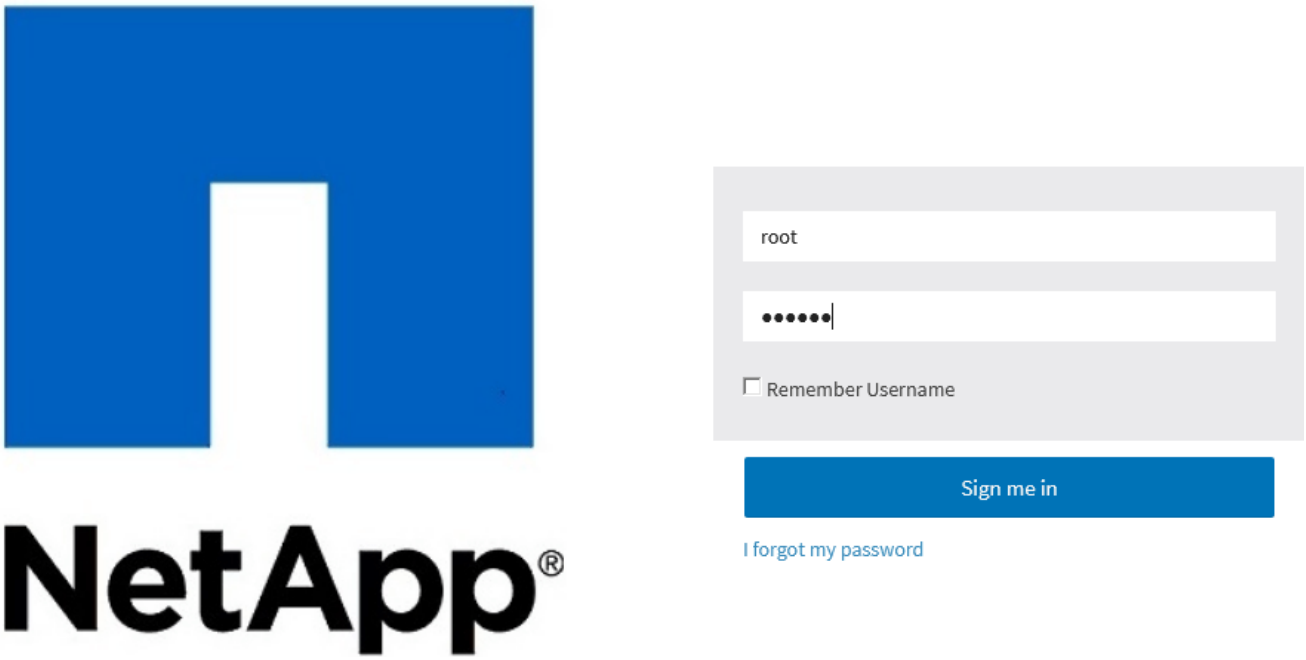
   Para *`BMC_Port_IP`*, utilize o DHCP ou o endereço IP estático para a porta de gestão BMC.

   É apresentada a página de início de sessão do BMC.

2. Digite o nome de usuário e a senha raiz, usando a senha definida quando você alterou a senha padrão do root

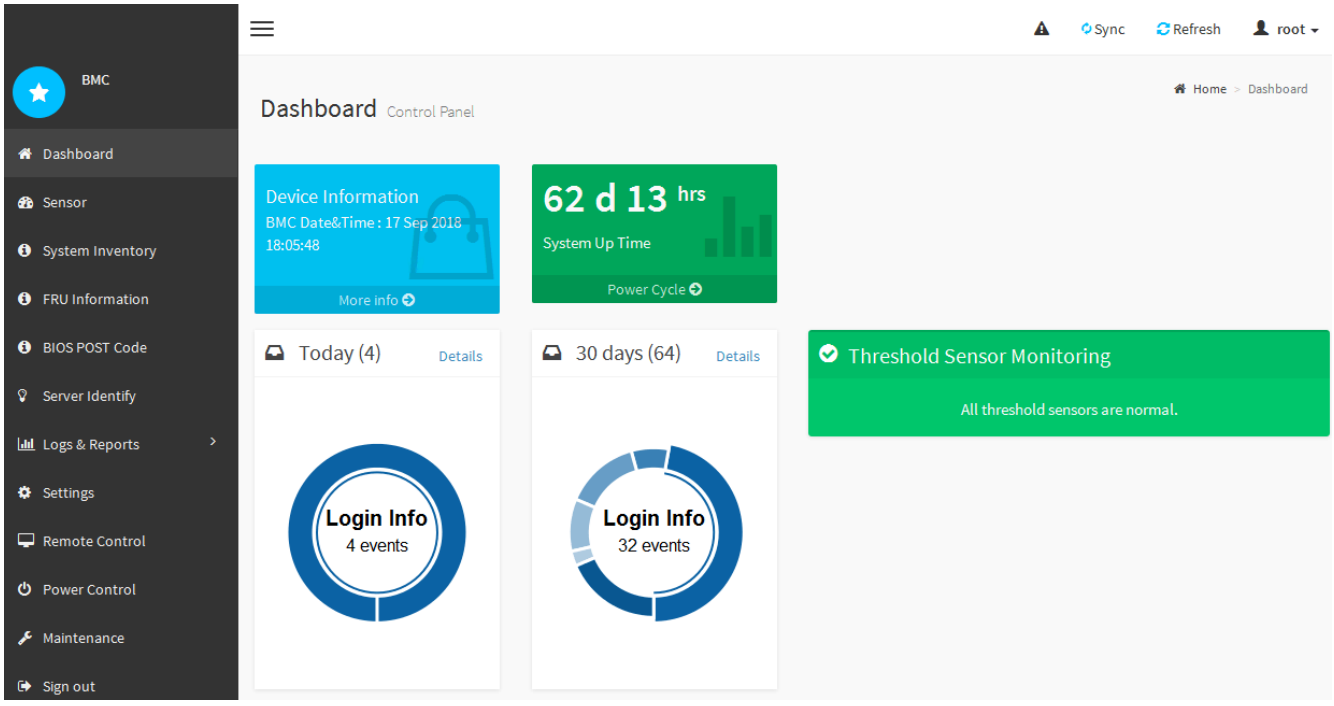
`root`

password



3. Clique em **Sign me in**

   O painel BMC é exibido.



4. Opcionalmente, crie usuários adicionais selecionando **Configurações Gerenciamento de usuários** e clicando em qualquer usuário "habilitado".

Quando os usuários entram pela primeira vez, eles podem ser solicitados a alterar sua senha para aumentar a segurança.

Informações relacionadas

"Alterar a senha raiz da interface BMC"

Configurar definições SNMP para o utilitário de serviços

Se estiver familiarizado com a configuração do SNMP para hardware, pode utilizar a interface BMC para configurar as definições SNMP para o utilitário de serviços. Você pode fornecer strings de comunidade seguras, ativar Trap SNMP e especificar até cinco destinos SNMP.

O que você vai precisar

- Você sabe como acessar o painel do BMC.
- Tem experiência em configurar definições SNMP para equipamento SNMPv1-v2c.

Passos

1. No painel BMC, selecione **Configurações Configurações Configurações SNMP**.
2. Na página Configurações SNMP, selecione **Ativar SNMP V1/V2** e, em seguida, forneça uma String comunitária somente leitura e uma String Comunidade de leitura-escrita.

   A String da Comunidade somente leitura é como uma ID de usuário ou senha. Você deve alterar esse valor para evitar que intrusos obtenham informações sobre a configuração da rede. A cadeia de Comunidade de leitura-escrita protege o dispositivo contra alterações não autorizadas.

3. Opcionalmente, selecione **Ativar Trap** e insira as informações necessárias.

   Introduza o IP de destino para cada trap SNMP utilizando um endereço IP. Nomes de domínio totalmente qualificados não são suportados.

   Ative traps se quiser que o utilitário de serviços envie notificações imediatas para um console SNMP quando ele estiver em um estado incomum. Os traps podem indicar condições de ligação para cima/para baixo, temperaturas que excedem determinados limites ou tráfego elevado.

4. Opcionalmente, clique em **Send Test Trap** para testar suas configurações.
5. Se as configurações estiverem corretas, clique em **Salvar**.

Configurar notificações por e-mail para alertas

Se você quiser que as notificações por e-mail sejam enviadas quando os alertas ocorrerem, use a interface do BMC para configurar as configurações SMTP, usuários, destinos de LAN, políticas de alerta e filtros de eventos.

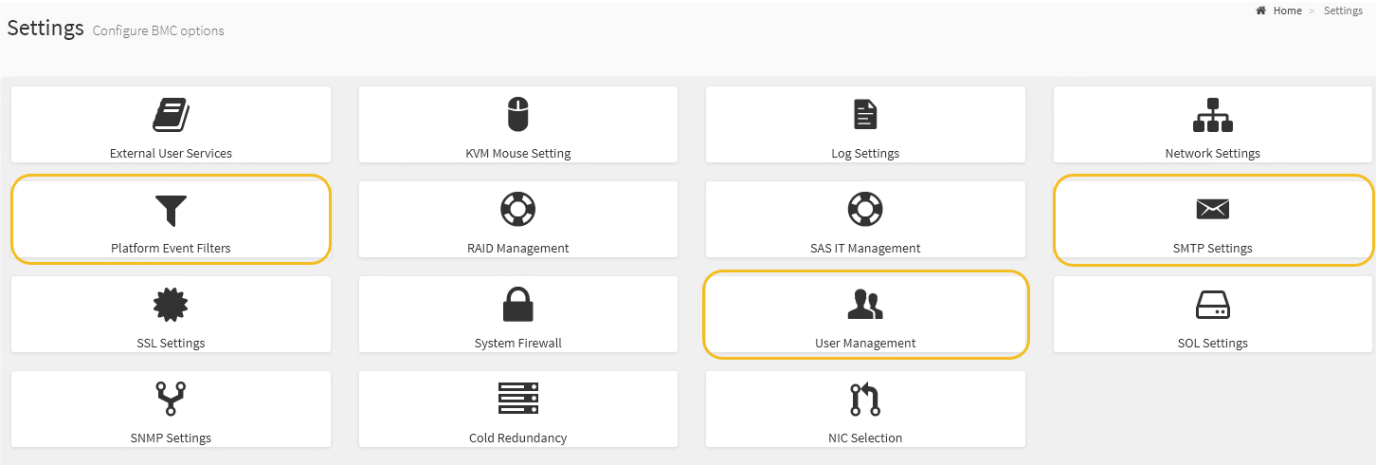
O que você vai precisar

Você sabe como acessar o painel do BMC.

Sobre esta tarefa

Na interface do BMC, você usa as opções **Configurações SMTP**, **Gerenciamento de usuários** e **filtros de**

evento da plataforma na página Configurações para configurar notificações por e-mail.



Passos

1. Configure as definições SMTP.
   a. Selecione **Configurações Configurações SMTP**.
   b. Para a ID de e-mail do remetente, introduza um endereço de e-mail válido.

      Este endereço de e-mail é fornecido como o endereço de quando o BMC envia e-mail.

2. Configure os usuários para receber alertas.
   a. No painel do BMC, selecione **Configurações Gerenciamento de usuários**.
   b. Adicione pelo menos um usuário para receber notificações de alerta.

      O endereço de e-mail que você configura para um usuário é o endereço para o qual o BMC envia notificações de alerta. Por exemplo, você pode adicionar um usuário genérico, como "usuário de notificação", e usar o endereço de e-mail de uma lista de distribuição de e-mail da equipe de suporte técnico.

3. Configure o destino da LAN para alertas.
   a. Selecione **Configurações filtros de evento de plataforma Destinos de LAN**.
   b. Configure pelo menos um destino de LAN.
      - Selecione **Email** como tipo de destino.
      - Para Nome de usuário do BMC, selecione um nome de usuário que você adicionou anteriormente.
      - Se você adicionou vários usuários e quer que todos eles recebam e-mails de notificação, você deve adicionar um destino de LAN para cada usuário.
   c. Envie um alerta de teste.
4. Configure políticas de alerta para que você possa definir quando e onde o BMC envia alertas.
   a. Selecione **Configurações filtros de evento da plataforma políticas de alerta**.
   b. Configure pelo menos uma política de alerta para cada destino de LAN.
      - Para número do Grupo de políticas, selecione **1**.
      - Para Ação de Política, selecione **sempre enviar alerta para este destino**.
      - Para Canal LAN, selecione **1**.

- No Seletor de destinos, selecione o destino da LAN para a política.

5. Configure filtros de eventos para direcionar alertas para diferentes tipos de eventos para os usuários apropriados.
   a. Selecione **Configurações filtros de evento da plataforma filtros de evento**.
   b. Para o número do grupo de políticas de alerta, digite **1**.
   c. Crie filtros para cada evento sobre o qual você deseja que o Grupo de políticas de Alerta seja notificado.
      - Você pode criar filtros de eventos para ações de energia, eventos de sensor específicos ou todos os eventos.
      - Se você não tiver certeza sobre quais eventos monitorar, selecione **todos os sensores** para tipo de sensor e **todos os eventos** para Opções de evento. Se receber notificações indesejadas, pode alterar as suas seleções mais tarde.

Opcional: Habilitando a criptografia de nó

Se você ativar a criptografia de nó, os discos do seu dispositivo podem ser protegidos pela criptografia de servidor de gerenciamento de chaves (KMS) seguro contra perda física ou remoção do site. Você deve selecionar e ativar a criptografia de nó durante a instalação do dispositivo e não pode desmarcar a criptografia de nó depois que o processo de criptografia KMS for iniciado.

O que você vai precisar

Consulte as informações sobre o KMS nas instruções de administração do StorageGRID.

Sobre esta tarefa

Um dispositivo com criptografia de nó ativada se coneta ao servidor de gerenciamento de chaves externas (KMS) configurado para o site StorageGRID. Cada cluster KMS (ou KMS) gerencia as chaves de criptografia para todos os nós de dispositivo no local. Essas chaves criptografam e descriptografam os dados em cada disco em um dispositivo que tem criptografia de nó ativada.

Um KMS pode ser configurado no Gerenciador de Grade antes ou depois que o dispositivo é instalado no StorageGRID. Consulte as informações sobre a configuração do KMS e do appliance nas instruções de administração do StorageGRID para obter detalhes adicionais.

- Se um KMS for configurado antes de instalar o dispositivo, a criptografia controlada pelo KMS será iniciada quando você ativar a criptografia de nó no dispositivo e adicioná-la a um site do StorageGRID onde o KMS está configurado.
- Se um KMS não for configurado antes de instalar o dispositivo, a criptografia controlada por KMS é executada em cada dispositivo que tem criptografia de nó ativada assim que um KMS é configurado e disponível para o site que contém o nó do dispositivo.

> Todos os dados existentes antes de um dispositivo que tenha criptografia de nó ativada se conetarem ao KMS configurado são criptografados com uma chave temporária que não é segura. O aparelho não está protegido contra remoção ou roubo até que a chave esteja definida para um valor fornecido pelo KMS.

Sem a chave KMS necessária para descriptografar o disco, os dados no dispositivo não podem ser recuperados e são efetivamente perdidos. Este é o caso sempre que a chave de descriptografia não pode ser recuperada do KMS. A chave fica inacessível se um cliente limpar a configuração do KMS, uma chave KMS

expira, a conexão com o KMS é perdida ou o dispositivo é removido do sistema StorageGRID onde suas chaves KMS são instaladas.

Passos

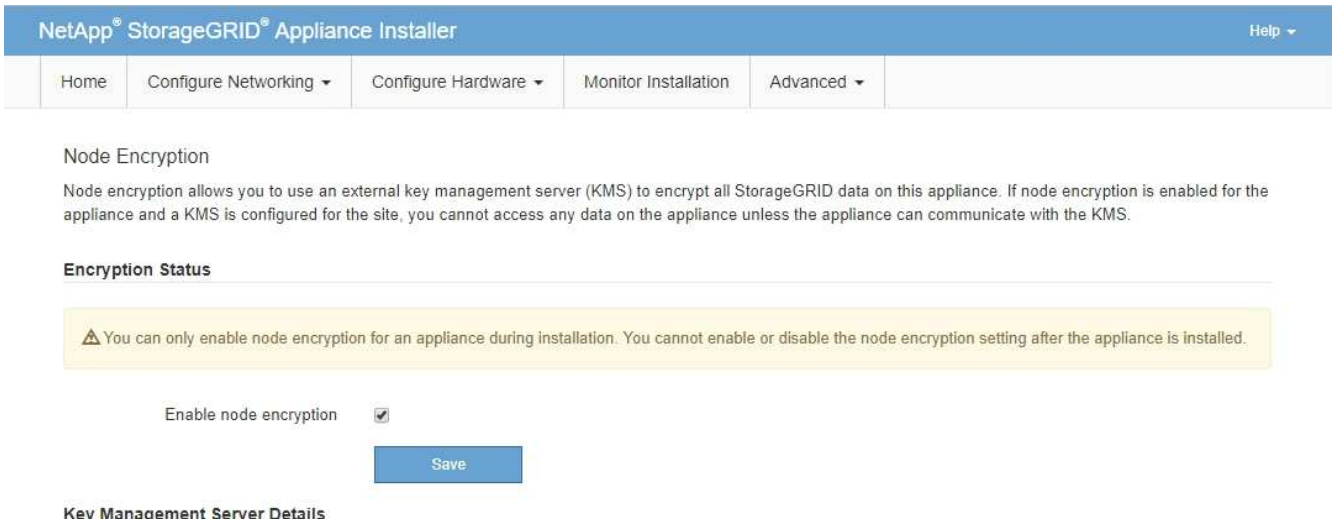
1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E `https://Controller_IP:8443`

   Controller_IP É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

   A página inicial do instalador do dispositivo StorageGRID é exibida.

   > Depois que o dispositivo tiver sido criptografado com uma chave KMS, os discos do appliance não podem ser descriptografados sem usar a mesma chave KMS.

2. Selecione **Configure hardware Node Encryption**.



3. Selecione **Ativar criptografia de nó**.

   Você pode desmarcar **Ativar criptografia de nó** sem risco de perda de dados até selecionar **Salvar** e o nó do dispositivo acessar as chaves de criptografia KMS em seu sistema StorageGRID e iniciar a criptografia de disco. Não é possível desativar a criptografia de nó após a instalação do dispositivo.

   > Depois de adicionar um dispositivo que tenha a criptografia de nó ativada a um site do StorageGRID que tenha um KMS, você não poderá parar de usar a criptografia KMS para o nó.

4. Selecione **Guardar**.
5. Implante o dispositivo como um nó no sistema StorageGRID.

   A encriptação controlada POR KMS começa quando o dispositivo acede às chaves KMS configuradas para o seu site StorageGRID. O instalador exibe mensagens de progresso durante o processo de criptografia KMS, o que pode levar alguns minutos, dependendo do número de volumes de disco no dispositivo.

> Os dispositivos são configurados inicialmente com uma chave de criptografia aleatória não KMS atribuída a cada volume de disco. Os discos são criptografados usando essa chave de criptografia temporária, que não é segura, até que o dispositivo que tem criptografia de nó habilitada acesse as chaves KMS configuradas para o site do StorageGRID.

Depois de terminar

Você pode exibir o status da criptografia do nó, os detalhes do KMS e os certificados em uso quando o nó do dispositivo está no modo de manutenção.

Informações relacionadas

"Administrar o StorageGRID"

"Monitorização da encriptação do nó no modo de manutenção"

Implantando um nó de dispositivo de serviços

Você pode implantar um dispositivo de serviços como nó de administração principal, um nó de administração não primário ou um nó de gateway. Os dispositivos SG100 e SG1000 podem operar como nós de gateway e nós de administração (primários ou não primários) ao mesmo tempo.

Implantando um dispositivo de serviços como nó de administração principal

Ao implantar um dispositivo de serviços como nó de administração principal, você usa o Instalador de dispositivos StorageGRID incluído no dispositivo para instalar o software StorageGRID ou faz o upload da versão de software que deseja instalar. Você deve instalar e configurar o nó Admin principal antes de instalar qualquer outro tipo de nó de dispositivo. Um nó de administração principal pode se conetar à rede de grade e à rede de administração opcional e à rede de cliente, se um ou ambos estiverem configurados.

O que você vai precisar

- O dispositivo foi instalado em um rack ou gabinete, conetado às redes e ligado.
- Links de rede, endereços IP e remapeamento de portas (se necessário) foram configurados para o dispositivo usando o Instalador de dispositivos StorageGRID.

> Se você tiver remapeado quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Você pode criar endpoints usando portas remapeadas, mas esses endpoints serão remapeados para as portas e serviços CLB originais, não para o serviço Load Balancer. Siga as etapas nas instruções de recuperação e manutenção para remover os remapas de portas.

> O serviço CLB está obsoleto.

- Você tem um laptop de serviço com um navegador da Web suportado.
- Você conhece um dos endereços IP atribuídos ao dispositivo. Você pode usar o endereço IP de qualquer rede StorageGRID conetada.

Sobre esta tarefa

Para instalar o StorageGRID em um nó de administração principal do dispositivo:

- Você usa o Instalador de dispositivos StorageGRID para instalar o software StorageGRID. Se você quiser instalar uma versão diferente do software, primeiro carregue-o usando o Instalador de dispositivos StorageGRID.
- Você espera enquanto o software está instalado.
- Quando o software tiver sido instalado, o dispositivo é reinicializado automaticamente.

Passos

1. Abra um navegador e insira o endereço IP do dispositivo. E
   `https://services_appliance_IP:8443`

   A página inicial do instalador do dispositivo StorageGRID é exibida.

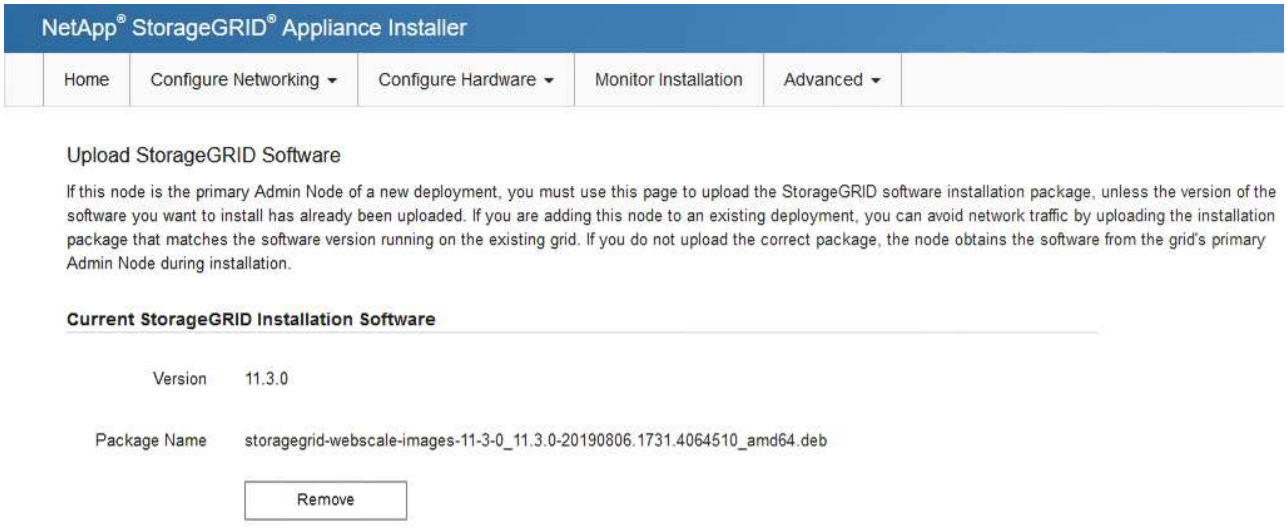
2. Na seção **this Node**, selecione **Primary Admin**.
3. No campo **Nome do nó**, insira o nome que deseja usar para este nó de appliance e clique em **Salvar**.

   O nome do nó é atribuído a este nó do dispositivo no sistema StorageGRID. Ele é mostrado na página Grid Nodes no Grid Manager.

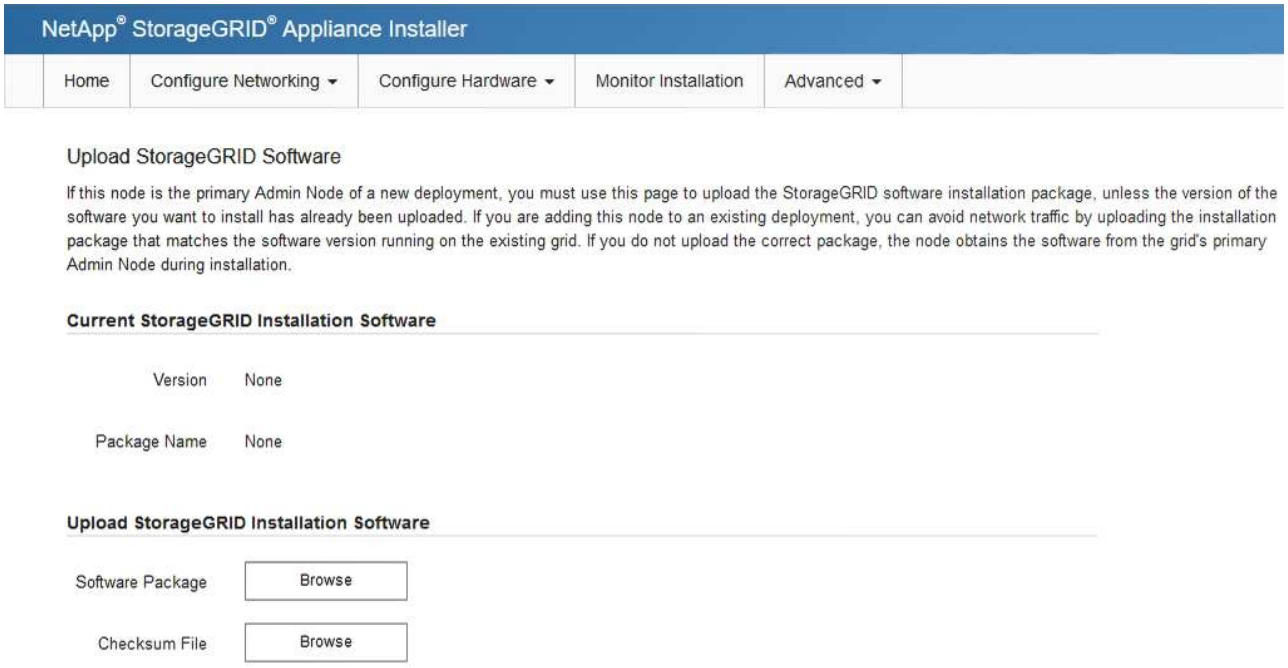
4. Opcionalmente, para instalar uma versão diferente do software StorageGRID, siga estas etapas:
   a. Transfira o arquivo de instalação a partir da página de transferências do NetApp para o StorageGRID.

      "NetApp Downloads: StorageGRID"

   b. Extraia o arquivo.
   c. No Instalador de dispositivos StorageGRID, selecione **Avançado carregar software StorageGRID**.
   d. Clique em **Remover** para remover o pacote de software atual.



   e. Clique em **Procurar** para obter o pacote de software que transferiu e extraiu e, em seguida, clique em **Procurar** para obter o ficheiro de checksum.



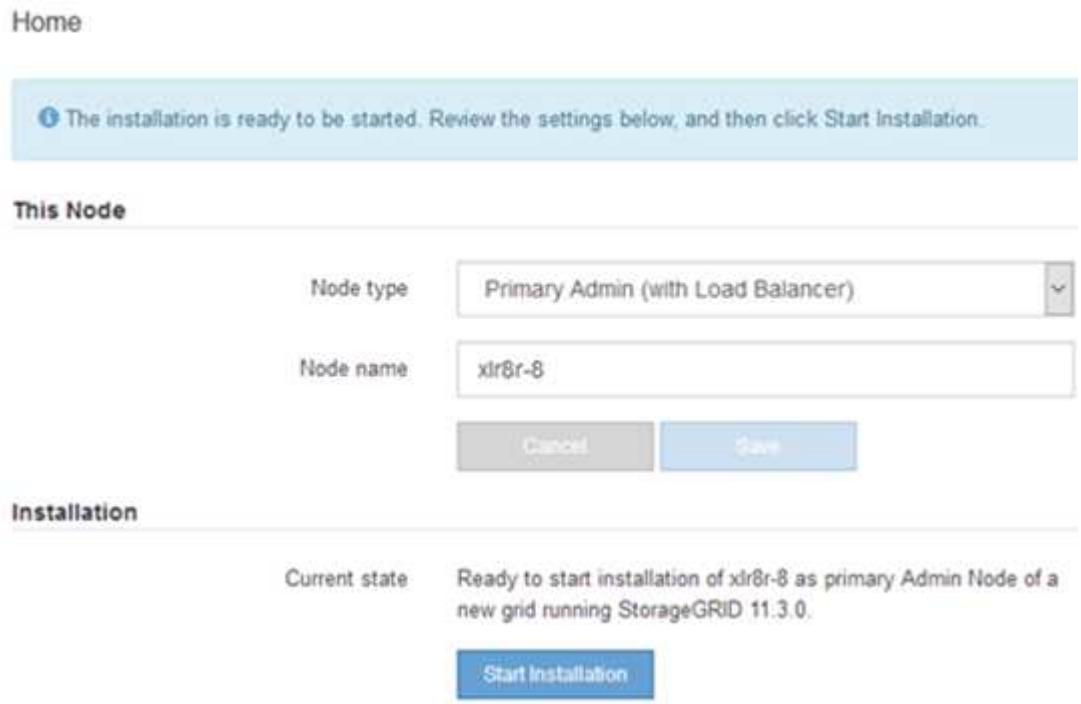
f. Selecione **Home** para voltar à página inicial.

5. Confirme se o estado atual é "'Pronto para iniciar a instalação do nome do nó de administração principal com a versão do software x.y'" e que o botão **Iniciar instalação** está ativado.

> Se você estiver implantando o dispositivo Admin Node como um destino de clonagem de nós, interrompa o processo de implantação aqui e continue o procedimento de clonagem de nós na recuperação e na manutenção.

"Manter recuperar"

6. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.



O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

> Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor** na barra de menus.

Informações relacionadas

"Implantando um dispositivo de serviços como um Gateway ou nó de administração não primário"

Implantando um dispositivo de serviços como um Gateway ou nó de administração não primário

Ao implantar um dispositivo de serviços como nó de gateway ou nó de administrador não primário, você usa o Instalador de dispositivos StorageGRID incluído no dispositivo.

O que você vai precisar

- O dispositivo foi instalado em um rack ou gabinete, conetado às redes e ligado.
- Links de rede, endereços IP e remapeamento de portas (se necessário) foram configurados para o dispositivo usando o Instalador de dispositivos StorageGRID.

> Se você tiver remapeado quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Você pode criar endpoints usando portas remapeadas, mas esses endpoints serão remapeados para as portas e serviços CLB originais, não para o serviço Load Balancer. Siga as etapas nas instruções de recuperação e manutenção para remover os remapas de portas.

> O serviço CLB está obsoleto.

- O nó de administração principal do sistema StorageGRID foi implantado.
- 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.
- Você tem um laptop de serviço com um navegador da Web suportado.
- Você sabe o endereço IP atribuído ao aparelho. Você pode usar o endereço IP de qualquer rede StorageGRID conetada.

Sobre esta tarefa

Para instalar o StorageGRID em um nó de dispositivo de serviços:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do nó do dispositivo.
- Você inicia a instalação e espera enquanto o software está instalado.

  Ao longo das tarefas de instalação do Appliance Gateway Node, 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. A instalação de um nó de administração não primário não requer sua aprovação.

> Não implante os dispositivos de serviço SG100 e SG1000 no mesmo local. Pode resultar em performance imprevisível.

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 dispositivo. Você também pode usar o Instalador de dispositivos para carregar um arquivo JSON que contém informações de configuração. "Automatizando a instalação e a configuração do dispositivo"Consulte .

Passos

1. Abra um navegador e insira o endereço IP do 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.

   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.

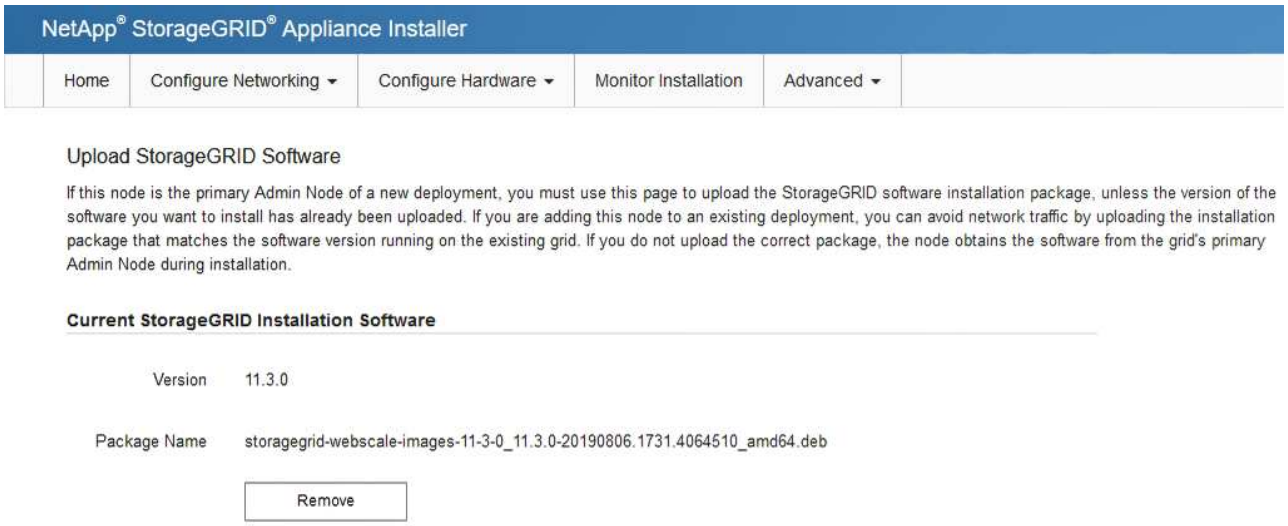
4. No campo **Nome do nó**, insira o nome que deseja usar para este nó de appliance e clique em **Salvar**.

   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.

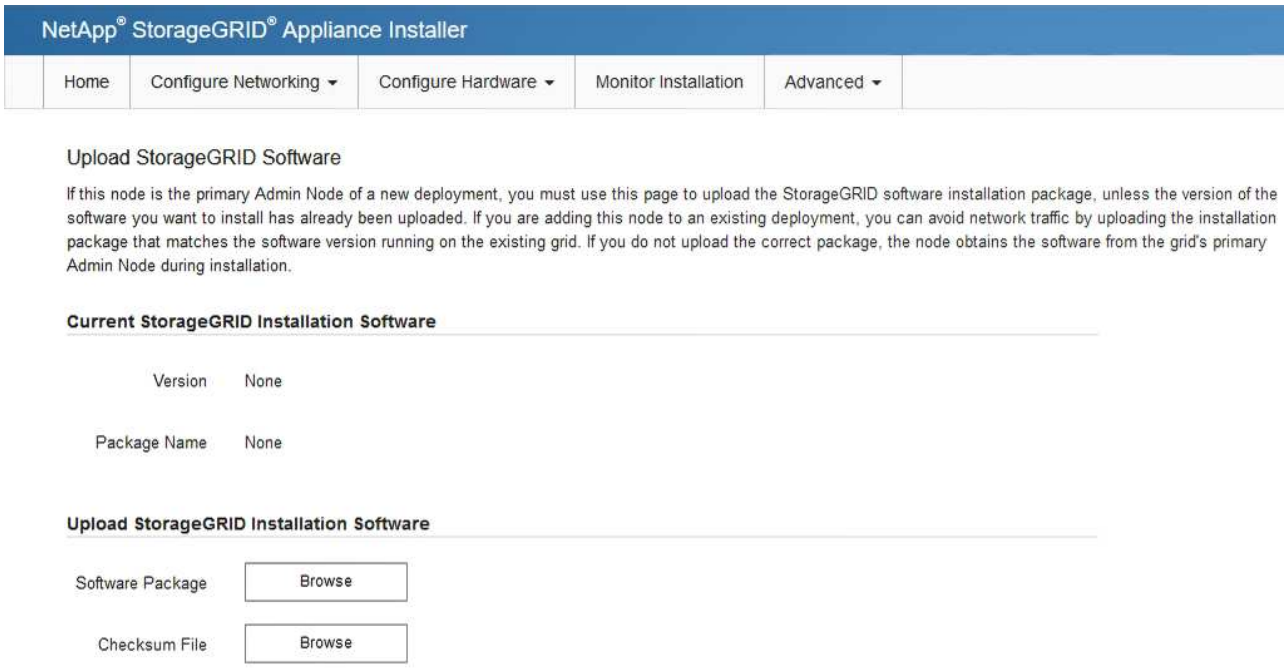
5. Opcionalmente, para instalar uma versão diferente do software StorageGRID, siga estas etapas:
   a. Transfira o arquivo de instalação a partir da página de transferências do NetApp para o StorageGRID.

      "NetApp Downloads: StorageGRID"

   b. Extraia o arquivo.
   c. No Instalador de dispositivos StorageGRID, selecione **Avançado carregar software StorageGRID**.
   d. Clique em **Remover** para remover o pacote de software atual.



   e. Clique em **Procurar** para obter o pacote de software que transferiu e extraiu e, em seguida, clique em **Procurar** para obter o ficheiro de checksum.

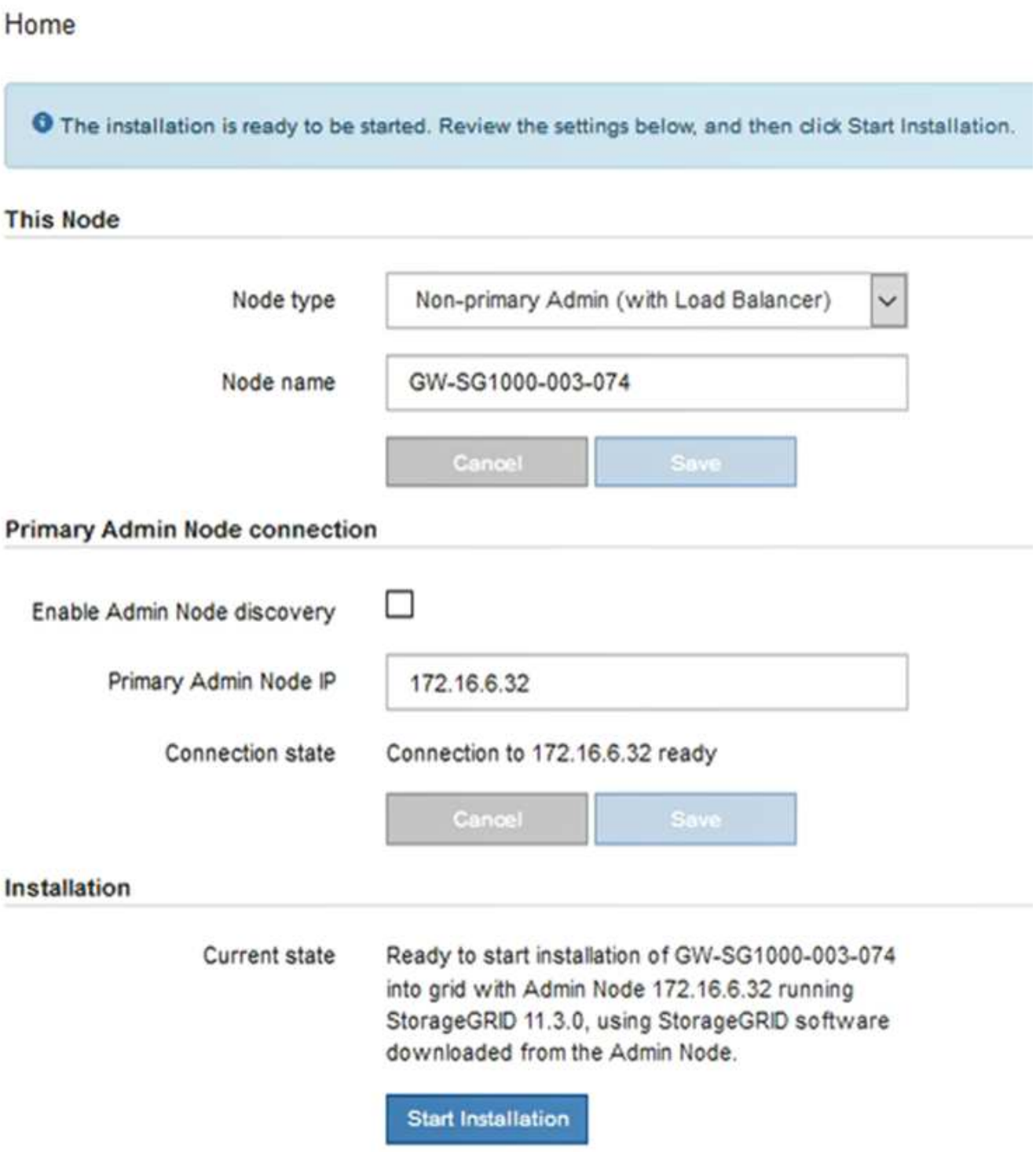


   f. Selecione **Home** para voltar à página inicial.

6. Na seção Instalação, confirme se o estado atual é "Pronto para iniciar a instalação *`node name`* na grade com nó Admin primário *`admin_ip`* " e se o botão **Iniciar instalação** está ativado.

Se o botão **Start Installation** (Iniciar instalação) não estiver ativado, poderá ser necessário alterar a configuração da rede ou as definições da porta. Para obter instruções, consulte as instruções de instalação e manutenção do seu aparelho.

7. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.



O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor** na barra de menus.

8. Se a grade incluir vários nós de dispositivo, repita as etapas anteriores para cada dispositivo.

Informações relacionadas

"Implantando um dispositivo de serviços como nó de administração principal"

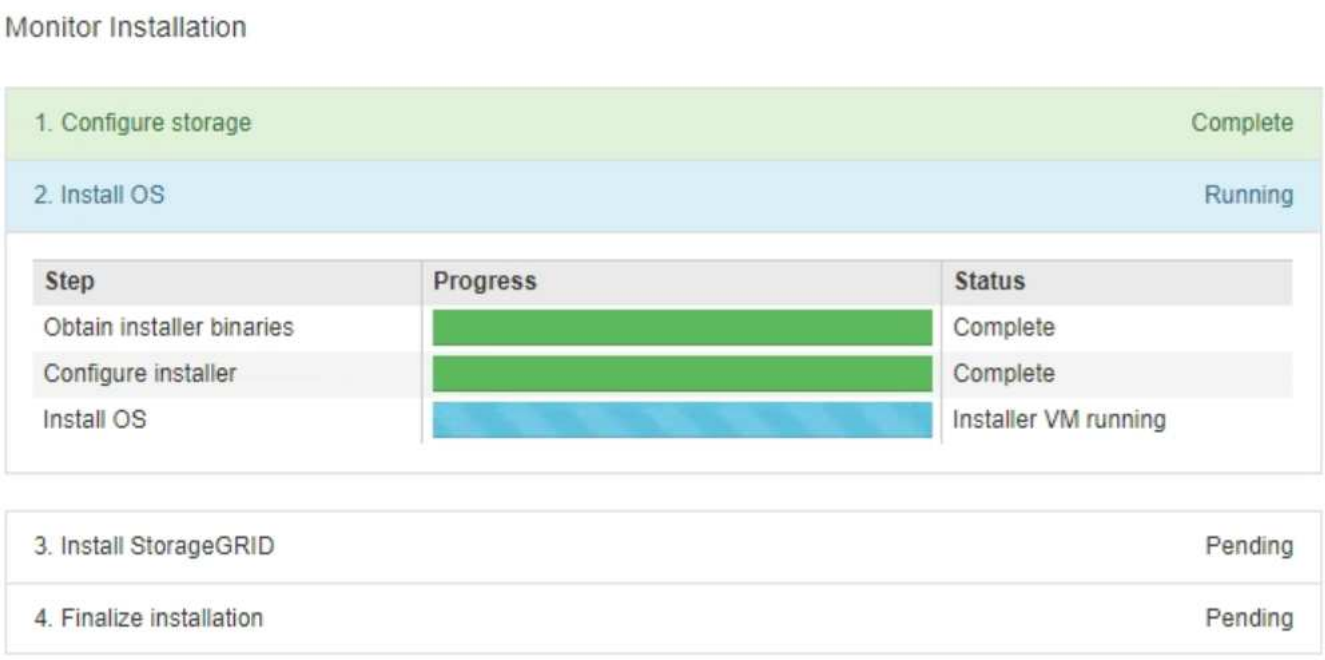
Monitoramento da instalação do dispositivo de serviços

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 serão mostradas com uma barra de status verde e um status de ""pulado"".

2. Reveja o progresso das duas primeiras fases de instalação.
   - **1. Configurar armazenamento**

     Durante esta etapa, o instalador limpa qualquer configuração existente das unidades no dispositivo e configura as configurações do host.

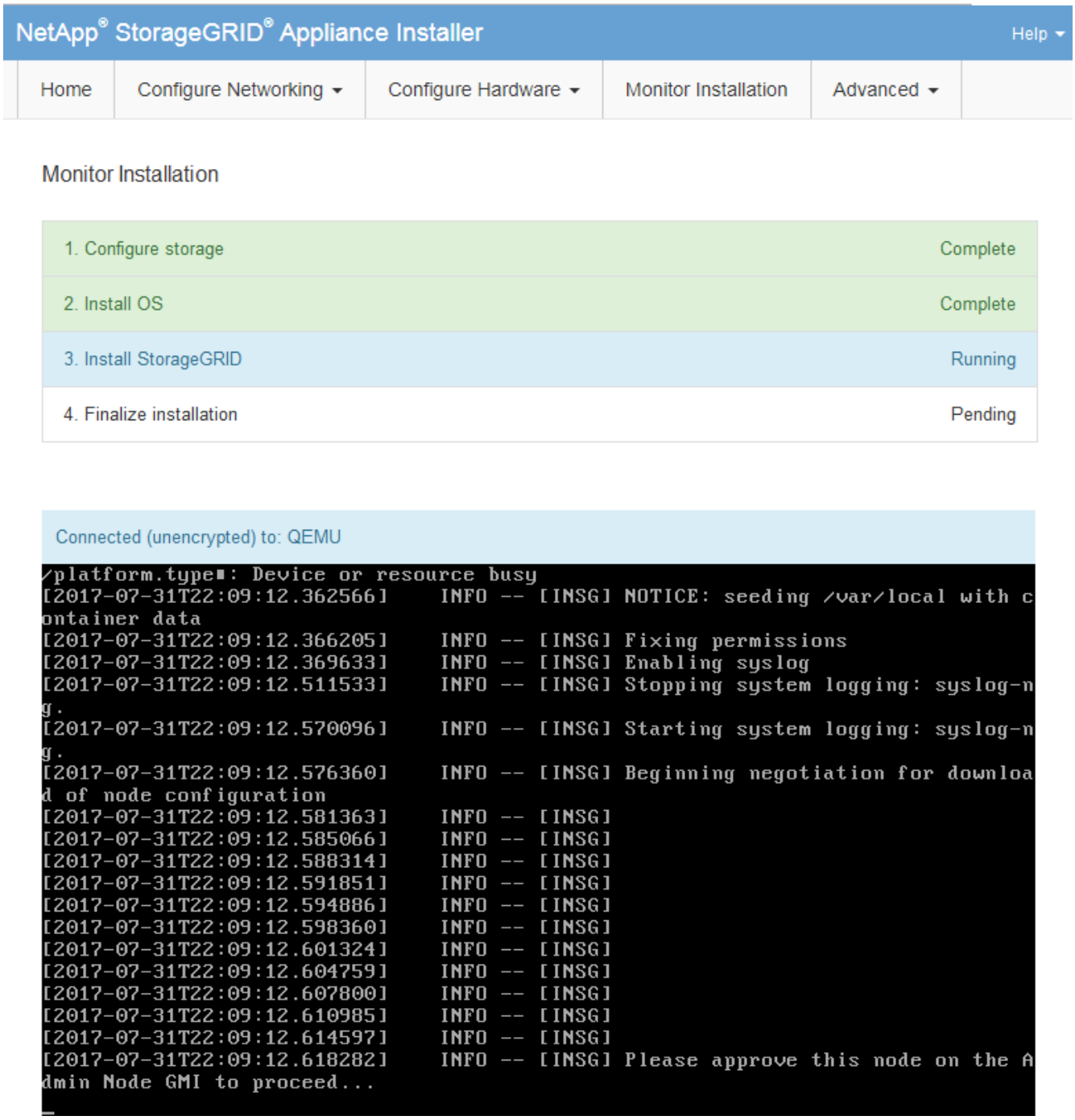
   - **2. Instale o os**

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 um dos seguintes processos ocorra:

   - Para todos os nós de appliance, exceto o nó de administrador principal, o estágio Instalar 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. Vá para a próxima etapa.
   - Para a instalação do nó de administração principal do dispositivo, não é necessário aprovar o nó. O aparelho é reinicializado. Você pode pular a próxima etapa.

   > ⓘ Durante a instalação de um nó de administração principal do appliance, aparece uma quinta fase (consulte o exemplo de captura de tela mostrando quatro fases). Se a quinta fase estiver em andamento por mais de 10 minutos, atualize a página da Web manualmente.



4. Vá para o Gerenciador de Grade, aprove o nó de grade pendente e conclua o processo de instalação do StorageGRID.

   Quando você clica em **Install** no Gerenciador de Grade, o estágio 3 é concluído e o estágio 4, **Finalize a instalação**, começa. Quando a fase 4 estiver concluída, o aparelho é reinicializado.

Automatizando a instalação e a configuração do dispositivo

Você pode automatizar a instalação e configuração de seus dispositivos e a configuração de todo o sistema StorageGRID.

Sobre esta tarefa

A automação da instalação e configuração pode ser útil para implantar várias instâncias do StorageGRID ou uma instância grande e complexa do StorageGRID.

Para automatizar a instalação e a configuração, use uma ou mais das seguintes opções:

- Crie um arquivo JSON que especifique as configurações para seus dispositivos. Carregue o arquivo JSON usando o instalador do dispositivo StorageGRID.

  Você pode usar o mesmo arquivo para configurar mais de um dispositivo.

- Use o script Python do StorageGRID`configure-sga.py` para automatizar a configuração de seus dispositivos.
- Use scripts Python adicionais para configurar outros componentes de todo o sistema StorageGRID (a "grade").

Você pode usar os scripts Python de automação do StorageGRID diretamente ou usá-los como exemplos de como usar a API REST de instalação do StorageGRID nas ferramentas de implantação e configuração de grade que você mesmo desenvolve. Consulte as informações sobre como baixar e extrair os arquivos de instalação do StorageGRID nas instruções de recuperação e manutenção.

Informações relacionadas

"Manter recuperar"

Automatizando a configuração do dispositivo usando o Instalador de dispositivos StorageGRID

Você pode automatizar a configuração de um appliance usando um arquivo JSON que contém as informações de configuração. Você carrega o arquivo usando o Instalador do StorageGRID Appliance.

O que você vai precisar

- O seu dispositivo tem de estar no firmware mais recente compatível com o StorageGRID 11,5 ou superior.
- Você deve estar conetado ao Instalador do StorageGRID Appliance no dispositivo que você está configurando usando um navegador compatível.

Sobre esta tarefa

É possível automatizar as tarefas de configuração do dispositivo, como configurar o seguinte:

- Rede de grade, rede de administração e endereços IP da rede de cliente
- Interface BMC
- Ligações de rede
  - Modo de ligação da porta
  - Modo de ligação de rede
  - Velocidade da ligação

Configurar o dispositivo usando um arquivo JSON carregado geralmente é mais eficiente do que executar a configuração manualmente usando várias páginas no Instalador de dispositivos StorageGRID, especialmente se você tiver que configurar muitos nós. Você deve aplicar o arquivo de configuração para cada nó um de cada vez.

Usuários experientes que desejam automatizar tanto a instalação quanto a configuração de seus dispositivos podem usar o `configure-sga.py` script. E "Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py"

Passos

1. Gere o arquivo JSON usando um dos seguintes métodos:
   - O aplicativo ConfigBuilder

     "ConfigBuilder.NetApp.com"

   - O `configure-sga.py` script de configuração do dispositivo. Você pode baixar o script do Instalador do StorageGRID Appliance (**Ajuda Script de configuração do appliance**). Consulte as instruções sobre como automatizar a configuração usando o script configure-sga.py.

     "Automatizando a instalação e a configuração dos nós de dispositivos usando o script configure-sga.py"

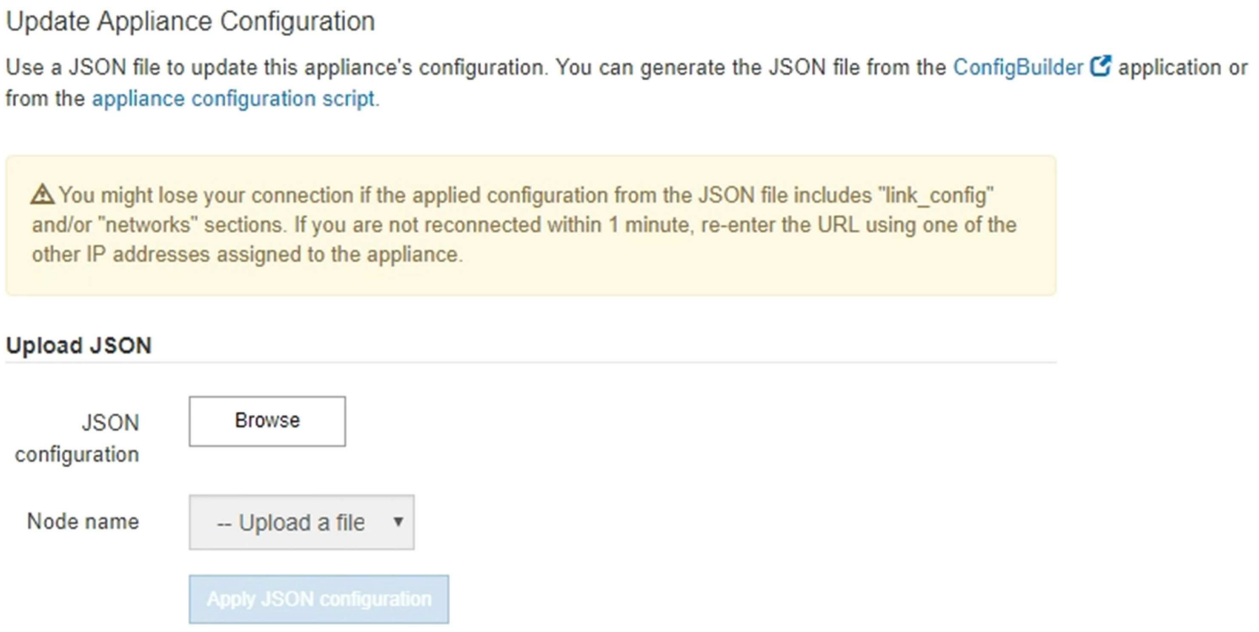
     Os nomes de nós no arquivo JSON devem seguir estes requisitos:

     - Deve ser um nome de host válido contendo pelo menos 1 e não mais de 32 carateres
     - Pode usar letras, números e hífens são permitidos
     - Não é possível iniciar ou terminar com um hífen ou conter apenas números

     Certifique-se de que os nomes dos nós (os nomes de nível superior) no arquivo JSON sejam únicos, ou você não poderá configurar mais de um nó usando o arquivo JSON.

2. Selecione **Avançado Atualizar Configuração do dispositivo**.

   É apresentada a página Update Appliance Configuration (Atualizar configuração do dispositivo).



3. Selecione o arquivo JSON com a configuração que você deseja carregar.

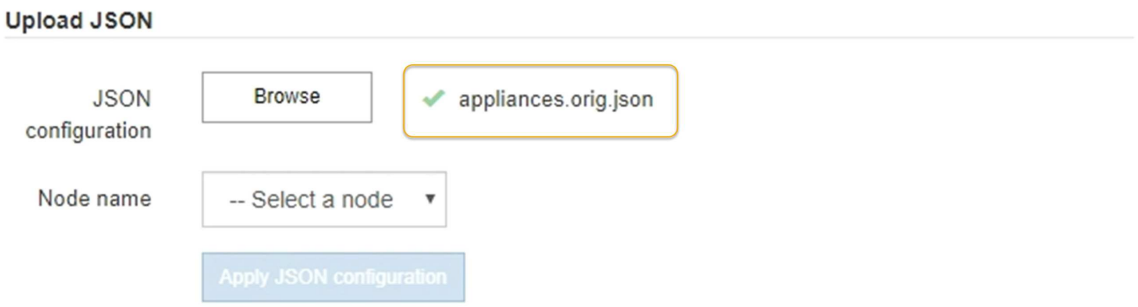
   a. Selecione **Procurar**.

   b. Localize e selecione o ficheiro.

   c. Selecione **Open**.

   O arquivo é carregado e validado. Quando o processo de validação estiver concluído, o nome do ficheiro é apresentado junto a uma marca de verificação verde.

   > Você pode perder a conexão com o dispositivo se a configuração do arquivo JSON incluir seções para "link_config", "redes" ou ambos. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do dispositivo usando um dos outros endereços IP atribuídos ao dispositivo.

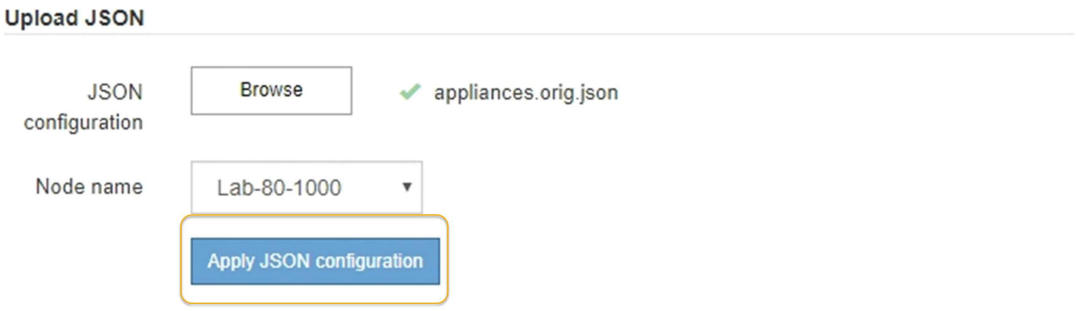


   A lista suspensa **Nome do nó** é preenchida com os nomes de nós de nível superior definidos no arquivo JSON.

   > Se o arquivo não for válido, o nome do arquivo será exibido em vermelho e uma mensagem de erro será exibida em um banner amarelo. O ficheiro inválido não é aplicado ao dispositivo. Você pode usar o ConfigBuilder para garantir que você tenha um arquivo JSON válido.

4. Selecione um nó na lista suspensa **Nome do nó**.

   O botão **Apply JSON Configuration** está ativado.



5. Selecione **Apply JSON Configuration**.

   A configuração é aplicada ao nó selecionado.

Você pode usar `configure-sga.py` o script para automatizar muitas das tarefas de instalação e configuração para os nós de dispositivos StorageGRID, incluindo a instalação e configuração de um nó de administrador principal. Este script pode ser útil se você tiver um grande número de dispositivos para configurar. Você também pode usar o script para gerar um arquivo JSON que contém informações de configuração do dispositivo.

O que você vai precisar

- O dispositivo foi instalado em um rack, conetado às redes e ligado.
- Links de rede e endereços IP foram configurados para o nó de administração principal usando o instalador do dispositivo StorageGRID.
- Se você estiver instalando o nó Admin principal, você saberá seu endereço IP.
- Se você estiver instalando e configurando outros nós, o nó Admin principal foi implantado e você sabe seu endereço IP.
- Para todos os nós que não o nó de administração principal, 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.
- Você baixou o `configure-sga.py` arquivo. O arquivo está incluído no arquivo de instalação, ou você pode acessá-lo clicando em **Ajuda Script de Instalação do dispositivo** no Instalador do StorageGRID Appliance.

> ⓘ Este procedimento é para usuários avançados com alguma experiência usando interfaces de linha de comando. Como alternativa, você também pode usar o Instalador de dispositivos StorageGRID para automatizar a configuração. E "Automatizando a configuração do dispositivo usando o Instalador de dispositivos StorageGRID"

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Para obter ajuda geral com a sintaxe do script e para ver uma lista dos parâmetros disponíveis, digite o seguinte:

   ```
   configure-sga.py --help
   ```

   O `configure-sga.py` script usa cinco subcomandos:

   - `advanced` Para interações avançadas do StorageGRID Appliance, incluindo a configuração do BMC e a criação de um arquivo JSON contendo a configuração atual do dispositivo
   - `configure` Para configurar o modo RAID, o nome do nó e os parâmetros de rede
   - `install` Para iniciar uma instalação do StorageGRID
   - `monitor` Para monitorar uma instalação do StorageGRID
   - `reboot` para reiniciar o aparelho

   Se você inserir um argumento de subcomando (avançado, configurar, instalar, monitorar ou reiniciar)

seguido da `--help` opção, você receberá um texto de ajuda diferente fornecendo mais detalhes sobre as opções disponíveis dentro desse subcomando
`configure-sga.py *subcommand* --help`

3. Para confirmar a configuração atual do nó do dispositivo, digite o seguinte local *`SGA-install-ip`* onde está qualquer um dos endereços IP do nó do dispositivo
`configure-sga.py configure *SGA-INSTALL-IP*`

Os resultados mostram informações de IP atuais para o dispositivo, incluindo o endereço IP do nó de administração principal e informações sobre as redes de administração, grade e cliente.

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
```

```
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4

        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

####################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
####################################################################
```

4. Se você precisar alterar qualquer um dos valores na configuração atual, use o `configure` subcomando

para atualizá-los. Por exemplo, se você quiser alterar o endereço IP que o dispositivo usa para conexão com o nó Admin principal para `172.16.2.99`, digite o seguinte
`configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP`

5. Se você quiser fazer backup da configuração do appliance em um arquivo JSON, use os subcomandos avançado e `backup-file` . Por exemplo, se você quiser fazer backup da configuração de um dispositivo com endereço IP *SGA-INSTALL-IP* para um arquivo chamado `appliance-SG1000.json`, digite o seguinte
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

   O arquivo JSON contendo as informações de configuração é gravado no mesmo diretório do qual você executou o script.

   > Verifique se o nome do nó de nível superior no arquivo JSON gerado corresponde ao nome do dispositivo. Não faça alterações neste arquivo, a menos que você seja um usuário experiente e tenha uma compreensão completa das APIs do StorageGRID.

6. Quando estiver satisfeito com a configuração do aparelho, utilize os `install` subcomandos e `monitor` para instalar o aparelho
`configure-sga.py install --monitor SGA-INSTALL-IP`
7. Se pretender reiniciar o aparelho, introduza o seguinte
`configure-sga.py reboot SGA-INSTALL-IP`

Automatizando a configuração do StorageGRID

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

O que você vai precisar

- 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 amostra (`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
   ```

Depois de terminar

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, você precisa extrair o `Passwords.txt` arquivo e procurar 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.
```

Visão geral das APIs REST de instalação

O StorageGRID fornece duas APIs REST para executar tarefas de instalação: A API de instalação do StorageGRID e a API do instalador do dispositivo StorageGRID.

Ambas as APIs usam 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 (JavaScript Object Notation).

> Todas as operações de API que você executa usando a página da Web do API Docs 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 seu sistema StorageGRID e, caso precise 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.

API do instalador do dispositivo StorageGRID

A API do instalador do dispositivo StorageGRID pode ser acessada por HTTPS a partir `*Controller_IP*:8443`do .

Para acessar a documentação da API, vá para o Instalador do StorageGRID Appliance no appliance e

selecione **Ajuda Documentação da API** na barra de menus.

A API do instalador do StorageGRID Appliance inclui as seguintes seções:

- **Clone** — operações para configurar e controlar a clonagem de nós.
- **Encryption** — operações para gerenciar a criptografia e visualizar o status da criptografia.
- **Configuração de hardware** — operações para configurar as configurações do sistema no hardware conetado.
- **Installation** — operações para iniciar a instalação do aparelho e para monitorar o status da instalação.
- **Networking** — operações relacionadas à configuração de rede, administrador e rede cliente para um dispositivo StorageGRID e configurações de porta de dispositivo.
- **Setup** — operações para ajudar na configuração inicial da instalação do dispositivo, incluindo solicitações para obter informações sobre o sistema e atualizar o IP do nó de administração principal.
- **Support** — operações para reiniciar o controlador e obter logs.
- **Upgrade** — operações relacionadas à atualização do firmware do appliance.
- * Uploadsg* — operações para upload de arquivos de instalação do StorageGRID.

Solução de problemas da instalação do hardware

Se você encontrar problemas durante a instalação, talvez seja útil revisar informações de solução de problemas relacionadas a problemas de configuração de hardware e conetividade.

Informações relacionadas

"A configuração do hardware parece travar"

"Solução de problemas de conexão"

Visualização dos códigos de arranque do aparelho

Quando você aplica energia ao aparelho, o BMC Registra uma série de códigos de inicialização. Você pode exibir esses códigos em um console gráfico conetado à porta de gerenciamento do BMC.

O que você vai precisar

- Você sabe como acessar o painel do BMC.
- Se você quiser usar uma máquina virtual baseada em kernel (KVM), você tem experiência em implantar e usar aplicativos KVM.
- Se você quiser usar serial-over-laN (sol), você tem experiência usando aplicativos de console IPMI sol.

Passos

1. Selecione um dos seguintes métodos para visualizar os códigos de arranque do controlador do aparelho e recolha o equipamento necessário.

Método	Equipamento necessário
Consola VGA	• Monitor compatível com VGA • Cabo VGA
KVM	• Aplicação KVM • Cabo RJ-45
Porta serial	• Cabo serial DB-9 • Terminal serial virtual
SOL	• Terminal serial virtual

2. Se você estiver usando um console VGA, execute estas etapas:
   a. Ligue um monitor compatível com VGA à porta VGA na parte posterior do aparelho.
   b. Veja os códigos exibidos no monitor.
3. Se você estiver usando o BMC KVM, execute estas etapas:
   a. Conete-se à porta de gerenciamento do BMC e faça login na interface da Web do BMC.
   b. Selecione **Controle remoto**.
   c. Inicie o KVM.
   d. Veja os códigos no monitor virtual.
4. Se você estiver usando uma porta serial e um terminal, execute estas etapas:
   a. Conete-se à porta serial DB-9 na parte traseira do aparelho.
   b. Utilize as definições `115200 8-N-1`.
   c. Veja os códigos impressos no terminal serial.
5. Se você estiver usando sol, execute estas etapas:
   a. Conete-se ao sol IPMI usando o endereço IP BMC e as credenciais de login.

      ```
      ipmitool -I lanplus -H 10.224.3.91 -U root -P calvin sol activate
      ```

   b. Veja os códigos no terminal serial virtual.
6. Utilize a tabela para procurar os códigos do seu aparelho.

Código	Indica
OLÁ	O script de inicialização mestre foi iniciado.
HP	O sistema está verificando se o firmware da placa de interface de rede (NIC) precisa ser atualizado.
RB	O sistema está reiniciando após a aplicação de atualizações de firmware.

Código	Indica
FP	As verificações de atualização do firmware do subsistema de hardware foram concluídas. Os serviços de comunicação entre controladores estão a iniciar.
HC	O sistema está a verificar se existem dados de instalação do StorageGRID.
HO	O dispositivo StorageGRID está em funcionamento.
HA	O StorageGRID está em execução.

Informações relacionadas

"Acessando a interface BMC"

Visualizar códigos de erro para o aparelho

Se ocorrer um erro de hardware quando o aparelho está inicializando, o BMC Registra um código de erro. Conforme necessário, você pode visualizar esses códigos de erro usando a interface do BMC e trabalhar com suporte técnico para resolver o problema.

O que você vai precisar

- Você sabe como acessar o painel do BMC.

Passos

1. No painel do BMC, selecione **Código POST do BIOS**.
2. Reveja as informações apresentadas para o Código atual e o Código anterior.

   Se algum dos códigos de erro a seguir for exibido, trabalhe com suporte técnico para resolver o problema.

Código	Indica
0x0E	Microcódigo não encontrado
0x0F	Microcódigo não carregado
0x50	Erro de inicialização da memória. Tipo de memória inválido ou velocidade de memória incompatível.
0x51	Erro de inicialização da memória. A leitura SPD falhou.
0x52	Erro de inicialização da memória. O tamanho de memória inválido ou os módulos de memória não correspondem.

Código	Indica
0x53	Erro de inicialização da memória. Nenhuma memória utilizável detetada.
0x54	Erro de inicialização de memória não especificado
0x55	Memória não instalada
0x56	Tipo ou velocidade de CPU inválida
0x57	Incompatibilidade de CPU
0x58	Falha no autoteste da CPU ou possível erro de cache da CPU
0x59	O micro-código da CPU não foi encontrado ou a atualização do micro-código falhou
0x5A	Erro interno da CPU
0x5B	Repor PPI não está disponível
0x5C	Falha do autoteste do PEI fase BMC
0xD0	Erro de inicialização da CPU
0xD1	Erro de inicialização da ponte Norte
0xD2	Erro de inicialização da ponte sul
0xD3	Alguns protocolos arquitetônicos não estão disponíveis
0xD4	Erro de alocação de recursos PCI. Sem recursos.
0xD5	Sem espaço para a ROM de opção herdada
0xD6	Não foram encontrados dispositivos de saída da consola
0xD7	Não foram encontrados dispositivos de entrada da consola
0xD8	Palavra-passe inválida

Código	Indica
0xD9	Erro ao carregar a opção de inicialização (erro loadImage retornado)
0xDA	Falha na opção de inicialização (erro retornado pela StartImage)
0xDB	Falha na atualização do flash
0xDC	O protocolo de reposição não está disponível
0xDD	Avaria no autoteste do BMC de fase DXE
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY
0xEF	RMC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERNAL
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK

Código	Indica
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

A configuração do hardware parece travar

O Instalador de dispositivos StorageGRID pode não estar disponível se falhas de hardware ou erros de cabeamento impedirem que o aparelho conclua seu processamento de inicialização.

Passos

1. Reveja os LEDs no aparelho e os códigos de inicialização e de erro exibidos no BMC.
2. Se você precisar de ajuda para resolver um problema, entre em Contato com o suporte técnico.

Informações relacionadas

"Visualização dos códigos de arranque do aparelho"

"Visualizar códigos de erro para o aparelho"

Solução de problemas de conexão

Se você encontrar problemas de conexão durante a instalação do StorageGRID Appliance, execute as etapas de ação corretiva listadas.

Não foi possível ligar ao aparelho

Se você não conseguir se conetar ao utilitário de serviços, pode haver um problema de rede ou a instalação de hardware pode não ter sido concluída com êxito.

Passos

1. Tente fazer ping no aparelho usando o endereço IP do aparelho
   `ping services_appliance_IP`
2. Se não receber resposta do ping, confirme que está a utilizar o endereço IP correto.

   Pode utilizar o endereço IP do dispositivo na rede de grelha, na rede de administração ou na rede de cliente.

3. Se o endereço IP estiver correto, verifique o cabeamento do dispositivo, transcetores QSFP ou SFP e a configuração da rede.

   Se isso não resolver o problema, entre em Contato com o suporte técnico.

4. Se o ping foi bem-sucedido, abra um navegador da Web.
5. Digite o URL do instalador do StorageGRID Appliance
   `https://appliances_controller_IP:8443`

   A página inicial é exibida.

Reiniciar o utilitário de serviços enquanto o Instalador de dispositivos StorageGRID está em execução

Talvez seja necessário reiniciar o utilitário de serviços enquanto o Instalador de dispositivos StorageGRID estiver em execução. Por exemplo, você pode precisar reiniciar o utilitário de serviços se a instalação falhar.

Sobre esta tarefa

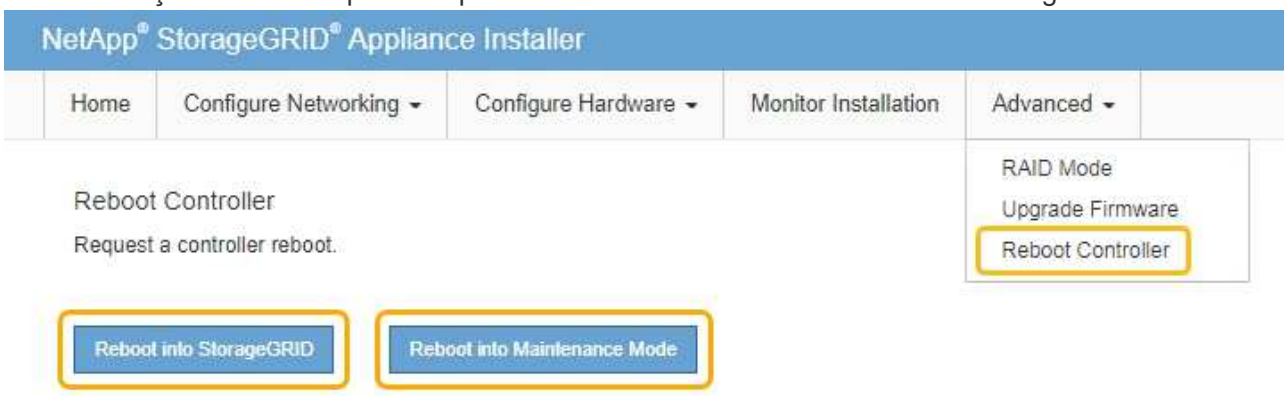
Este procedimento aplica-se apenas quando o utilitário de serviços está a executar o Instalador de dispositivos StorageGRID. Depois que a instalação estiver concluída, esta etapa não funcionará mais porque o Instalador de dispositivos StorageGRID não está mais disponível.

Passos

1. Na barra de menus do Instalador de dispositivos StorageGRID, clique em **Avançado Reiniciar controlador**.

   A página Reiniciar controlador é exibida.

2. No Instalador do StorageGRID Appliance, clique em **Avançado controlador de reinicialização** e selecione uma destas opções:
   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



   O utilitário de serviços é reinicializado.

Manutenção do aparelho

Poderá ser necessário efetuar procedimentos de manutenção no aparelho. Os procedimentos nesta seção pressupõem que o dispositivo já foi implantado como um nó de gateway ou um nó de administrador em um sistema StorageGRID.

Passos

- "Colocar um aparelho no modo de manutenção"
- "Ligar e desligar o LED de identificação do controlador"
- "Localizar o controlador em um data center"
- "Substituir o dispositivo de serviços"
- "Substituir uma fonte de alimentação no dispositivo de serviços"
- "Substituir uma ventoinha no dispositivo de serviços"
- "Substituir uma unidade no dispositivo de serviços"
- "Alterar a configuração do link do dispositivo de serviços"
- "Alterar a definição MTU"
- "Verificar a configuração do servidor DNS"
- "Monitorização da encriptação do nó no modo de manutenção"

Colocar um aparelho no modo de manutenção

Deve colocar o aparelho no modo de manutenção antes de efetuar procedimentos de manutenção específicos.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

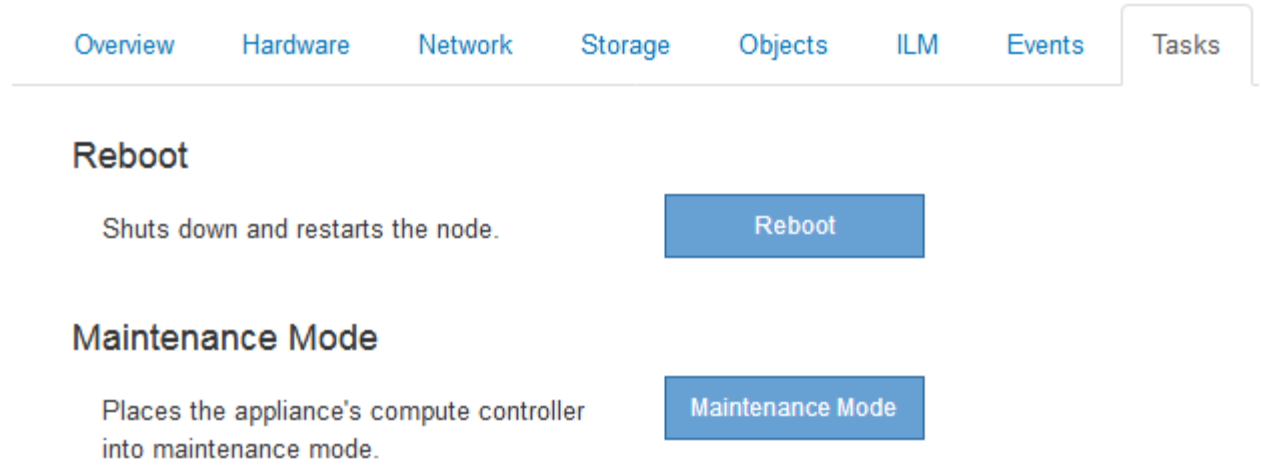
Sobre esta tarefa

Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

> A senha e a chave de host de um dispositivo StorageGRID no modo de manutenção permanecem as mesmas que eram quando o aparelho estava em serviço.

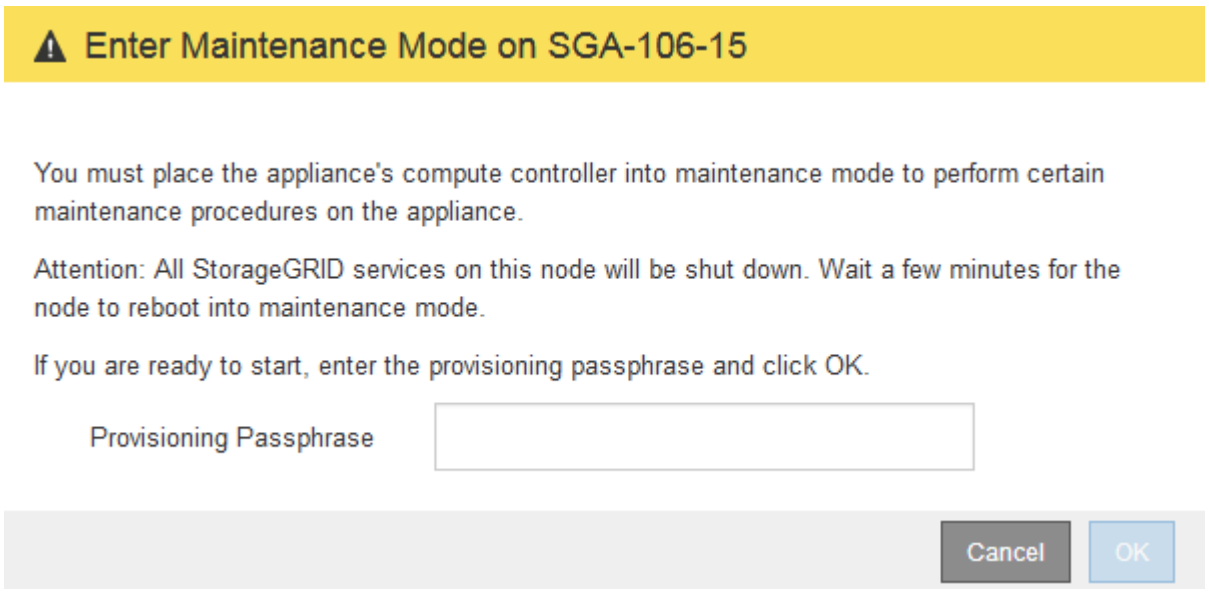
Passos

1. No Gerenciador de Grade, selecione **nós**.
2. Na exibição em árvore da página nós, selecione o nó de storage do dispositivo.
3. Selecione **tarefas**.



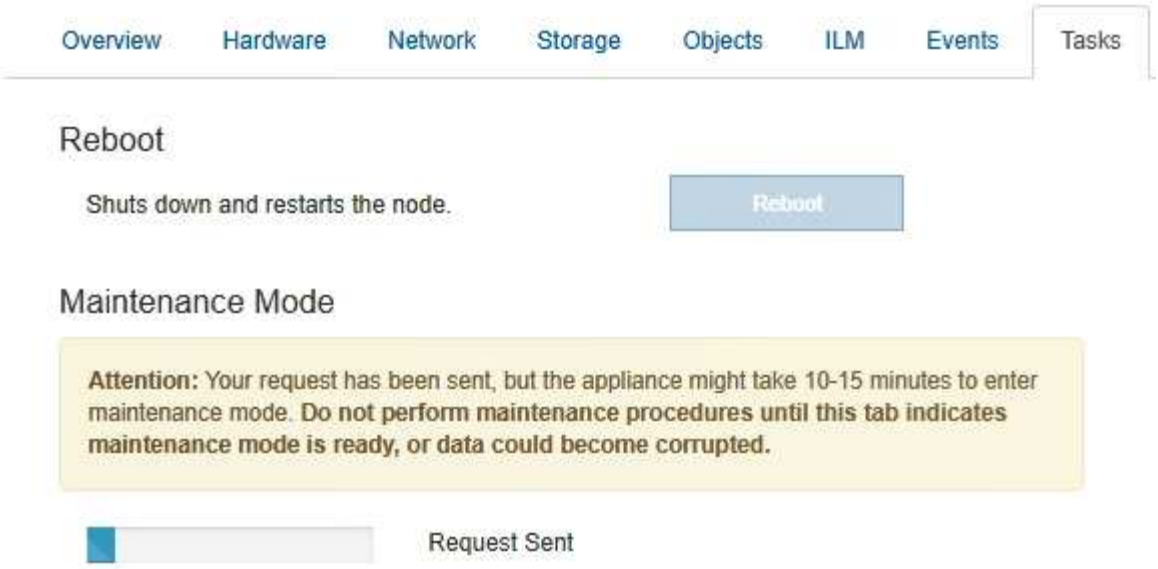
4. Selecione **Maintenance Mode** (modo de manutenção).

   É apresentada uma caixa de diálogo de confirmação.

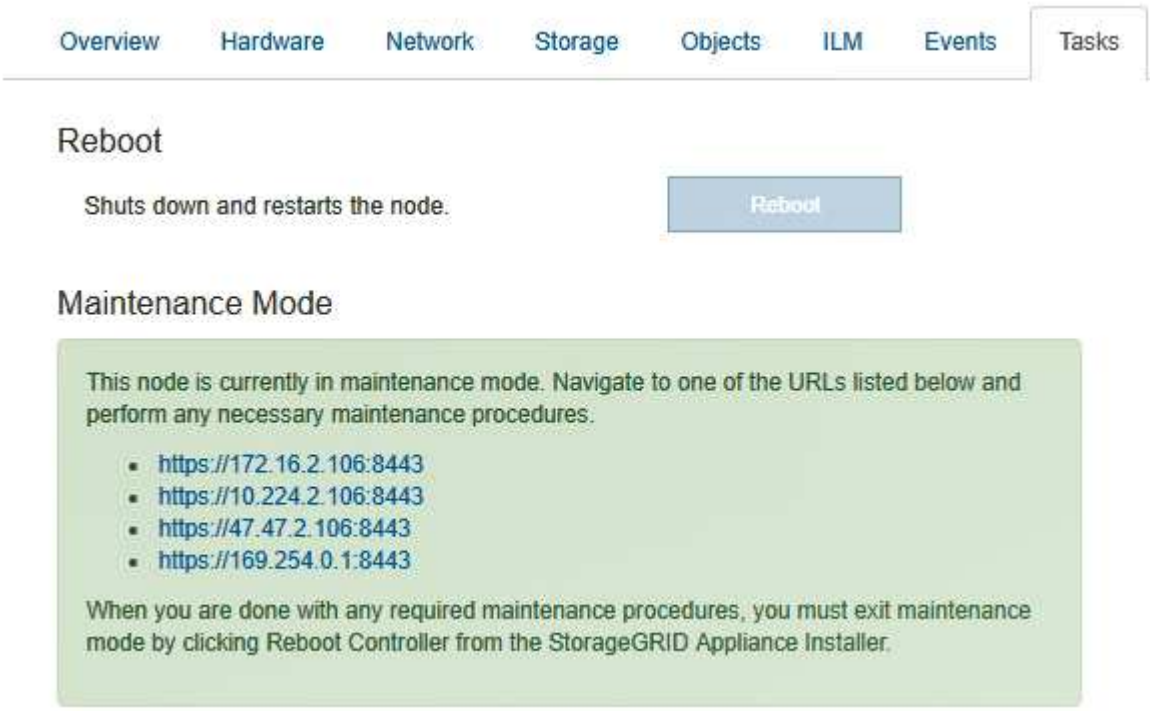


5. Introduza a frase-passe de aprovisionamento e selecione **OK**.

   Uma barra de progresso e uma série de mensagens, incluindo "Request Sent" (pedido enviado), "Stop" (Paragem de StorageGRID) e "Reboot" (reinício), indicam que o aparelho está a concluir os passos para entrar no modo de manutenção.



Quando o dispositivo está no modo de manutenção, uma mensagem de confirmação lista os URLs que você pode usar para acessar o Instalador do StorageGRID Appliance.



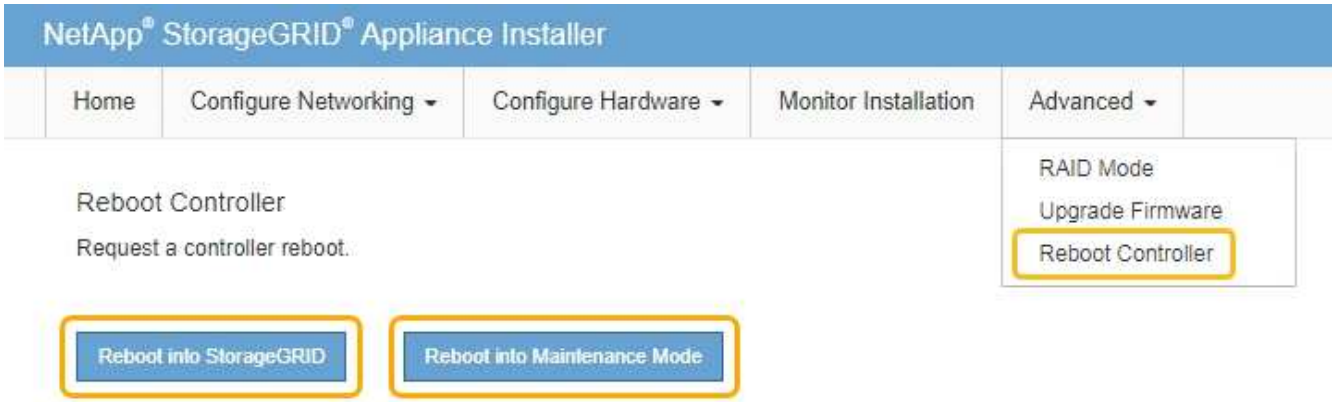
6. Para acessar o Instalador do StorageGRID Appliance, navegue até qualquer um dos URLs exibidos.

   Se possível, use o URL que contém o endereço IP da porta Admin Network do dispositivo.

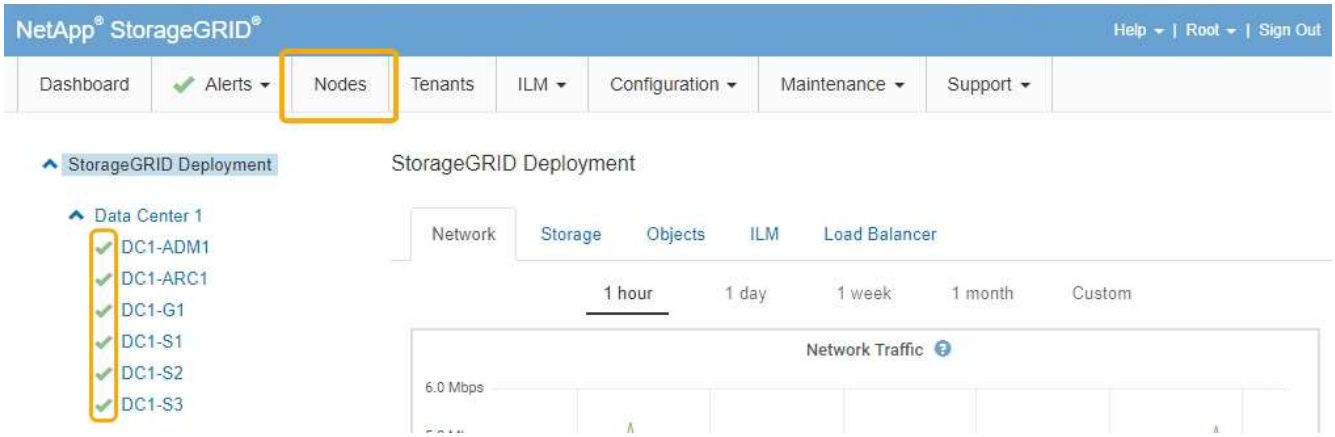
   > O acesso `https://169.254.0.1:8443` requer uma conexão direta com a porta de gerenciamento local.

7. A partir do instalador do dispositivo StorageGRID, confirme se o aparelho está no modo de manutenção.

8. Execute todas as tarefas de manutenção necessárias.
9. Depois de concluir as tarefas de manutenção, saia do modo de manutenção e retome a operação normal do nó. No Instalador de dispositivos StorageGRID, selecione **Avançado controlador de reinicialização** e, em seguida, selecione **Reiniciar no StorageGRID**.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Ligar e desligar o LED de identificação do controlador

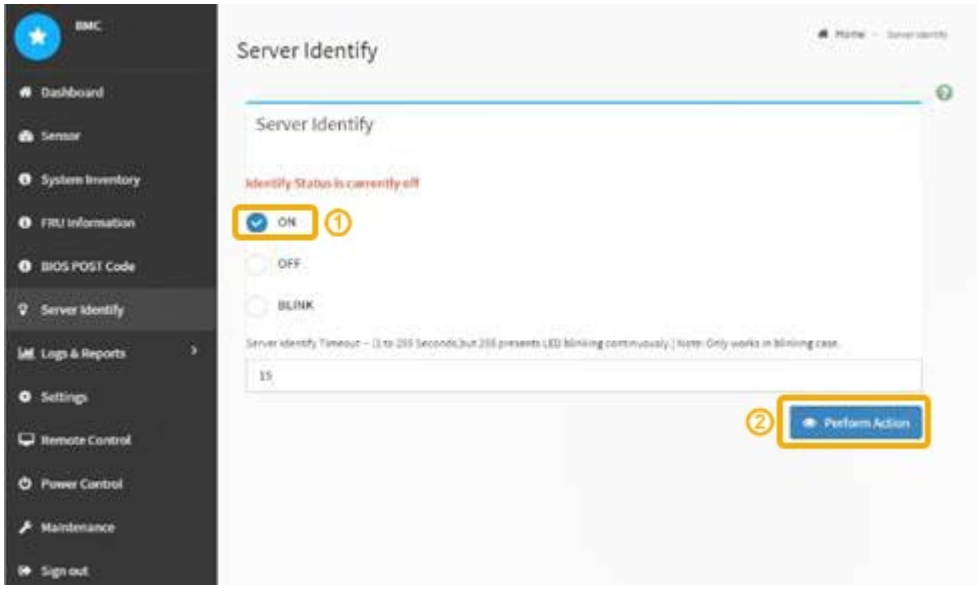
O LED de identificação azul na parte frontal e traseira do controlador pode ser ligado para ajudar a localizar o aparelho em um data center.

O que você vai precisar

Tem de ter o endereço IP BMC do controlador que pretende identificar.

Passos

1. Acesse a interface BMC do controlador.
2. Selecione **identificação do servidor**.
3. Selecione **ON** e, em seguida, selecione **Perform Action**.



Resultado

Os LEDs de identificação azul acendem-se na parte frontal (mostrada) e traseira do controlador.

Se um painel frontal estiver instalado no controlador, pode ser difícil ver o LED de identificação frontal.

Depois de terminar

Para desligar o LED de identificação do controlador:

- Pressione o interrutor Identify LED no painel frontal do controlador.
- Na interface BMC do controlador, selecione **identificação do servidor**, selecione **OFF** e, em seguida, selecione **Perform Action**.

Os LEDs de identificação azul na parte frontal e traseira do controlador apagam-se.

Informações relacionadas

"Localizar o controlador em um data center"

"Acessando a interface BMC"

Localizar o controlador em um data center

Localize o controlador para que você possa executar a manutenção ou atualizações de hardware.

O que você vai precisar

- Você determinou qual controlador requer manutenção.

  (Opcional) para ajudar a localizar o controlador no seu data center, ligue o LED de identificação azul.

  "Ligar e desligar o LED de identificação do controlador"

Passos

1. Encontre o controlador que precisa de manutenção no data center.
   - Procure um LED de identificação azul aceso na parte frontal ou traseira do controlador.

     O LED de identificação frontal está atrás do painel frontal do controlador e pode ser difícil ver se o painel frontal está instalado.

   - Verifique se há um número de peça correspondente nas etiquetas anexadas à frente de cada controlador.

2. Remova o painel frontal do controlador, se estiver instalado, para acessar os controles e indicadores do painel frontal.
3. Opcional: Desligue o LED de identificação azul se o tiver utilizado para localizar o controlador.
   - Pressione o interrutor Identify LED no painel frontal do controlador.
   - Use a interface BMC do controlador.

     "Ligar e desligar o LED de identificação do controlador"

Substituir o dispositivo de serviços

Pode ser necessário substituir o aparelho se não estiver a funcionar de forma ideal ou se tiver falhado.

O que você vai precisar

- Tem um aparelho de substituição com o mesmo número de peça do aparelho que está a substituir.
- Tem etiquetas para identificar cada cabo ligado ao aparelho.
- Você localizou fisicamente o dispositivo que está substituindo no data center. "Localizar o controlador em um data center"Consulte .
- O aparelho foi colocado no modo de manutenção. "Colocar um aparelho no modo de manutenção"Consulte .

Sobre esta tarefa

O nó StorageGRID não estará acessível enquanto você substituir o dispositivo. Se o aparelho estiver a funcionar o suficiente, pode efetuar um encerramento controlado no início deste procedimento.

> Se estiver a substituir o dispositivo antes de instalar o software StorageGRID, poderá não conseguir aceder ao instalador do StorageGRID Appliance imediatamente após concluir este procedimento. Embora você possa acessar o Instalador de dispositivos StorageGRID de outros hosts na mesma sub-rede que o appliance, você não pode acessá-lo de hosts em outras sub-redes. Esta condição deve resolver-se dentro de 15 minutos (quando qualquer entrada de cache ARP para o tempo limite do dispositivo original), ou você pode limpar a condição imediatamente, limpando quaisquer entradas de cache ARP antigas manualmente do roteador ou gateway local.

Passos

1. Quando o aparelho tiver sido colocado no modo de manutenção, desligue o aparelho.
   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. Desligue o aparelho
      `shutdown -h now`

2. Utilize um de dois métodos para verificar se a alimentação do aparelho está desligada:
   - O LED indicador de alimentação na parte frontal do aparelho está apagado.
   - A página Controle de energia da interface BMC indica que o aparelho está desligado.
3. Se as redes StorageGRID conetadas ao dispositivo usarem servidores DHCP, atualize as configurações de DNS/rede e endereço IP.

   a. Localize a etiqueta de endereço MAC na parte frontal do dispositivo e determine o endereço MAC da porta Admin Network.

      O rótulo de endereço MAC lista o endereço MAC da porta de gerenciamento BMC.

      Para determinar o endereço MAC da porta Admin Network, você deve adicionar **2** ao número hexadecimal na etiqueta. Por exemplo, se o endereço MAC na etiqueta terminar em **09**, o endereço MAC da porta Admin terminaria em **0B**. Se o endereço MAC na etiqueta terminar em **(*y*)FF**, o endereço MAC da porta Admin terminaria em **(*y*(1)01**. Você pode facilmente fazer esse cálculo abrindo o Calculator no Windows, definindo-o para o modo Programador, selecionando Hex, digitando o endereço MAC e, em seguida, digitando * 2 *.

   b. Peça ao administrador da rede para associar o DNS/rede e o endereço IP do dispositivo removido com o endereço MAC do dispositivo de substituição.

      Deve certificar-se de que todos os endereços IP do aparelho original foram atualizados antes de ligar a alimentação ao aparelho de substituição. Caso contrário, o dispositivo obterá novos endereços IP DHCP quando inicializa e poderá não conseguir reconetar-se ao StorageGRID. Esta etapa se aplica a todas as redes StorageGRID conetadas ao dispositivo.

   Se o dispositivo original tiver utilizado um endereço IP estático, o novo dispositivo irá adotar automaticamente os endereços IP do aparelho que removeu.

4. Retire e substitua o aparelho:

   a. Identifique os cabos e, em seguida, desligue os cabos e quaisquer transcetores de rede.

      Para evitar um desempenho degradado, não torça, dobre, aperte ou pise nos cabos.

   b. Remova o aparelho com falha do gabinete ou rack.
   c. Transfira as duas fontes de alimentação, oito ventoinhas de arrefecimento e dois SSDs do aparelho com falha para o aparelho de substituição.

      Siga as instruções fornecidas para a substituição destes componentes.

   d. Instale o aparelho de substituição no gabinete ou rack.
   e. Substitua os cabos e quaisquer transcetores óticos.
   f. Ligue o aparelho e monitorize os LEDs do aparelho e os códigos de arranque.

      Use a interface BMC para monitorar o status de inicialização.

5. Confirme se o nó do dispositivo é exibido no Gerenciador de Grade e se nenhum alerta é exibido.

Informações relacionadas

"Instalar o aparelho em um gabinete ou rack (SG100 e SG1000)"

"Visualização de indicadores de status nos aparelhos SG100 e SG1000"

"Visualização dos códigos de arranque do aparelho"

Substituir uma fonte de alimentação no dispositivo de serviços

O dispositivo de serviços tem duas fontes de alimentação para redundância. Se uma das fontes de alimentação falhar, você deve substituí-la o mais rápido possível para garantir que o aparelho tenha alimentação redundante.

O que você vai precisar

- Desembalou a fonte de alimentação de substituição.
- Localizou fisicamente o aparelho onde está a substituir a fonte de alimentação no centro de dados.

  "Localizar o controlador em um data center"

- Você pode confirmar que a outra fonte de alimentação está instalada e funcionando.

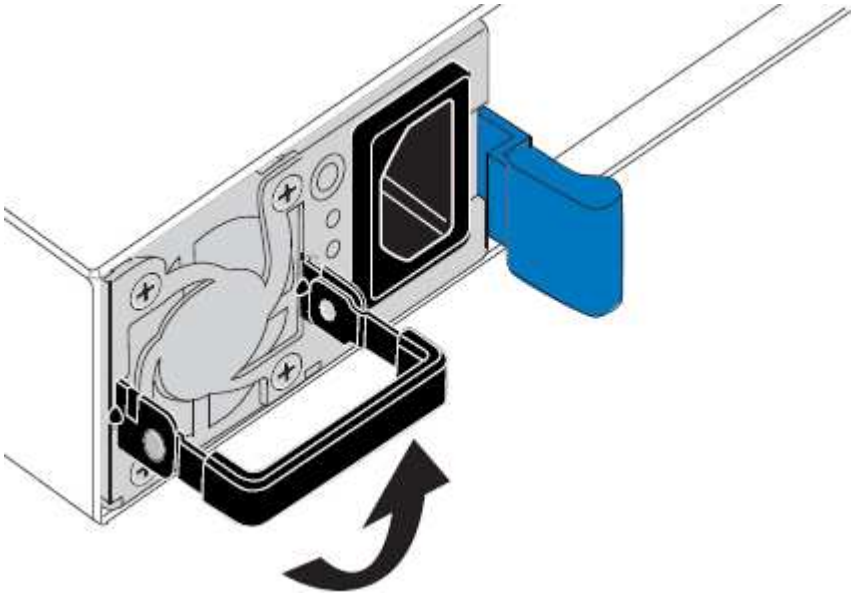
Sobre esta tarefa

A figura mostra as duas fontes de alimentação para o SG100, que estão acessíveis a partir da parte de trás do aparelho.

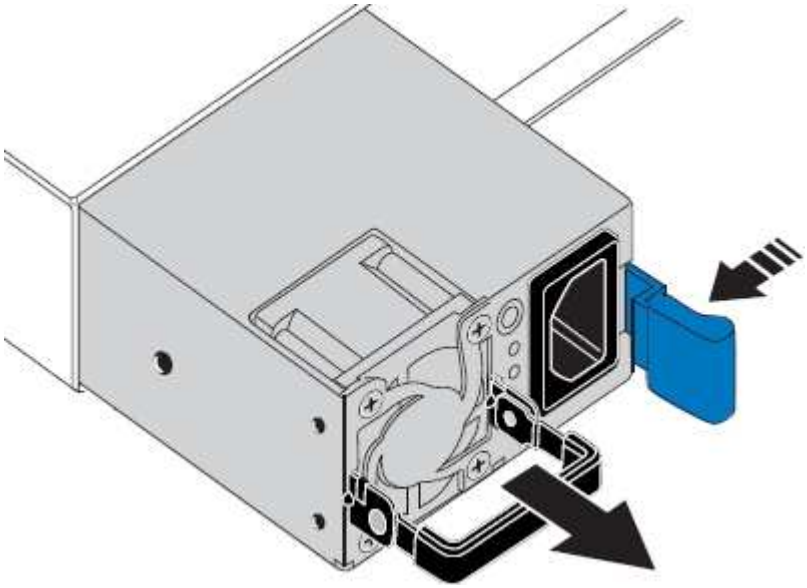
As fontes de alimentação para o SG1000 são idênticas.

Passos

1. Desconete o cabo de alimentação da fonte de alimentação.
2. Levante o manípulo do excêntrico.

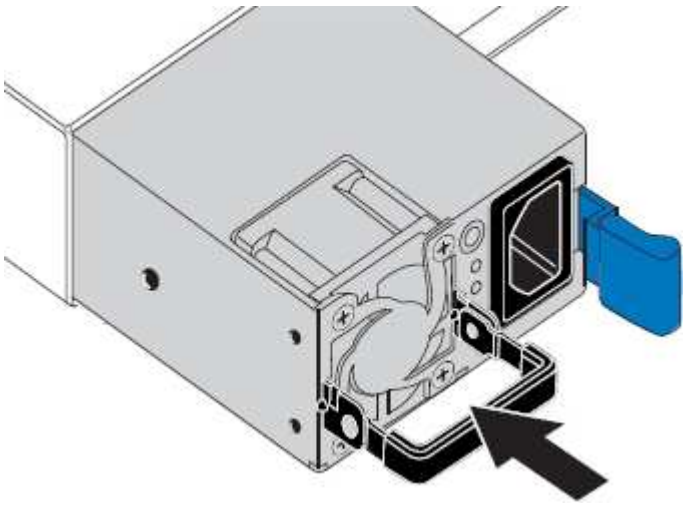


3. Pressione o trinco azul e puxe a fonte de alimentação para fora.



4. Faça deslizar a fonte de alimentação de substituição para o chassis.

   Certifique-se de que o trinco azul se encontra no lado direito ao deslizar a unidade para dentro.



5. Empurre o manípulo do came para baixo para fixar a fonte de alimentação.
6. Ligue o cabo de alimentação à fonte de alimentação e certifique-se de que o LED verde se acende.

Substituir uma ventoinha no dispositivo de serviços

O aparelho de serviços tem oito ventiladores de refrigeração. Se uma das ventoinhas falhar, deve substituí-la o mais rapidamente possível para garantir que o aparelho arrefeça corretamente.

O que você vai precisar

- Desembalou a ventoinha de substituição.
- Você localizou fisicamente o aparelho onde está substituindo o ventilador no data center.

  "Localizar o controlador em um data center"

- Você confirmou que os outros ventiladores estão instalados e funcionando.
- O aparelho foi colocado no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

O nó do aparelho não estará acessível enquanto substituir a ventoinha.

A fotografia mostra um ventilador para o aparelho de serviços. As ventoinhas de arrefecimento estão acessíveis depois de retirar a tampa superior do aparelho.

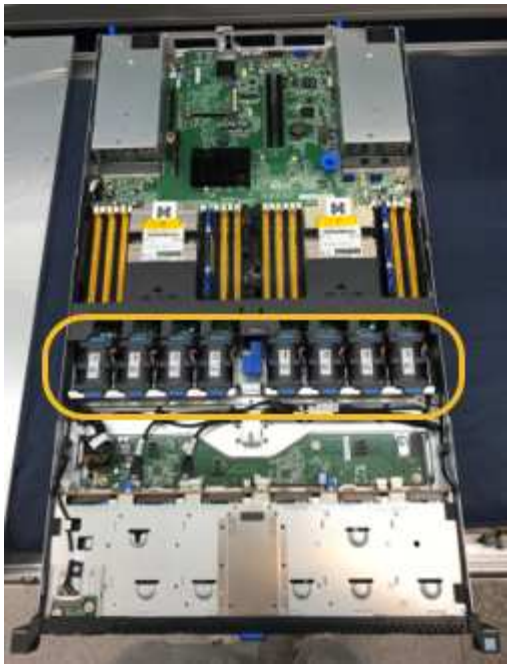
> Cada uma das duas unidades de fonte de alimentação também contém um ventilador. Esses ventiladores não estão incluídos neste procedimento.

Passos

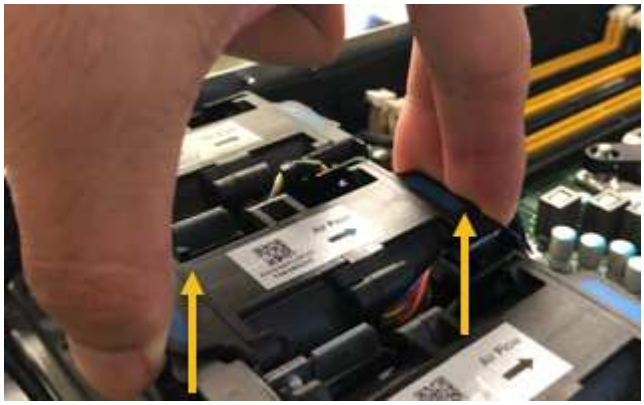
1. Quando o aparelho tiver sido colocado no modo de manutenção, desligue o aparelho.
   a. Faça login no nó da grade:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar 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. Desligue o aparelho de serviços
      `shutdown -h now`
2. Use um dos dois métodos para verificar se a energia do dispositivo de serviços está desligada:
   - O LED indicador de alimentação na parte frontal do aparelho está apagado.
   - A página Controle de energia da interface BMC indica que o aparelho está desligado.
3. Levante o trinco da tampa superior e retire a tampa do aparelho.
4. Localize o ventilador que falhou.

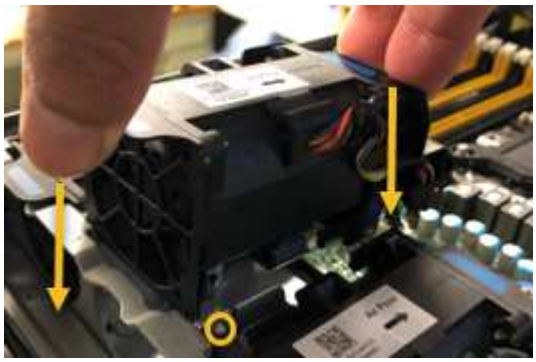


5. Levante a ventoinha avariada para fora do chassis.

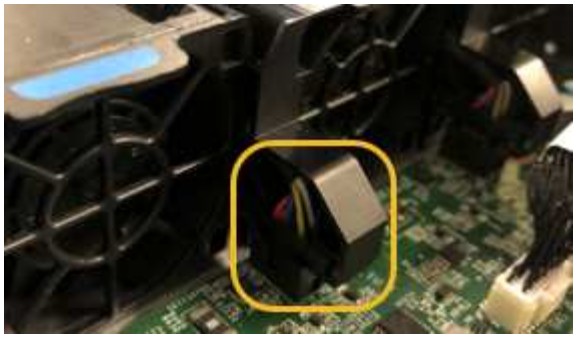


6. Faça deslizar a ventoinha de substituição para a ranhura aberta no chassis.

   Alinhe a extremidade da ventoinha com o pino-guia. O pino é circulado na fotografia.



7. Pressione firmemente o conetor da ventoinha na placa de circuito impresso.



8. Volte a colocar a tampa superior no aparelho e pressione o trinco para baixo para fixar a tampa no lugar.
9. Ligue o aparelho e monitorize os LEDs do controlador e os códigos de arranque.

   Use a interface BMC para monitorar o status de inicialização.

10. Confirme se o nó do dispositivo é exibido no Gerenciador de Grade e se nenhum alerta é exibido.

Substituir uma unidade no dispositivo de serviços

Os SSDs no dispositivo de serviços contêm o sistema operacional StorageGRID. Além disso, quando o dispositivo é configurado como um nó Admin, os SSDs também contêm logs de auditoria, métricas e tabelas de banco de dados. As unidades são espelhadas usando RAID1 para redundância. Se uma das unidades falhar, você deve substituí-la o mais rápido possível para garantir a redundância.

O que você vai precisar

- Você localizou fisicamente o dispositivo onde está substituindo a unidade no data center.

  "Localizar o controlador em um data center"

- Você verificou qual unidade falhou observando que seu LED esquerdo está piscando em âmbar.

  Se remover a unidade de trabalho, irá reduzir o nó do dispositivo. Consulte as informações sobre como visualizar indicadores de status para verificar a falha.

- Obteve a unidade de substituição.
- Você obteve proteção ESD adequada.

Passos

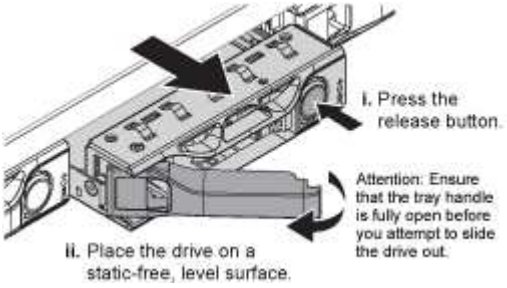
1. Verifique se o LED esquerdo da unidade está piscando em âmbar.

   Você também pode usar o Gerenciador de Grade para monitorar o status dos SSDs. Selecione **nós**. Em seguida, selecione **`Appliance Node` hardware**. Se uma unidade tiver falhado, o campo Storage RAID Mode (modo RAID de armazenamento) contém uma mensagem sobre qual unidade falhou.

2. Enrole a extremidade da correia da pulseira ESD à volta do pulso e fixe a extremidade do clipe a um solo metálico para evitar descargas estáticas.
3. Desembale a unidade de substituição e coloque-a numa superfície plana e livre de estática perto do aparelho.

   Salve todos os materiais de embalagem.

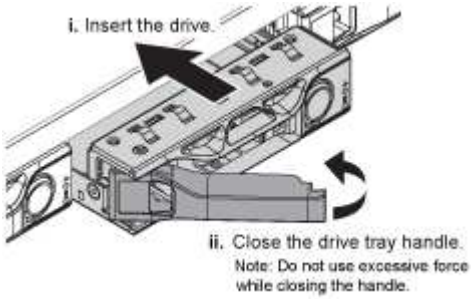
4. Pressione o botão de liberação na unidade com falha.



A alavanca nas molas de acionamento abre parcialmente e a unidade solta-se da ranhura.

5. Abra a alça, deslize a unidade para fora e coloque-a em uma superfície plana e livre de estática.
6. Pressione o botão de liberação na unidade de substituição antes de inseri-la no slot da unidade.

As molas do trinco abrem.



7. Insira a unidade de substituição na ranhura e, em seguida, feche a pega da unidade.

> Não utilize força excessiva ao fechar a pega.

Quando a unidade estiver totalmente inserida, você ouvirá um clique.

A unidade é reconstruída automaticamente com dados espelhados da unidade de trabalho. Você pode verificar o status da reconstrução usando o Gerenciador de Grade. Selecione **nós**. Em seguida, selecione **`Appliance Node` hardware**. O campo Storage RAID Mode (modo RAID de armazenamento) contém uma mensagem "reconstruindo" até que a unidade seja completamente reconstruída.

8. Entre em Contato com o suporte técnico sobre a substituição da unidade.

O suporte técnico fornecerá instruções para retornar a unidade com falha.

Alterar a configuração do link do dispositivo de serviços

Você pode alterar a configuração do link Ethernet do dispositivo de serviços. Pode alterar o modo de ligação de porta, o modo de ligação de rede e a velocidade de ligação.

O que você vai precisar

- Tem de colocar o aparelho no modo de manutenção. Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

  "Colocar um aparelho no modo de manutenção"

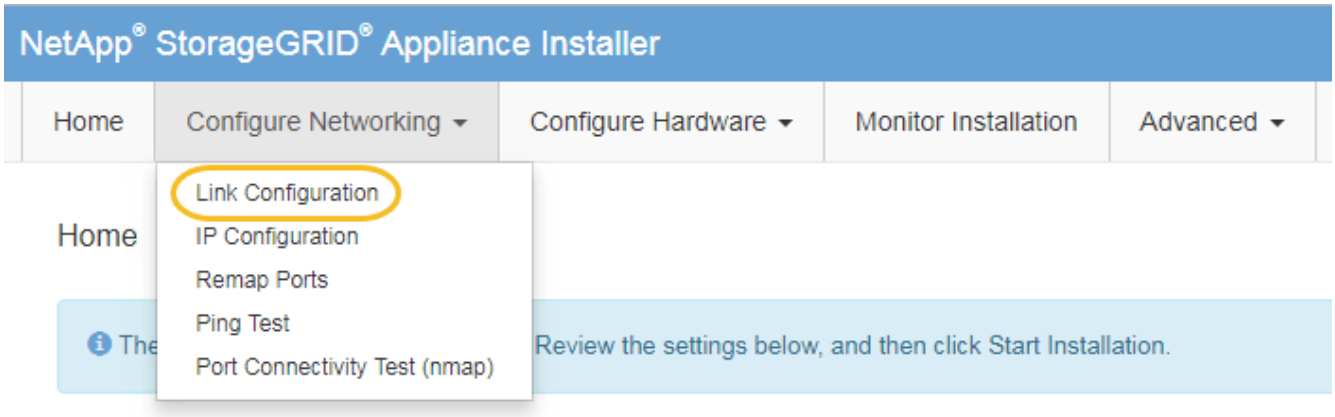
Sobre esta tarefa

As opções para alterar a configuração do link Ethernet do dispositivo de serviços incluem:

- Alterar o modo **Port bond** de fixo para agregado, ou de agregado para fixo
- Alteração do **modo de ligação de rede** de ative-Backup para LACP ou de LACP para ative-Backup
- Ativar ou desativar a marcação de VLAN ou alterar o valor de uma tag VLAN
- Alterar a velocidade da ligação

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Configurar rede Configuração de ligação**.



2. Faça as alterações desejadas na configuração do link.

   Para obter mais informações sobre as opções, consulte ""Configurando links de rede".

3. Quando estiver satisfeito com suas seleções, clique em **Salvar**.

   Poderá perder a ligação se tiver efetuado alterações à rede ou à ligação através da qual está ligado. Se você não estiver conetado novamente dentro de 1 minuto, insira novamente o URL do Instalador de appliance StorageGRID usando um dos outros endereços IP atribuídos ao appliance
   `https://services_appliance_IP:8443`

4. Faça as alterações necessárias nos endereços IP do aparelho.

   Se você fez alterações nas configurações de VLAN, a sub-rede do dispositivo pode ter sido alterada. Se você precisar alterar os endereços IP do dispositivo, siga as instruções para configurar endereços IP.

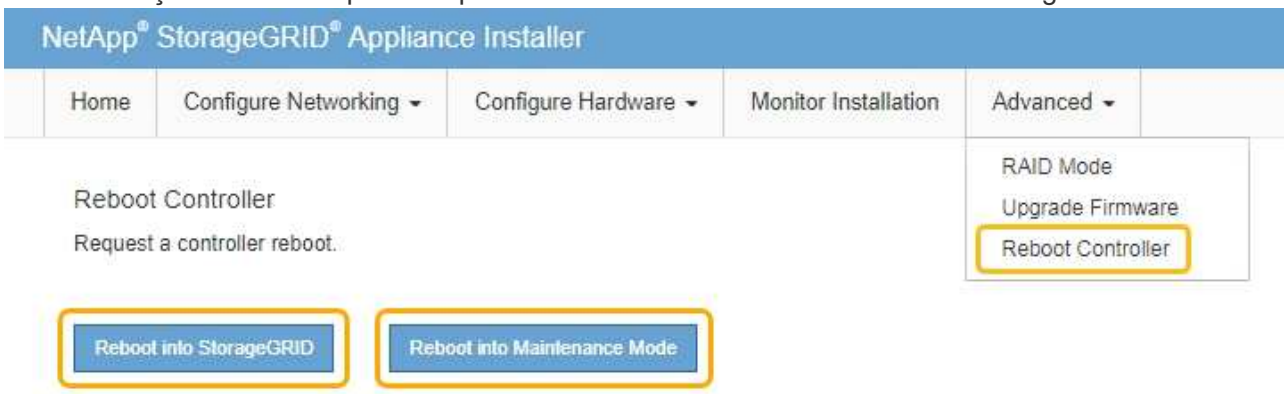
   "Configurando endereços IP do StorageGRID"

5. Selecione **Configurar rede Teste de ping** no menu.
6. Use a ferramenta Teste de ping para verificar a conetividade com endereços IP em qualquer rede que possa ter sido afetada pelas alterações de configuração de link feitas ao configurar o dispositivo.

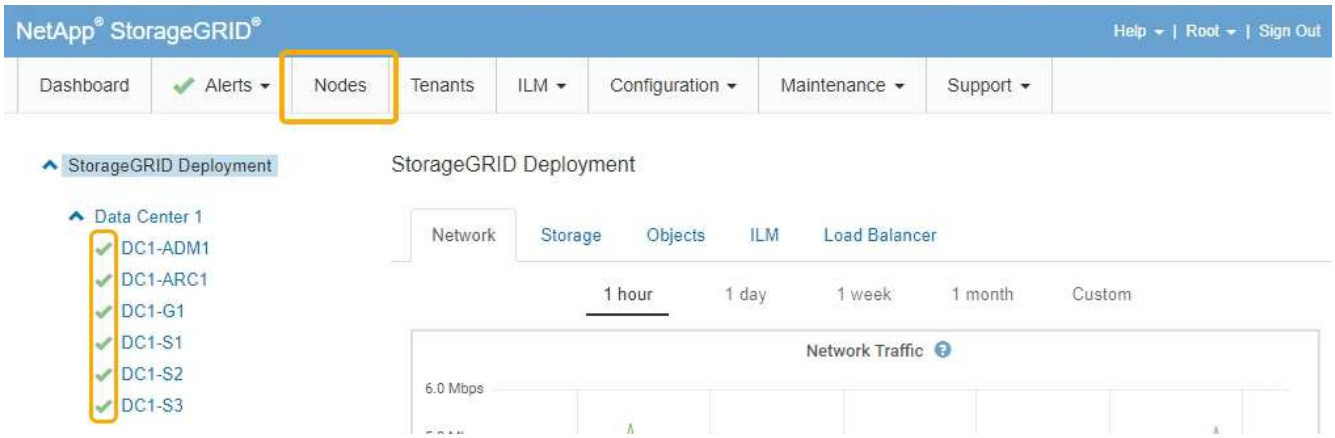
   Além de quaisquer outros testes que você escolher executar, confirme que você pode fazer ping no endereço IP da rede de Grade do nó Admin principal e no endereço IP da rede de Grade de pelo menos um outro nó. Se necessário, retorne às instruções para configurar links de rede e corrija quaisquer problemas.

7. Uma vez que você estiver satisfeito que as alterações de configuração do link estão funcionando, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



   Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Alterar a definição MTU

Você pode alterar a configuração MTU atribuída quando configurou endereços IP para o nó do dispositivo.

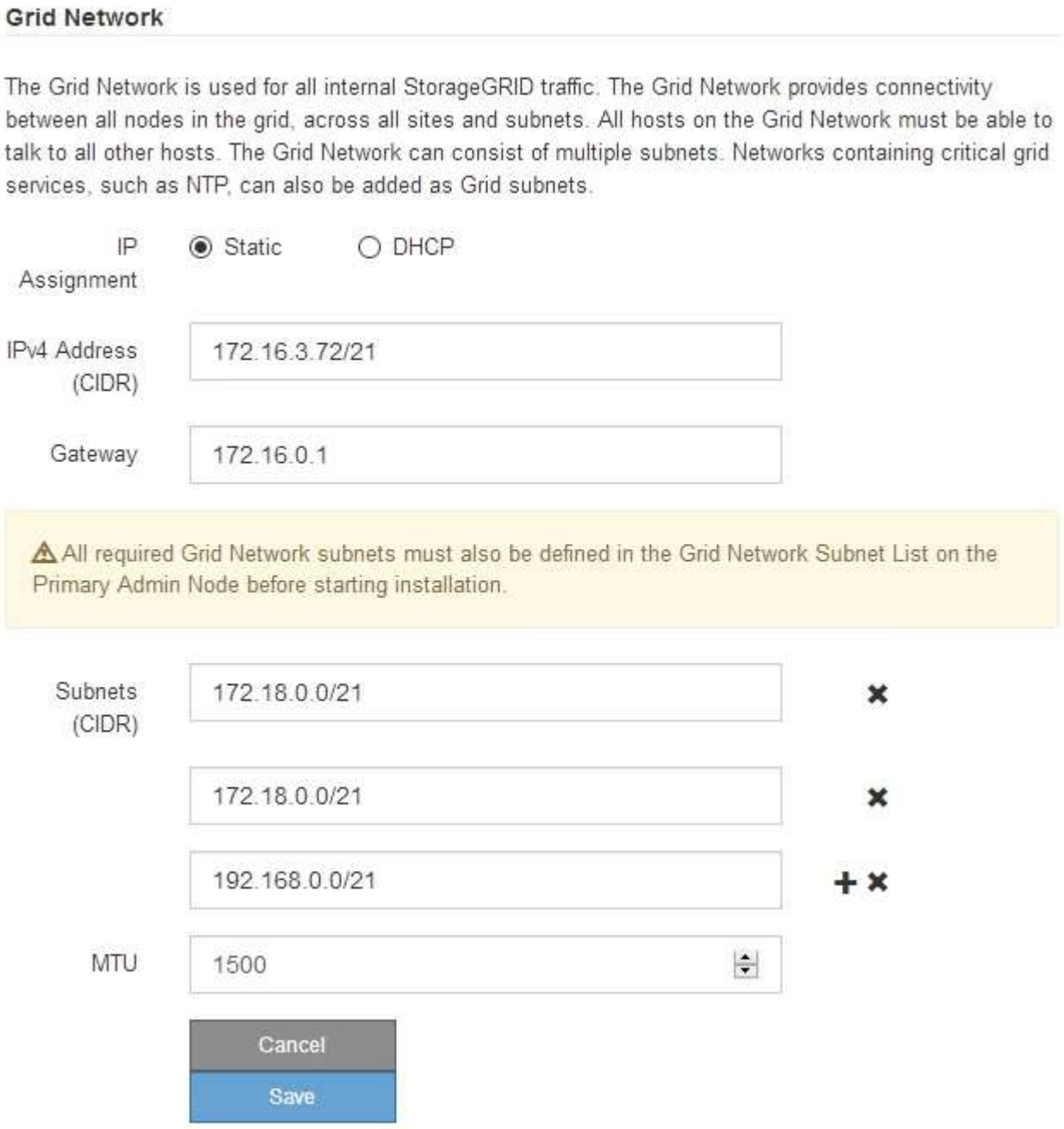
O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Passos

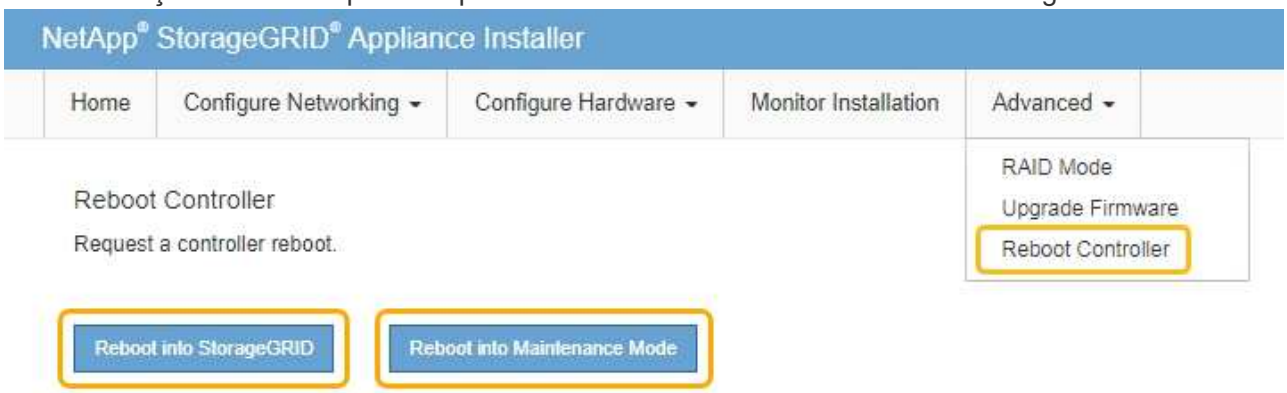
1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração IP**.
2. Faça as alterações desejadas nas configurações de MTU para rede de Grade, rede de Admin e rede de cliente.



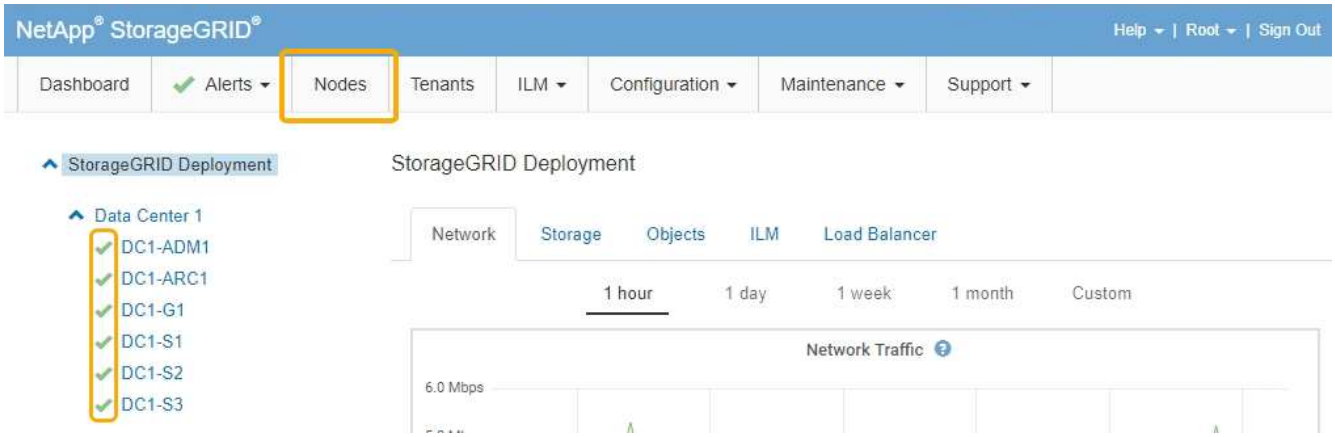
O valor MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conetado. Caso contrário, problemas de desempenho da rede ou perda de pacotes podem ocorrer.

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.

3. Quando estiver satisfeito com as definições, selecione **Guardar**.
4. Reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:
   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Administrar o StorageGRID"

Verificar a configuração do servidor DNS

Você pode verificar e alterar temporariamente os servidores DNS (sistema de nomes de domínio) que estão atualmente em uso por este nó de appliance.

O que você vai precisar

O aparelho foi colocado no modo de manutenção.

"Colocar um aparelho no modo de manutenção"

Sobre esta tarefa

Talvez seja necessário alterar as configurações do servidor DNS se um dispositivo criptografado não puder se conetar ao servidor de gerenciamento de chaves (KMS) ou ao cluster KMS porque o nome do host para o KMS foi especificado como um nome de domínio em vez de um endereço IP. Quaisquer alterações efetuadas nas definições de DNS do dispositivo são temporárias e perdem-se quando sai do modo de manutenção. Para tornar essas alterações permanentes, especifique os servidores DNS no Gerenciador de Grade (**Manutenção rede servidores DNS**).

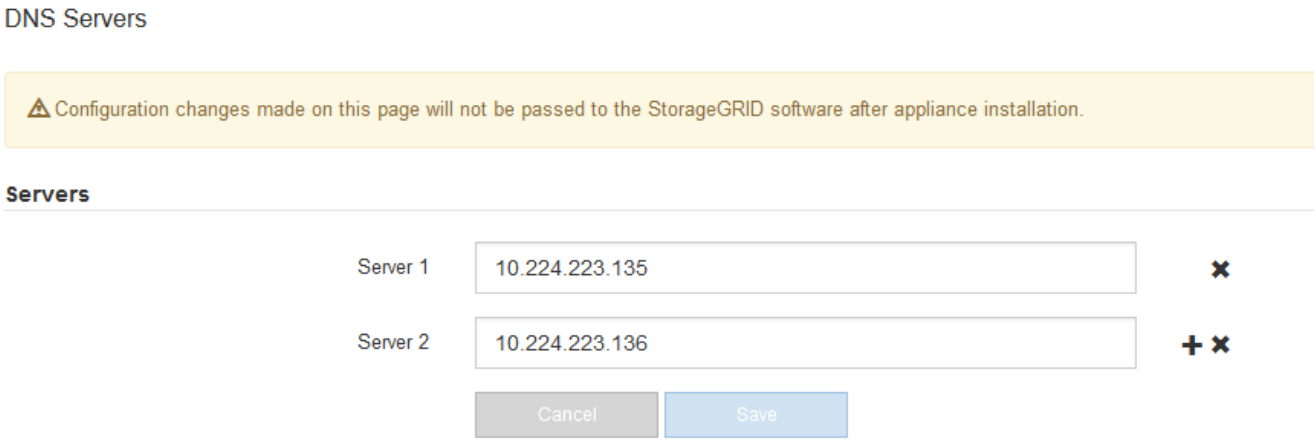
- As alterações temporárias na configuração DNS são necessárias apenas para dispositivos encriptados por nó onde o servidor KMS é definido utilizando um nome de domínio totalmente qualificado, em vez de um endereço IP, para o nome de anfitrião.
- Quando um dispositivo criptografado por nó se coneta a um KMS usando um nome de domínio, ele deve se conetar a um dos servidores DNS definidos para a grade. Um desses servidores DNS converte o nome de domínio em um endereço IP.
- Se o nó não conseguir alcançar um servidor DNS para a grade, ou se você alterou as configurações de DNS em toda a grade quando um nó de dispositivo criptografado por nó estava off-line, o nó não consegue se conetar ao KMS. Os dados criptografados no dispositivo não podem ser descriptografados até que o problema de DNS seja resolvido.

Para resolver um problema de DNS que impede a ligação KMS, especifique o endereço IP de um ou mais servidores DNS no Instalador de aplicações StorageGRID. Essas configurações de DNS temporárias permitem que o dispositivo se conete ao KMS e descriptografar dados no nó.

Por exemplo, se o servidor DNS para a grade mudar enquanto um nó criptografado estava off-line, o nó não será capaz de alcançar o KMS quando ele voltar on-line, uma vez que ainda está usando os valores DNS anteriores. A introdução do novo endereço IP do servidor DNS no Instalador de aplicações StorageGRID permite que uma ligação KMS temporária desencripte os dados do nó.

Passos

1. No Instalador do StorageGRID Appliance, selecione **Configurar rede Configuração de DNS**.
2. Verifique se os servidores DNS especificados estão corretos.



3. Se necessário, altere os servidores DNS.

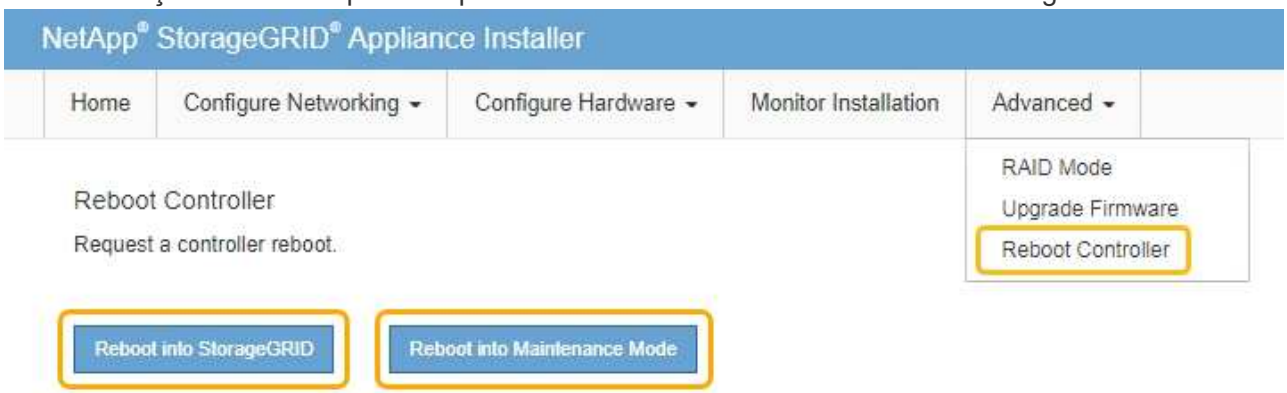
> As alterações efetuadas nas definições de DNS são temporárias e perdem-se quando sai do modo de manutenção.

4. Quando estiver satisfeito com as definições de DNS temporárias, selecione **Guardar**.

   O nó usa as configurações do servidor DNS especificadas nesta página para se reconetar ao KMS, permitindo que os dados no nó sejam descriptografados.

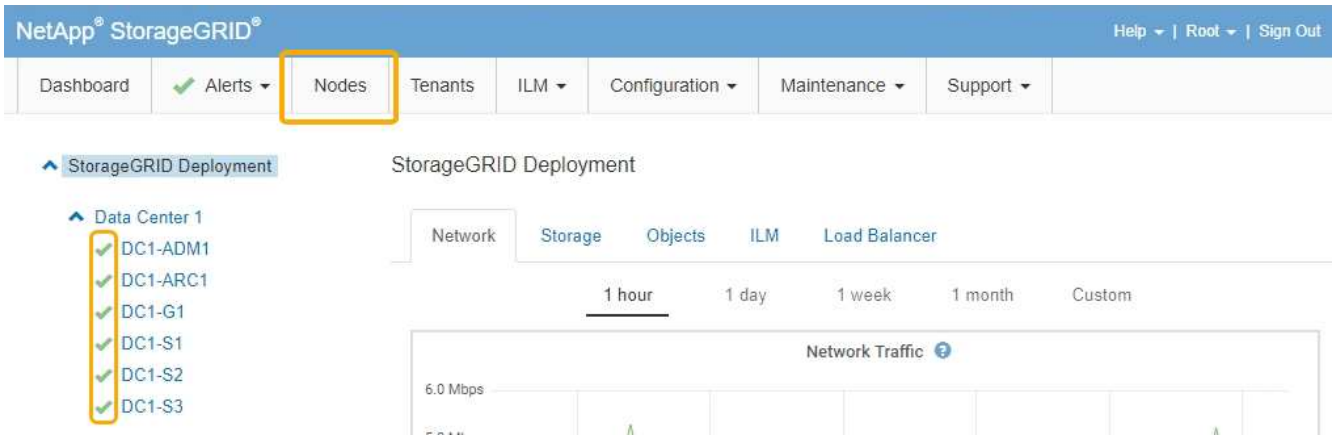
5. Depois que os dados do nó forem descriptografados, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Quando o nó reinicializa e realegra a grade, ele usa os servidores DNS de todo o sistema listados no Gerenciador de Grade. Depois de reingressar na grade, o dispositivo não usará mais os servidores DNS temporários especificados no Instalador de dispositivos StorageGRID enquanto o dispositivo estava no modo de manutenção.

Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔ para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Monitorização da encriptação do nó no modo de manutenção

Se você ativou a criptografia de nó para o dispositivo durante a instalação, poderá monitorar o status de criptografia de nó de cada nó do dispositivo, incluindo os detalhes do estado de criptografia de nó e do servidor de gerenciamento de chaves (KMS).

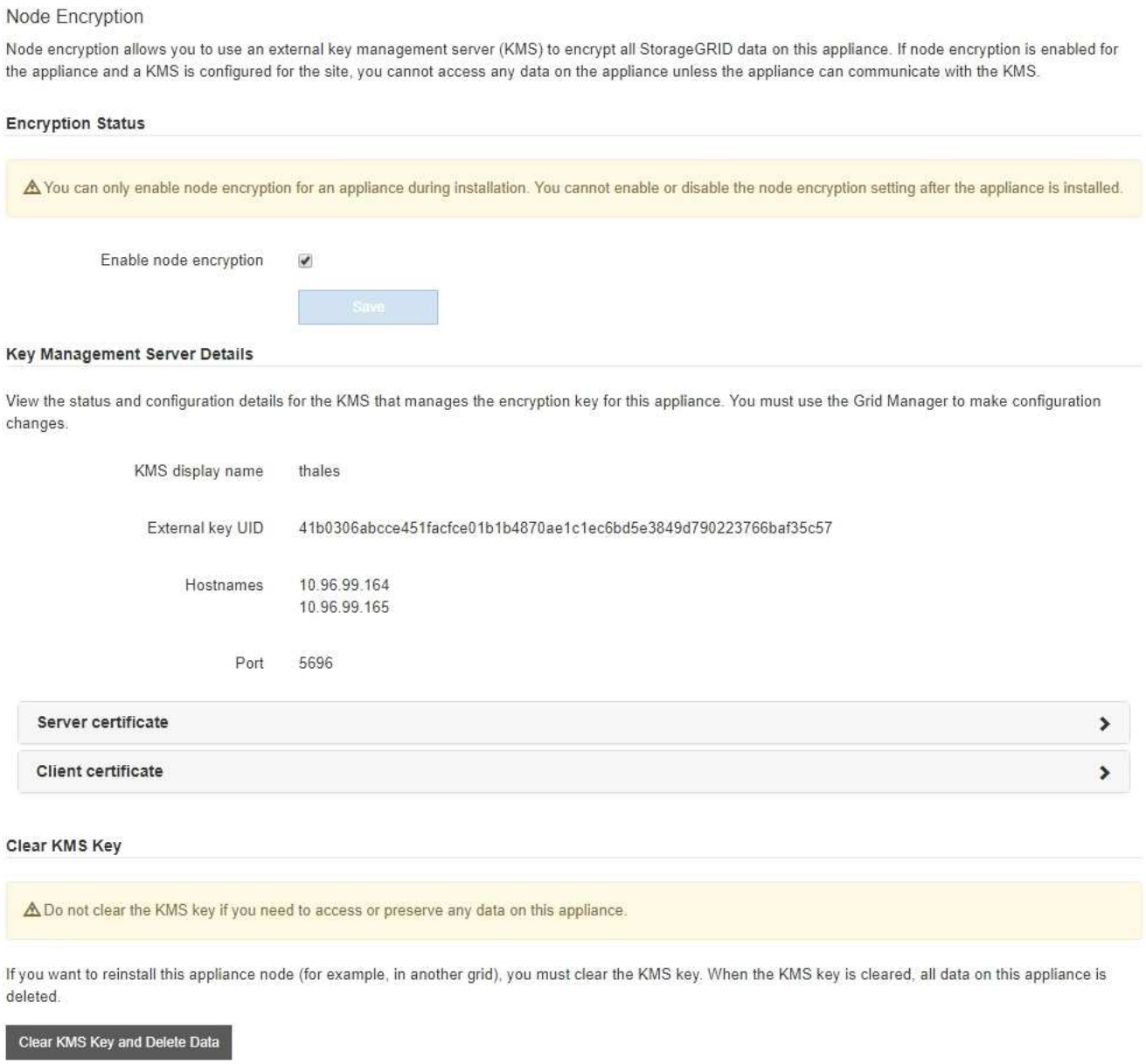
O que você vai precisar

- A criptografia do nó deve ter sido ativada para o dispositivo durante a instalação. Não é possível ativar a criptografia de nó depois que o dispositivo estiver instalado.
- O aparelho foi colocado no modo de manutenção.

  "Colocar um aparelho no modo de manutenção"

Passos

1. No Instalador de dispositivos StorageGRID, selecione **Configurar hardware criptografia de nó**.



A página criptografia do nó inclui estas três seções:

- O estado de encriptação mostra se a encriptação do nó está ativada ou desativada para o dispositivo.
- Detalhes do servidor de gerenciamento de chaves mostra informações sobre o KMS sendo usado para criptografar o dispositivo. Você pode expandir as seções de certificado de servidor e cliente para exibir detalhes e status do certificado.
  - Para resolver problemas com os próprios certificados, como a renovação de certificados expirados, consulte as informações sobre o KMS nas instruções de administração do StorageGRID.
  - Se houver problemas inesperados ao se conetar aos hosts KMS, verifique se os servidores DNS (sistema de nomes de domínio) estão corretos e se a rede do appliance está configurada corretamente.

    "Verificar a configuração do servidor DNS"

  - Se você não conseguir resolver os problemas do certificado, entre em Contato com o suporte técnico.

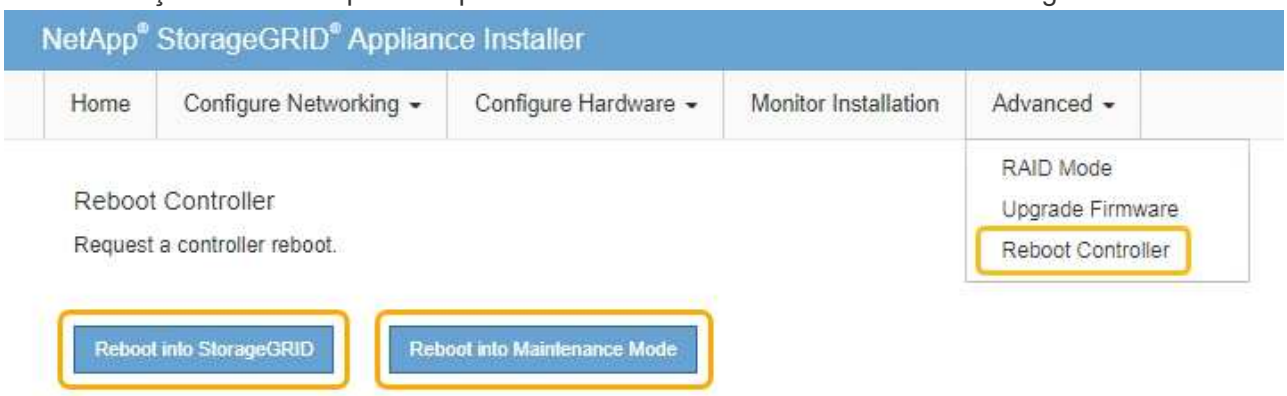
- Limpar chave KMS desativa a criptografia de nó para o dispositivo, remove a associação entre o dispositivo e o servidor de gerenciamento de chaves que foi configurado para o site StorageGRID e exclui todos os dados do dispositivo. Tem de limpar a chave KMS antes de poder instalar o aparelho noutro sistema StorageGRID.

  "Limpando a configuração do servidor de gerenciamento de chaves"

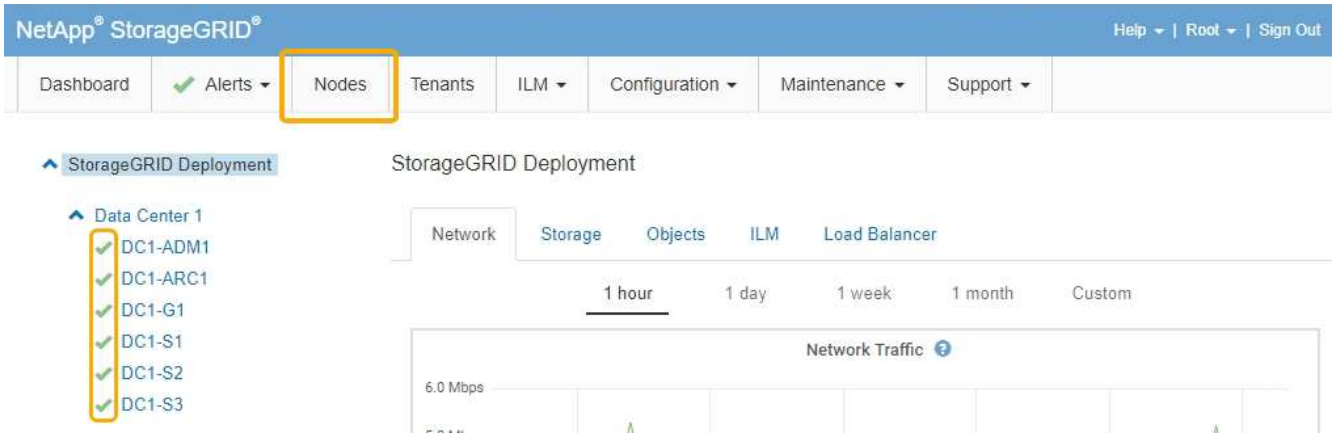
  Limpar a configuração do KMS exclui os dados do dispositivo, tornando-os permanentemente inacessíveis. Estes dados não são recuperáveis.

2. Quando terminar de verificar o estado da encriptação do nó, reinicie o nó. No Instalador do StorageGRID Appliance, selecione **Avançado controlador de reinicialização** e, em seguida, selecione uma destas opções:

   - Selecione **Reboot into StorageGRID** para reiniciar o controlador com o nó rejuntando a grade. Selecione esta opção se terminar de trabalhar no modo de manutenção e estiver pronto para retornar o nó à operação normal.
   - Selecione **Reboot into Maintenance Mode** (Reiniciar no modo de manutenção) para reiniciar o controlador com o nó restante no modo de manutenção. Selecione esta opção se houver operações de manutenção adicionais que você precisa executar no nó antes de voltar a unir a grade.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Informações relacionadas

"Administrar o StorageGRID"

Limpando a configuração do servidor de gerenciamento de chaves

Limpar a configuração do servidor de gerenciamento de chaves (KMS) desativa a criptografia de nó no seu dispositivo. Depois de limpar a configuração do KMS, os dados do seu aparelho são excluídos permanentemente e não são mais acessíveis. Estes dados não são recuperáveis.

O que você vai precisar

Se você precisar preservar dados no dispositivo, você deve executar um procedimento de desativação de nós antes de limpar a configuração do KMS.

> Quando o KMS é eliminado, os dados no aparelho serão eliminados permanentemente e deixarão de estar acessíveis. Estes dados não são recuperáveis.

Desative o nó para mover quaisquer dados que ele contenha para outros nós no StorageGRID. Consulte as instruções de recuperação e manutenção para a desativação do nó da grade.

Sobre esta tarefa

A limpeza da configuração do KMS do appliance desativa a criptografia do nó, removendo a associação entre o nó do appliance e a configuração do KMS para o site do StorageGRID. Os dados no dispositivo são então excluídos e o dispositivo é deixado em um estado de pré-instalação. Este processo não pode ser revertido.

Você deve limpar a configuração do KMS:

- Antes de instalar o aparelho em outro sistema StorageGRID, isso não usa um KMS ou que usa um KMS diferente.

  > Não limpe a configuração do KMS se você planeja reinstalar um nó de dispositivo em um sistema StorageGRID que usa a mesma chave KMS.

- Antes de poder recuperar e reinstalar um nó onde a configuração do KMS foi perdida e a chave KMS não é recuperável.
- Antes de devolver qualquer aparelho que estava anteriormente em uso em seu site.
- Após a desativação de um dispositivo que tinha a criptografia de nó ativada.

> Desative o dispositivo antes de limpar o KMS para mover seus dados para outros nós em seu sistema StorageGRID. Limpar o KMS antes de desativar o aparelho resultará em perda de dados e pode tornar o aparelho inoperável.

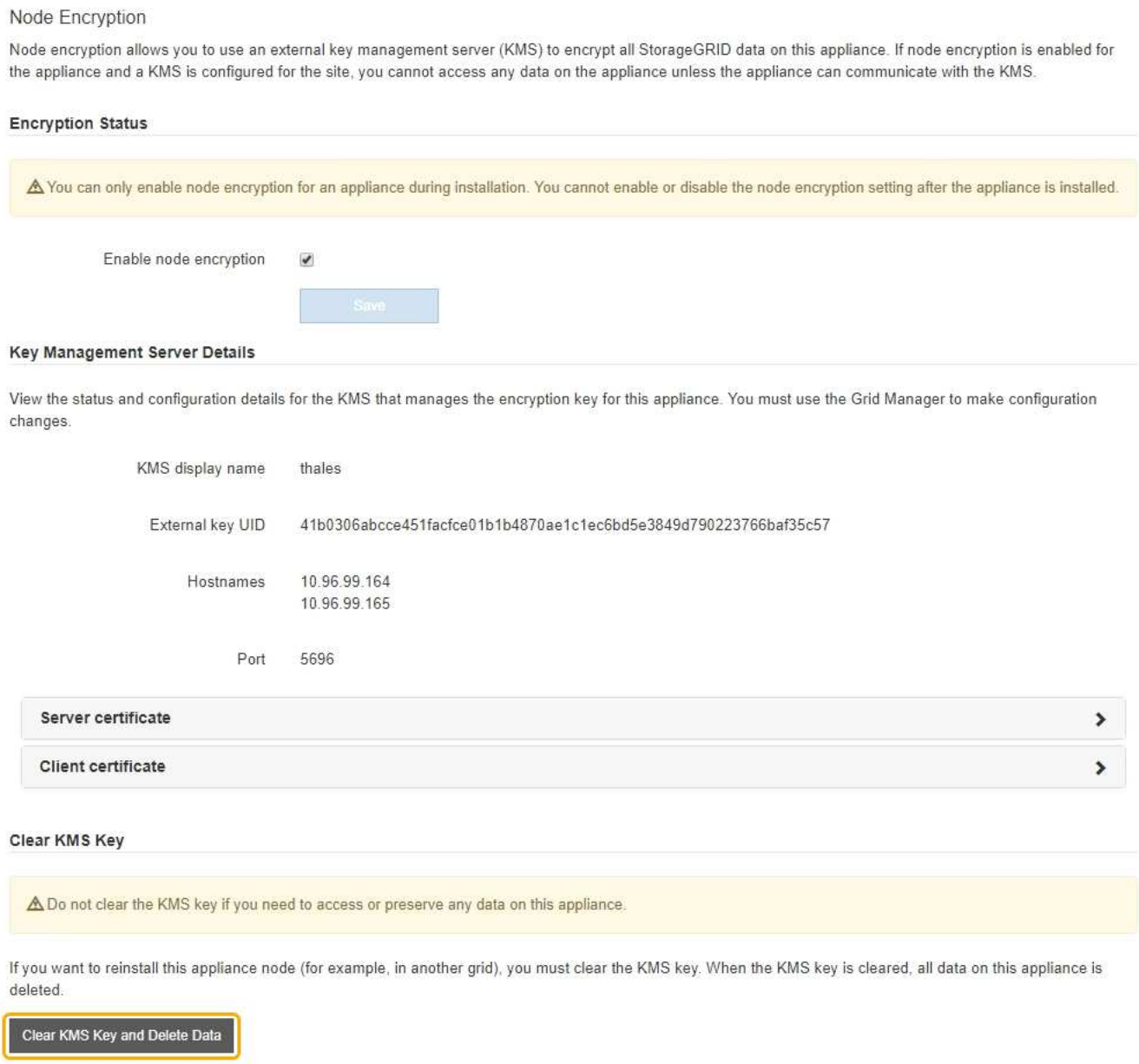
Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
   `https://Controller_IP:8443`

   `Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

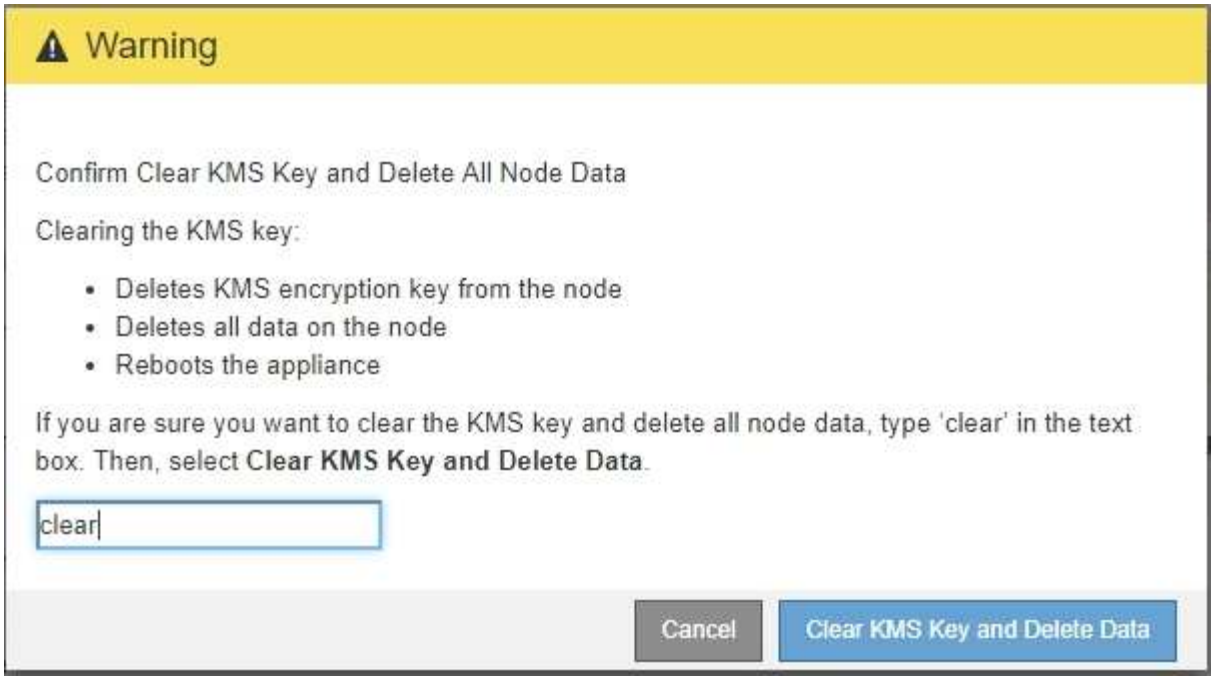
   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Selecione **Configure hardware Node Encryption**.



> Se a configuração do KMS for limpa, os dados no dispositivo serão excluídos permanentemente. Estes dados não são recuperáveis.

3. Na parte inferior da janela, selecione **Limpar chave KMS e Excluir dados**.
4. Se tiver certeza de que deseja limpar a configuração do KMS, digite `clear` e selecione **Limpar chave KMS e Excluir dados**.



A chave de criptografia KMS e todos os dados são excluídos do nó e o dispositivo é reinicializado. Isso pode levar até 20 minutos.

5. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo. E
`https://Controller_IP:8443`

`Controller_IP` É o endereço IP do controlador de computação (não o controlador de storage) em qualquer uma das três redes StorageGRID.

A página inicial do instalador do dispositivo StorageGRID é exibida.

6. Selecione **Configure hardware Node Encryption**.
7. Verifique se a criptografia do nó está desativada e se as informações de chave e certificado em **Key Management Server Details** e **Clear KMS Key e Delete Data** control são removidas da janela.

A criptografia do nó não pode ser reativada no dispositivo até que seja reinstalada em uma grade.

Depois de terminar

Depois de o aparelho reiniciar e verificar se o KMS foi limpo e se o aparelho está num estado de pré-instalação, pode remover fisicamente o aparelho do sistema StorageGRID. Consulte as instruções de recuperação e manutenção para obter informações sobre como preparar um aparelho para reinstalação.

Informações relacionadas

"Administrar o StorageGRID"

"Manter recuperar"

Configurar e gerenciar

Administrar o StorageGRID

Saiba como configurar o sistema StorageGRID.

- "Administrar um sistema StorageGRID"
- "Controlar o acesso do administrador ao StorageGRID"
- "Configurando servidores de gerenciamento de chaves"
- "Gerenciamento de locatários"
- "Configurando conexões de cliente S3 e Swift"
- "Gerenciamento de redes e conexões StorageGRID"
- "Configurando o AutoSupport"
- "Gerenciando nós de storage"
- "Gerenciando nós de administração"
- "Gerenciando nós de arquivamento"
- "Migração de dados para o StorageGRID"

Administrar um sistema StorageGRID

Use estas instruções para configurar e administrar um sistema StorageGRID.

Essas instruções descrevem como usar o Gerenciador de Grade para configurar grupos e usuários, criar contas de locatário para permitir que aplicativos clientes S3 e Swift armazenem e recuperem objetos, configurem e gerenciem redes StorageGRID, configurem AutoSupport, gerenciem configurações de nó e muito mais.

> As instruções para gerenciar objetos com regras e políticas de gerenciamento de ciclo de vida das informações (ILM) foram movidas para "Gerenciar objetos com ILM"o .

Estas instruções destinam-se ao pessoal técnico que irá configurar, administrar e dar suporte a um sistema StorageGRID depois de instalado.

O que você vai precisar

- 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.

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87

Navegador da Web	Versão mínima suportada
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Iniciar sessão no Grid Manager

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.

O que você vai precisar

- Tem de ter as suas credenciais de início de sessão.
- Você deve ter o URL para o Gerenciador de Grade.
- Você deve estar usando um navegador da Web compatível.
- Os cookies devem estar ativados no seu navegador.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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, os nós de administração não são exatamente os mesmos:

- Reconhecimentos de alarmes (sistema legado) feitos em um nó Admin não são copiados para outros nós Admin. Por esse motivo, as informações exibidas para alarmes podem não ter a mesma aparência em cada nó de administração.
- Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

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 o principal preferido 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.

Passos

1. Inicie um navegador da Web compatível.
2. Na barra de endereços do navegador, insira o URL do Gerenciador de Grade:

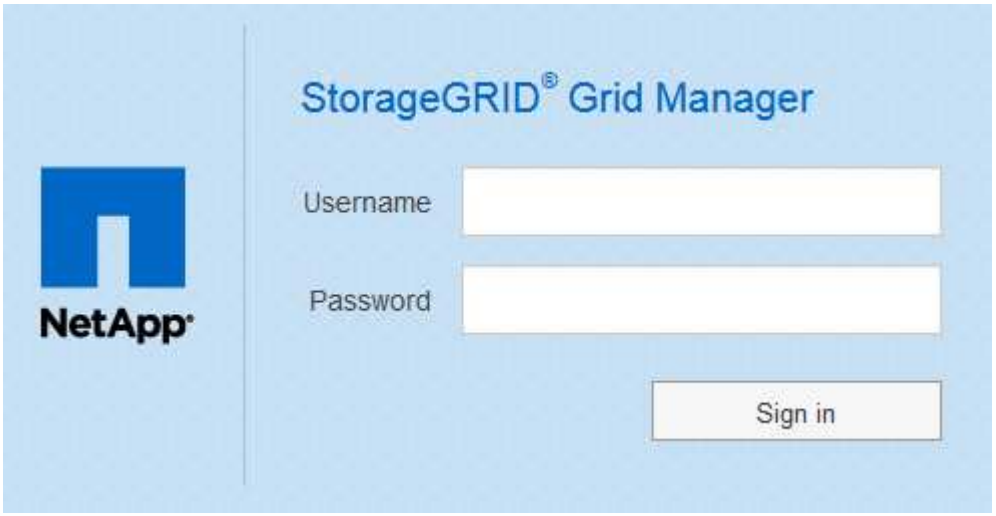
`https://FQDN_or_Admin_Node_IP/`

`_FQDN_or_Admin_Node_IP_`Onde está um nome de domínio totalmente qualificado ou o endereço IP de um nó Admin ou o endereço IP virtual de um grupo de HA de nós Admin.

Se você precisar acessar o Gerenciador de Grade em uma porta diferente da porta padrão para HTTPS (443), digite o seguinte, onde *FQDN_or_Admin_Node_IP* é um nome de domínio totalmente qualificado ou endereço IP, e a porta é o número da porta:

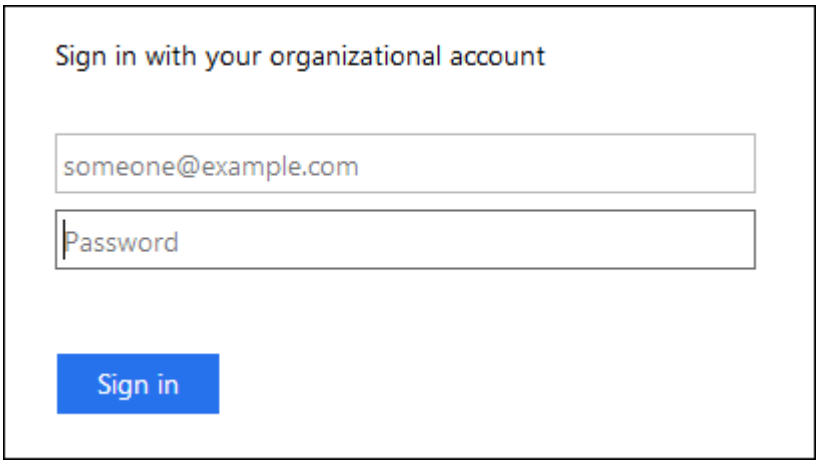
`https://FQDN_or_Admin_Node_IP:port/`

3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Entre no Gerenciador de Grade:
   - Se o logon único (SSO) não estiver sendo usado para seu sistema StorageGRID:
     i. Insira seu nome de usuário e senha para o Gerenciador de Grade.
     ii. Clique em **entrar**.



   - Se o SSO estiver ativado para o seu sistema StorageGRID e esta é a primeira vez que você acessou o URL neste navegador:
     i. Clique em **entrar**. Você pode deixar o campo ID da conta em branco.

ii. Insira suas credenciais SSO padrão na página de login SSO da sua organização. Por exemplo:

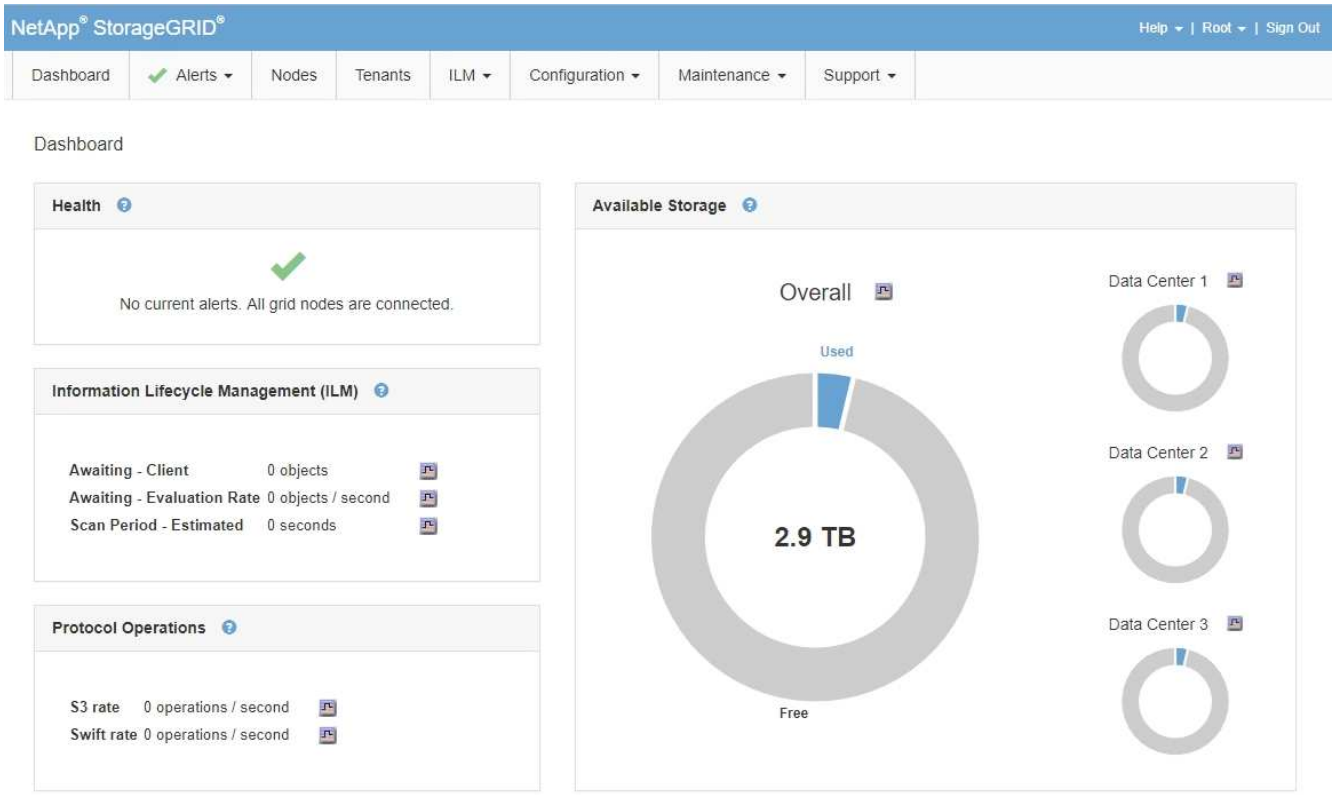


- Se o SSO estiver ativado para o seu sistema StorageGRID e você tiver acessado anteriormente o Gerenciador de Grade ou uma conta de locatário:

  i. Faça um dos seguintes procedimentos:

  - Digite **0** (o ID da conta do Gerenciador de Grade) e clique em **entrar**.
  - Selecione **Gerenciador de Grade** se aparecer na lista de contas recentes e clique em **entrar**.

ii. 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 de Controle. Para saber quais informações são fornecidas, consulte ""visualizando o Painel"" nas instruções para monitoramento e solução de problemas do StorageGRID.



5. Se você quiser entrar em outro nó de administração:

Opção	Passos
SSO não ativado	a. 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. b. Insira seu nome de usuário e senha para o Gerenciador de Grade. c. Clique em **entrar**.

Opção	Passos
SSO ativado	Na barra de endereços do navegador, insira o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração. Se você tiver feito login em um nó de administrador, poderá acessar outros nós de administrador sem ter que fazer login novamente. No entanto, se sua sessão SSO expirar, você será solicitado a fornecer suas credenciais novamente. **Observação:** SSO não está disponível na porta do Gerenciador de Grade restrito. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Informações relacionadas

"Requisitos do navegador da Web"

"Controlar o acesso através de firewalls"

"Configurando certificados de servidor"

"Configurando logon único"

"Gerenciando grupos de administradores"

"Gerenciamento de grupos de alta disponibilidade"

"Use uma conta de locatário"

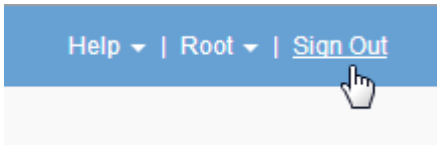
"Monitorizar Resolução de problemas"

Sair do Gerenciador de Grade

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. Localize o link **Sair** no canto superior direito da interface do usuário.



2. Clique em **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 do Locatário, você também deverá sair da conta do locatário para sair do SSO.

Informações relacionadas

"Configurando logon único"

"Use uma conta de locatário"

Alterar a sua palavra-passe

Se você é um usuário local do Gerenciador de Grade, você pode alterar sua própria senha.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

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*** **> alterar senha**.
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. Clique em **Salvar**.

Alterando a senha de provisionamento

Use este procedimento para alterar a senha de provisionamento do StorageGRID. A frase-passe é necessária para procedimentos de recuperação, expansão e manutenção. A frase-passe também é necessária para fazer o download dos backups do pacote de recuperação que incluem as informações de topologia de grade e as chaves de criptografia para o sistema StorageGRID.

O que você vai precisar

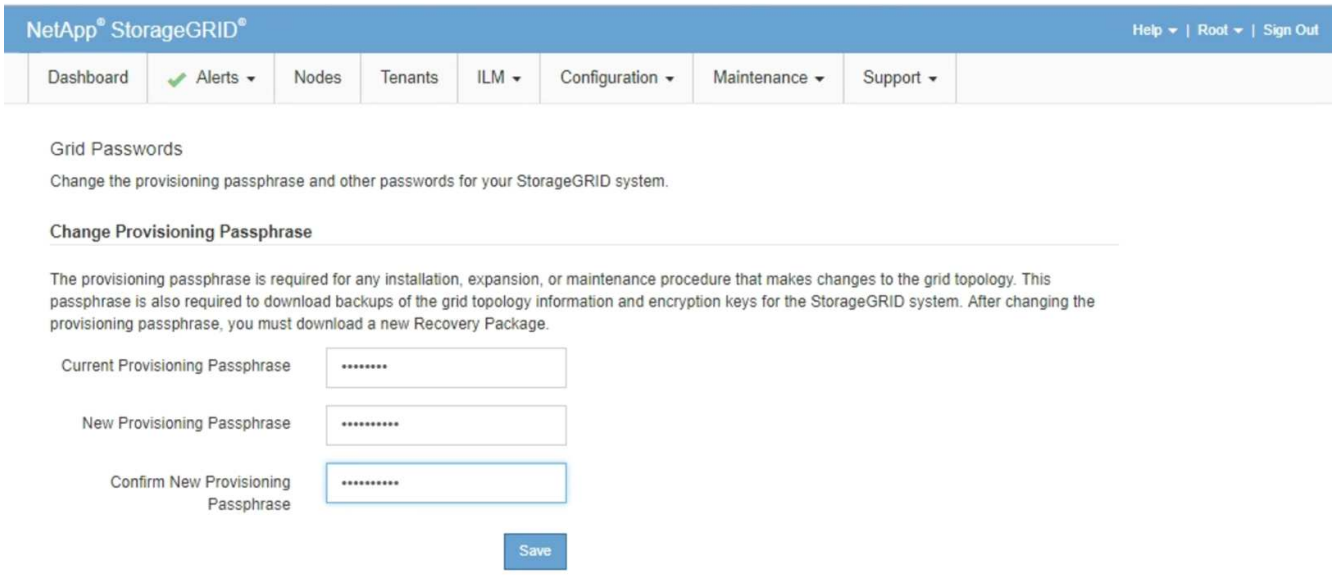
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento atual.

Sobre esta tarefa

A frase-passe de aprovisionamento é necessária para muitos procedimentos de instalação e manutenção e para transferir o pacote de recuperação. 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 **Configuração** > **Controle de Acesso** > **senhas de Grade**.

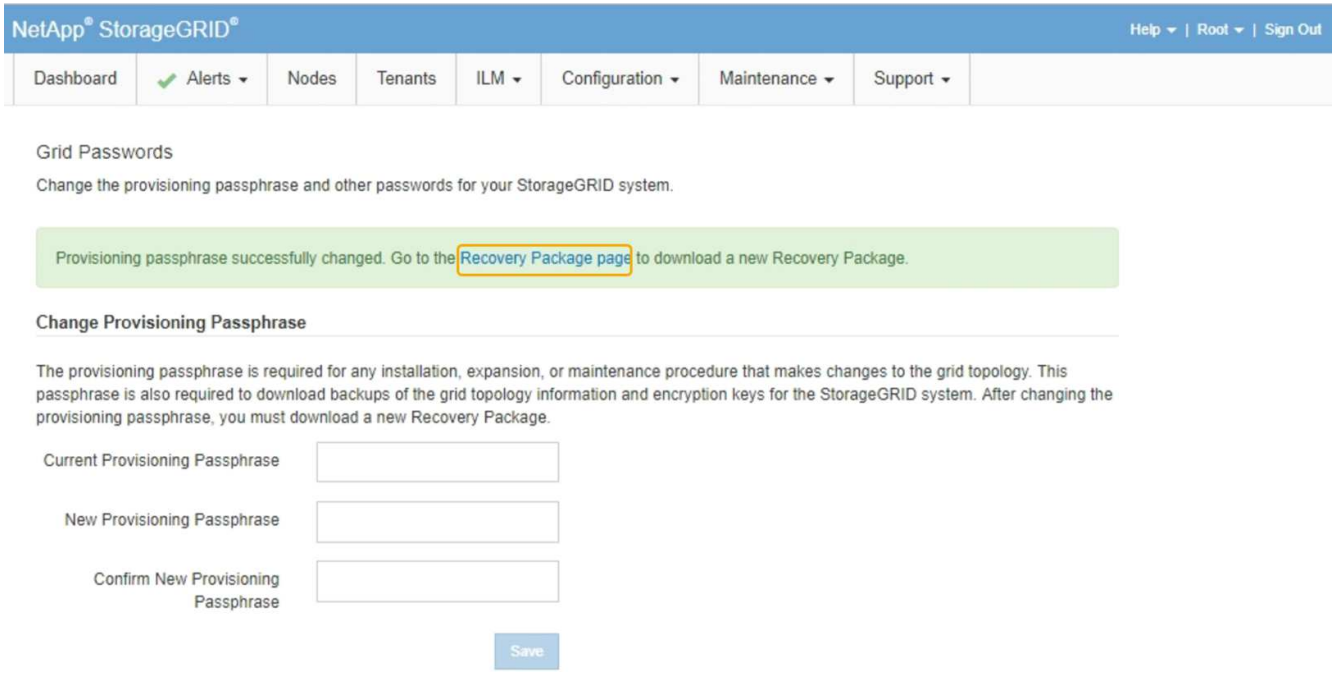


2. Introduza a sua frase-passe de aprovisionamento atual.
3. Introduza a nova frase-passe.a frase-passe tem de conter, no mínimo, 8 e não mais de 32 carateres. As senhas são sensíveis a maiúsculas e minúsculas.

> Armazene a nova senha de provisionamento em um local seguro. É necessário para procedimentos de instalação, expansão e manutenção.

4. Digite novamente a nova senha e clique em **Salvar**.

   O sistema exibe um banner verde de sucesso quando a alteração da senha de provisionamento estiver concluída. A mudança deve levar menos de um minuto.



5. Selecione o link **Pacote de recuperação** dentro do banner de sucesso.
6. Faça o download do novo Pacote de recuperação do Gerenciador de Grade. Selecione **Maintenance** > **Recovery Package** e insira a nova senha de provisionamento.

> 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.

Alterar o tempo limite da sessão do navegador

Você pode controlar se os usuários do Grid Manager e do Tenant Manager estão desconetados se estiverem inativos por mais de um determinado período de tempo.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

O tempo limite de inatividade da GUI é predefinido para 900 segundos (15 minutos). Se a sessão do navegador de um usuário não estiver ativa por esse período de tempo, a sessão expirará.

Conforme necessário, você pode aumentar ou diminuir o período de tempo limite definindo a opção de exibição tempo limite de inatividade da GUI.

Se o logon único (SSO) estiver ativado e a sessão do navegador do usuário expirar, o sistema se comportará como se o usuário clicasse em **Sair** manualmente. O usuário deve reinserir suas credenciais SSO para acessar o StorageGRID novamente.

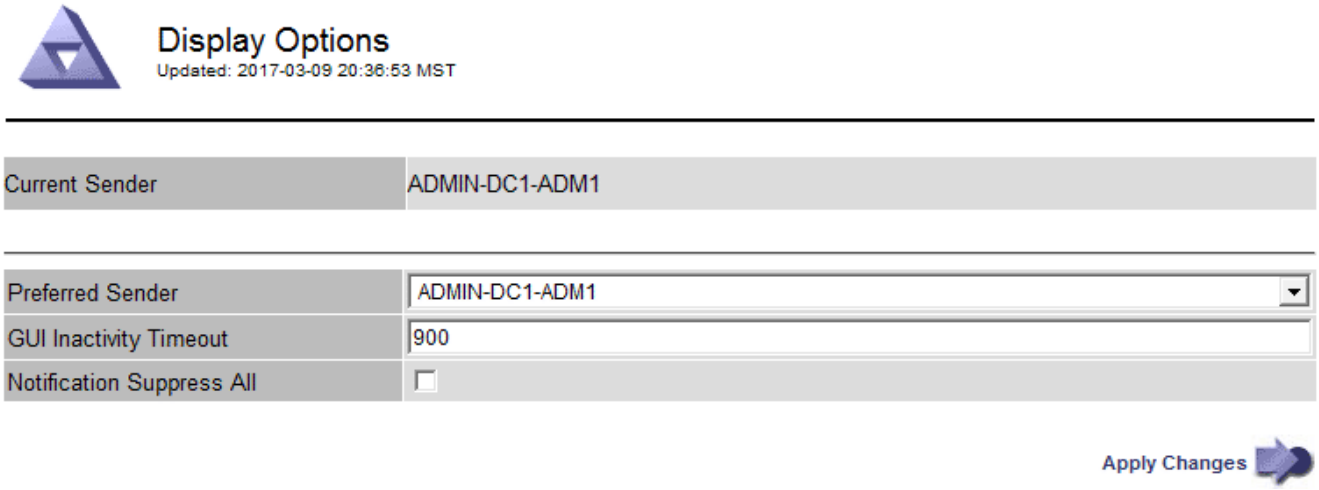
O tempo limite da sessão do usuário também pode ser controlado pelo seguinte:

- Um temporizador StorageGRID separado, não configurável, incluído para a segurança do sistema. Por padrão, 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 automaticamente desconetado, mesmo que o valor do tempo limite de inatividade da GUI 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 SSO esteja habilitado para o StorageGRID.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**.
2. Para **tempo limite de inatividade da GUI**, insira um período de tempo limite de 60 segundos ou mais.

   Defina este campo como 0 se não pretender utilizar esta funcionalidade. Os usuários são desconetados 16 horas após o início de sessão, quando seus tokens de autenticação expiram.



3. Clique em **aplicar alterações**.

   A nova configuração não afeta os usuários conetados atualmente. Os usuários devem entrar novamente ou atualizar seus navegadores para que a nova configuração de tempo limite entre em vigor.

Informações relacionadas

"Como o single sign-on funciona"

"Use uma conta de locatário"

Visualizar informações de 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Se houver um problema com a licença de software para este sistema StorageGRID, o painel Saúde no Painel inclui um ícone de Status da Licença e um link **Licença**. O número indica quantos problemas relacionados à licença existem.

Passo

Para visualizar a licença, execute um dos seguintes procedimentos:

- No painel Saúde do Painel, clique no ícone Status da Licença ou no link **Licença**. Este link aparece somente se houver um problema com a licença.
- Selecione **Manutenção** > **sistema** > **Licença**.

A Página de Licença é exibida e fornece as seguintes informações somente de leitura sobre a licença atual:

- ID do sistema StorageGRID, que é o número de identificação exclusivo para esta instalação do StorageGRID
- Número de série da licença
- Capacidade de armazenamento licenciada da rede
- Data de término da licença de software
- Data de término do contrato de serviço de suporte
- Conteúdo do arquivo de texto da licença

> Para as licenças emitidas antes do StorageGRID 10,3, a capacidade de armazenamento licenciada não está incluída no ficheiro de licença e é apresentada uma mensagem "consulte o Contrato de licença" em vez de um valor.

Atualizando 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.

O que você vai precisar

- Você deve ter um novo arquivo de licença para aplicar ao seu sistema StorageGRID.

- Você deve ter permissões de acesso específicas.
- Você deve ter a senha de provisionamento.

Passos

1. Selecione **Manutenção** > **sistema** > **Licença**.
2. Introduza a frase-passe de aprovisionamento do seu sistema StorageGRID na caixa de texto **frase-passe de aprovisionamento**.
3. Clique em **Procurar**.
4. Na caixa de diálogo abrir, localize e selecione o novo arquivo de licença (`.txt`) e clique em **abrir**.

   O novo ficheiro de licença é validado e apresentado.

5. Clique em **Salvar**.

Usando 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.

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.

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, consulte as informações sobre como usar contas de locatário.
- `/private`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas. Essas APIs são destinadas apenas para uso interno e não são documentadas publicamente. Essas APIs também estão sujeitas a alterações sem aviso prévio.

Informações relacionadas

"Use uma conta de locatário"

"Prometheus: Noções básicas de consulta"

Operações da API Grid Management

A API Grid Management organiza as operações de API disponíveis nas seções a seguir.

- * 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.
- **Alarms** — operações para listar alarmes atuais (sistema legado) e retornar informações sobre a integridade da grade, incluindo os alertas atuais e um resumo dos estados de conexão do nó.

- **Alert-history** — operações em alertas resolvidos.
- **Alert-receivers** — operações em recetores de notificação de alerta (e-mail).
- **Alert-rules** — operações em regras de alerta.
- **Alert-silences** — 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*").

  > 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.
- **dns-serviders** — operações para listar e alterar servidores DNS externos configurados.
- **Endpoint-domain-nanos** — operações para listar e alterar nomes de domínio de endpoint.
- **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 site).
- **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).
- **Licença** — operações para recuperar e atualizar a licença StorageGRID.
- **Logs** — operações para coletar e baixar arquivos de log.
- **Métricas** — operações em métricas do StorageGRID, incluindo consultas instantâneas de métricas 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-health** — operações no status de integridade do nó.
- **ntp-serviders** — operações para listar ou atualizar servidores NTP (Network Time Protocol) externos.
- **Objects** — operações em objetos e metadados de objetos.
- **Recovery** — operações para o procedimento de recuperação.
- **Recovery-package** — operações para baixar o Recovery Package.
- **Regions** — operações para visualizar e criar regiões.
- **S3-object-lock** — operações em configurações globais de bloqueio de objetos S3D.
- **Server-certificate** — operações para visualizar e atualizar certificados de servidor do Grid Manager.
- **snmp** — operações na configuração SNMP atual.
- **Traffic-classes** — 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.

Emissão de solicitações de API

A interface do usuário Swagger fornece detalhes completos e documentação para cada operação da API.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

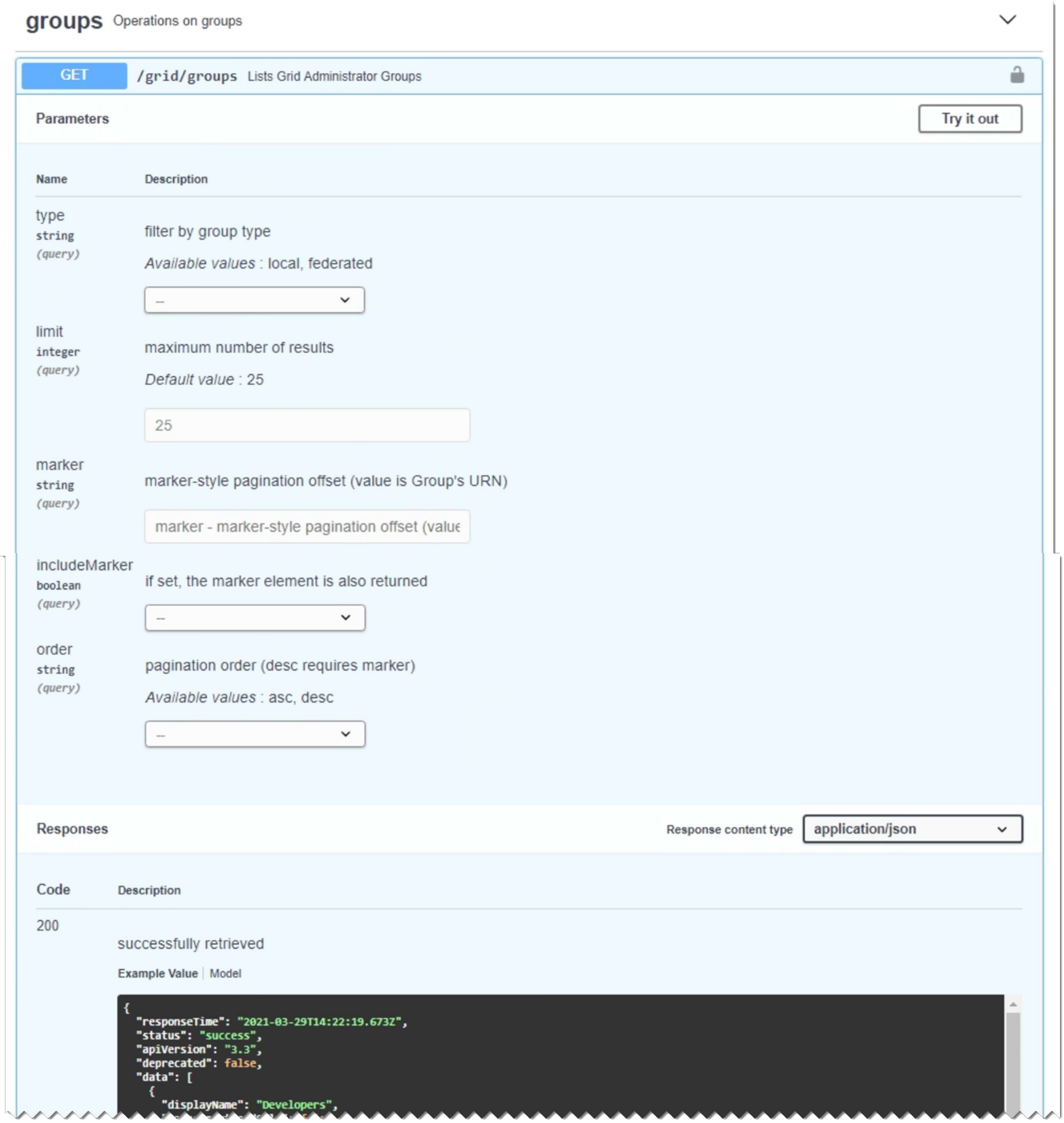
> Todas as operações de API que você executa usando a página da Web do API Docs são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. Selecione **Ajuda** > **Documentação da API** no cabeçalho do Grid Manager.
2. Selecione a operação desejada.

   Ao expandir uma operação de API, você pode ver as ações HTTP disponíveis, como GET, PUT, UPDATE e DELETE.

3. 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.



4. 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.
5. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode clicar em **modelo** para aprender os requisitos para cada campo.
6. Clique em **Experimente**.
7. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
8. Clique em **Executar**.
9. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

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 3 da API.

`https://hostname_or_ip_address/api/v3/authorize`

A versão principal da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que são ***not compatible*** com versões mais antigas. A versão menor da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que ***are 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 de gerenciamento de grade está 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.

> Você pode usar a API Grid Management para configurar as versões suportadas. Consulte a seção "config" da documentação da API Swagger para obter mais informações. Você deve desativar o suporte para a versão mais antiga depois de atualizar todos os clientes da API Grid Management 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 v1 API at POST "/api/v1/authorize"
```

Determinando quais versões de API são suportadas na versão atual

Use a seguinte solicitação de API para retornar uma lista das principais versões da API suportada:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especificando uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v3`) ou um cabeçalho (`Api-Version: 3`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Proteção contra falsificação de solicitação entre sites (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 `"Content-Type: application/json"` cabeçalho para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

Usando a API se o logon único estiver ativado

Se o logon único (SSO) tiver sido ativado para o seu sistema StorageGRID, você não poderá usar as solicitações padrão de autenticação API para fazer login e sair da API de gerenciamento de grade ou da API de gerenciamento de locatário.

Iniciar sessão na API se o início de sessão único estiver ativado

Se o logon único (SSO) tiver sido ativado, você deverá emitir uma série de solicitações de API para obter um token de autenticação do AD FS válido para a API de Gerenciamento de Grade ou a API de Gerenciamento de locatário.

O que você vai precisar

- 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 arquivos de instalação do StorageGRID (`./rpms`para Linux ou CentOS, para Ubuntu ou Debian, `./debs` 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: Uma SubjectConfirmation válida não foi encontrada nesta resposta.

  > 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: Versão SAML não suportada.

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 nome de usuário SSO
   - O domínio onde o StorageGRID está instalado
   - O endereço para StorageGRID
   - Se você quiser acessar a API de gerenciamento do locatário, insira o ID da conta do locatário. E

   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 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://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=For
msAuthentication" --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.

Sair 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.

Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID simplesmente 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=true"` 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=fZDNboMwEI
RfhZ...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=true"` 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
```

Usando certificados de segurança do StorageGRID

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).

Uma autoridade de certificação externa (CA) pode emitir certificados personalizados que são totalmente compatíveis com as políticas de segurança de informações da sua organização. O StorageGRID também inclui uma autoridade de certificação (CA) integrada que gera certificados de CA internos durante a instalação do sistema. Esses certificados internos de CA são usados, por padrão, para proteger o tráfego interno do StorageGRID. Embora você possa usar os certificados de CA internos 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 às diretrizes de fortalecimento do sistema para certificados de servidor.

  "Endurecimento do sistema"

- 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.

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado de cliente administrador	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.	**Configuração** > **Controle de Acesso** > **certificados de Cliente**	"Configurando certificados de cliente de administrador"
Certificado de federação de identidade	Servidor	Autentica a conexão entre o StorageGRID e um ative Directory externo, OpenLDAP ou Oracle Directory Server.usado para federação de identidade, o que permite que grupos de administradores e usuários sejam gerenciados por um sistema externo.	**Configuração** > **Controle de Acesso** > **Federação de identidade**	"Usando a federação de identidade"
Certificado de logon único (SSO)	Servidor	Autentica a conexão entre os Serviços de Federação do ative Directory (AD FS) e o StorageGRID que é usado para solicitações de logon único (SSO).	**Configuração** > **Controle de Acesso** > **Início de sessão único**	"Configurando logon único"

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado de servidor de gerenciamento de chaves (KMS)	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.	**Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**	"Adicionar um servidor de gerenciamento de chaves (KMS)"
Certificado de notificação de alerta por e-mail	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 de e-mail**	"Monitorizar Resolução de problemas"

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado de ponto final do balanceador de carga	Servidor	Autentica a conexão entre clientes S3 ou Swift e o serviço StorageGRID Load Balancer em nós de gateway ou nós de administração. Você carrega ou gera um certificado do balanceador de carga quando configura um endpoint do balanceador de carga. Os aplicativos do cliente usam o certificado do balanceador de carga ao se conetar ao StorageGRID para salvar e recuperar dados do objeto. **Nota:** o certificado do balanceador de carga é o certificado mais utilizado durante a operação normal do StorageGRID.	**Configuração** > **Configurações de rede** > **pontos finais do Load Balancer**	• "Configuração dos pontos de extremidade do balanceador de carga" • Criando um ponto de extremidade do balanceador de carga para FabricPool "Configurar o StorageGRID para FabricPool"

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado do servidor de interface de gerenciamento	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. Você pode usar o certificado de CA interno ou carregar um certificado personalizado.	**Configuração** > **Configurações de rede** > **certificados de servidor**	• "Configurando certificados de servidor" • "Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"
Certificado de endpoint do Cloud Storage Pool	Servidor	Autentica a conexão do pool de storage de nuvem do StorageGRID para um local de storage externo (como o storage S3 Glacier ou Microsoft Azure Blob). Um certificado diferente é necessário para cada tipo de provedor de nuvem.	**ILM** > **conjuntos de armazenamento**	"Gerenciar objetos com ILM"
Certificado de endpoint de serviços de plataforma	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**	"Use uma conta de locatário"

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado do servidor de extremidade do serviço API do Object Storage	Servidor	Autentica conexões de cliente S3 ou Swift seguras ao serviço LDR (local Distribution Router) em um nó de armazenamento ou ao serviço CLB (descontinuado Connection Load Balancer) em um nó de gateway.	**Configuração** > **Configurações de rede** > **pontos finais do Load Balancer**	"Configurando um certificado de servidor personalizado para conexões ao nó de armazenamento ou ao serviço CLB"

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 ou Swift 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.

Controlar o acesso do administrador ao StorageGRID

Você pode controlar o acesso do administrador ao sistema StorageGRID abrindo ou fechando portas de firewall, gerenciando grupos de administração e usuários, configurando logon único (SSO) e fornecendo certificados de cliente para permitir acesso externo seguro às métricas do StorageGRID.

- "Controlar o acesso através de firewalls"
- "Usando a federação de identidade"
- "Gerenciando grupos de administradores"
- "Gerenciamento de usuários locais"
- "Usando logon único (SSO) para StorageGRID"
- "Configurando certificados de cliente de administrador"

Controlar o acesso através de firewalls

Quando quiser controlar o acesso através de firewalls, abra ou feche portas específicas no firewall externo.

Controlar o acesso 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.

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.
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 da API de gerenciamento não podem acessar o Gerenciador do locatário ou a API de gerenciamento do locatário. • As solicitações de conteúdo interno serão rejeitadas.

Porta	Descrição	Se a porta estiver aberta…
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

"Iniciar sessão no Grid Manager"

"Criando uma conta de locatário se o StorageGRID não estiver usando SSO"

"Resumo: Endereços IP e portas para conexões de clientes"

"Gerenciando redes de clientes não confiáveis"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

Usando 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.

Configurando a federação de identidade

Você pode configurar a federação de identidade se quiser que os grupos de administração e usuários sejam gerenciados em outro sistema, como ative Directory, OpenLDAP ou Oracle Directory Server.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Se você pretende ativar o logon único (SSO), você deve usar o ative Directory como a origem de identidade federada e o AD FS como o provedor de identidade. Consulte ""requisitos para utilizar o início de sessão único.""
- Você deve estar usando o ative Directory, OpenLDAP ou Oracle Directory Server como o provedor de identidade.

Se pretender utilizar um serviço LDAP v3 que não esteja listado, tem de contactar o suporte técnico.

- 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.

Sobre esta tarefa

Você deve configurar uma origem de identidade para o Gerenciador de Grade se quiser importar os seguintes tipos de grupos federados:

- 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 origem 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.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.
2. Selecione **Ativar federação de identidade**.

   São apresentados os campos para configurar o servidor LDAP.

3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.

   Você pode selecionar **ative Directory**, **OpenLDAP** ou **Other**.

   Se selecionar **OpenLDAP**, tem de configurar o servidor OpenLDAP. Consulte as diretrizes para configurar um servidor OpenLDAP.

   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.
   - **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. Na secção Configurar servidor LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias.
   - **Nome do host**: O nome do host do servidor 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`

   - **Senha**: A senha associada ao nome de usuário.
   - **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 base do usuário** a que pertencem.

6. Na seção **Transport Layer Security (TLS)**, selecione uma configuração de segurança.
   - **Use STARTTLS (recomendado)**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada.
   - **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Esta opção é suportada por razões de compatibilidade.
   - **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido.

     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 padrão instalado no sistema operacional para proteger conexões.
- **Use certificado CA personalizado**: Use um certificado de segurança personalizado.

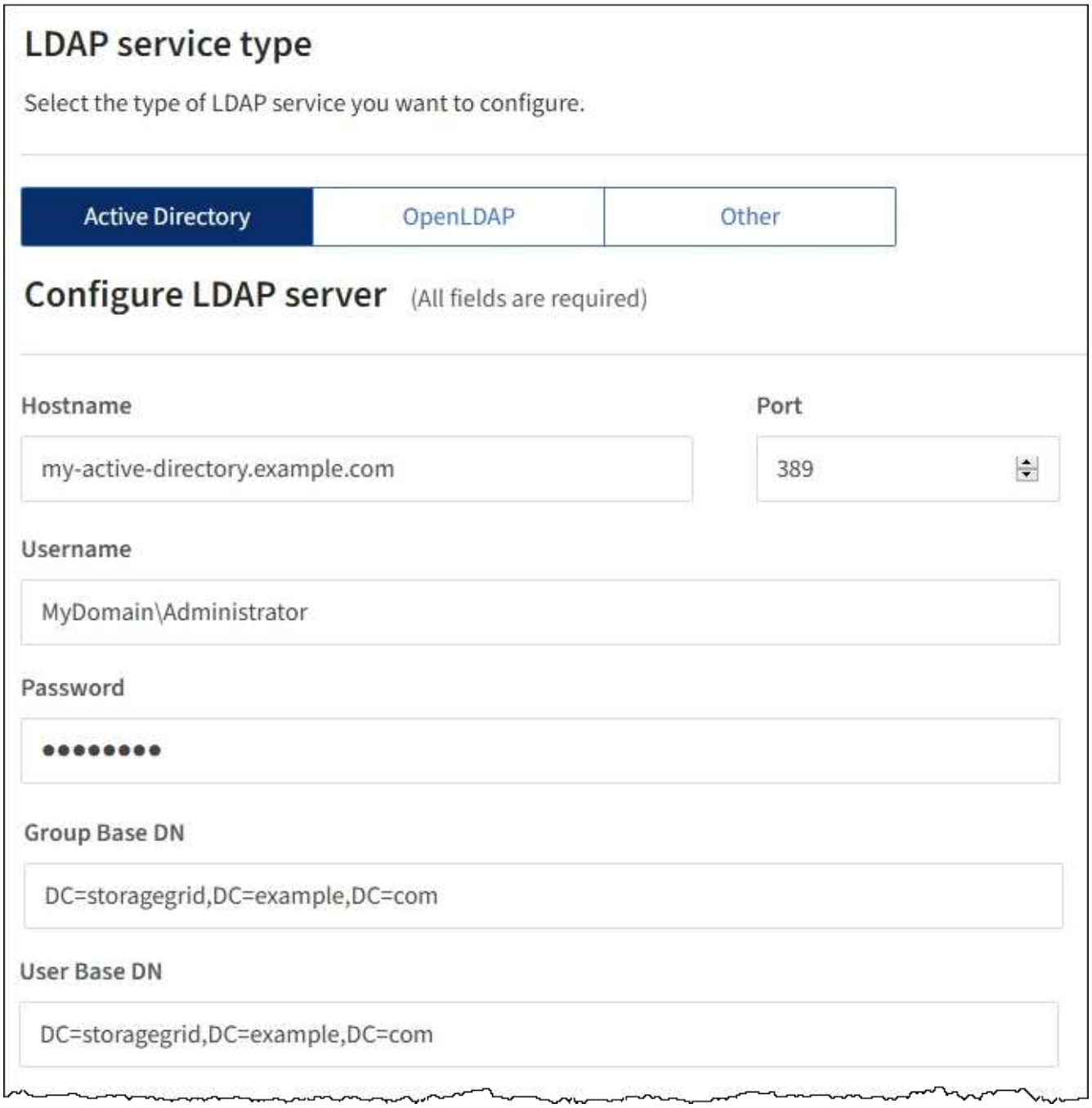
  Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

8. Opcionalmente, selecione **testar conexão** para validar suas configurações de conexão para o servidor LDAP.

   Uma mensagem de confirmação aparece no canto superior direito da página se a conexão for válida.

9. Se a conexão for válida, selecione **Salvar**.

   A captura de tela a seguir mostra valores de configuração de exemplo para um servidor LDAP que usa o ative Directory.



Informações relacionadas

"Cifras suportadas para conexões TLS de saída"

"Requisitos para o uso de logon único"

"Criando uma conta de locatário"

"Use uma conta de locatário"

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.

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para manutenção de associação reversa em grupo no Guia do Administrador para OpenLDAP.

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 Guia do Administrador para OpenLDAP.

Informações relacionadas

"Documentação do OpenLDAP: Guia do administrador da versão 2,4"

Forçando 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.

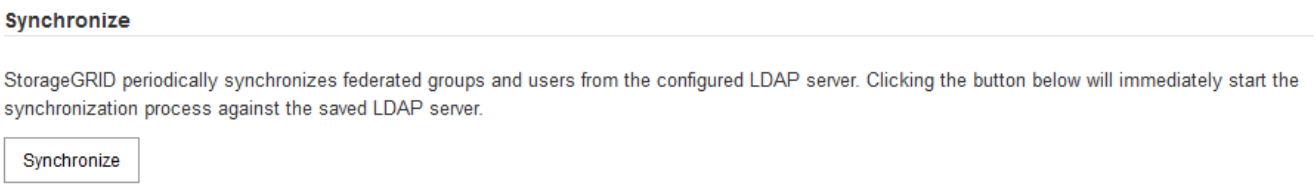
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- A origem da identidade deve estar ativada.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.

   A página Federação de identidade é exibida. O botão **Sincronizar** está na parte inferior da página.

2. Clique em **Sincronizar**.

   Uma mensagem de confirmação indica que a sincronização foi iniciada com êxito. 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.

Desativando 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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 ou alarmes não serão gerados para contas que não foram 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.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.
2. Desmarque a caixa de seleção **Ativar Federação de identidade**.
3. Clique em **Salvar**.

Informações relacionadas

"Desativação do logon único"

Gerenciando 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.

Criando grupos 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.

O que você vai precisar

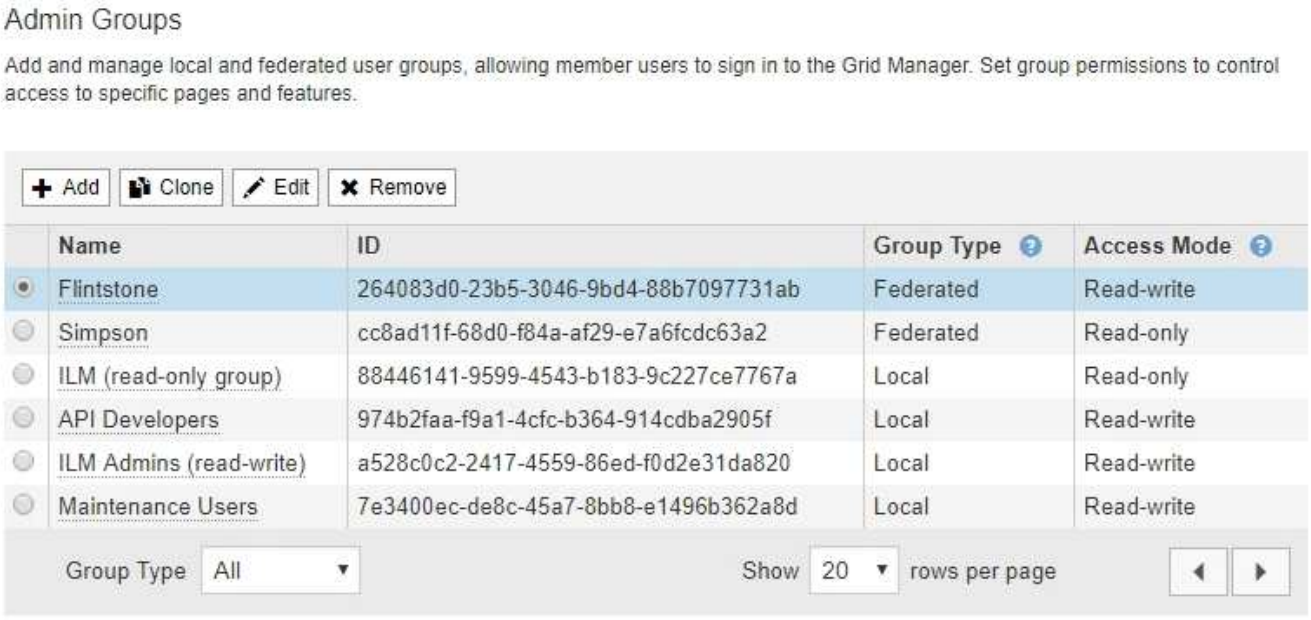
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

- Se você pretende importar um grupo federado, você deve ter a federação de identidade configurada e o grupo federado já deve existir na origem de identidade configurada.

Passos

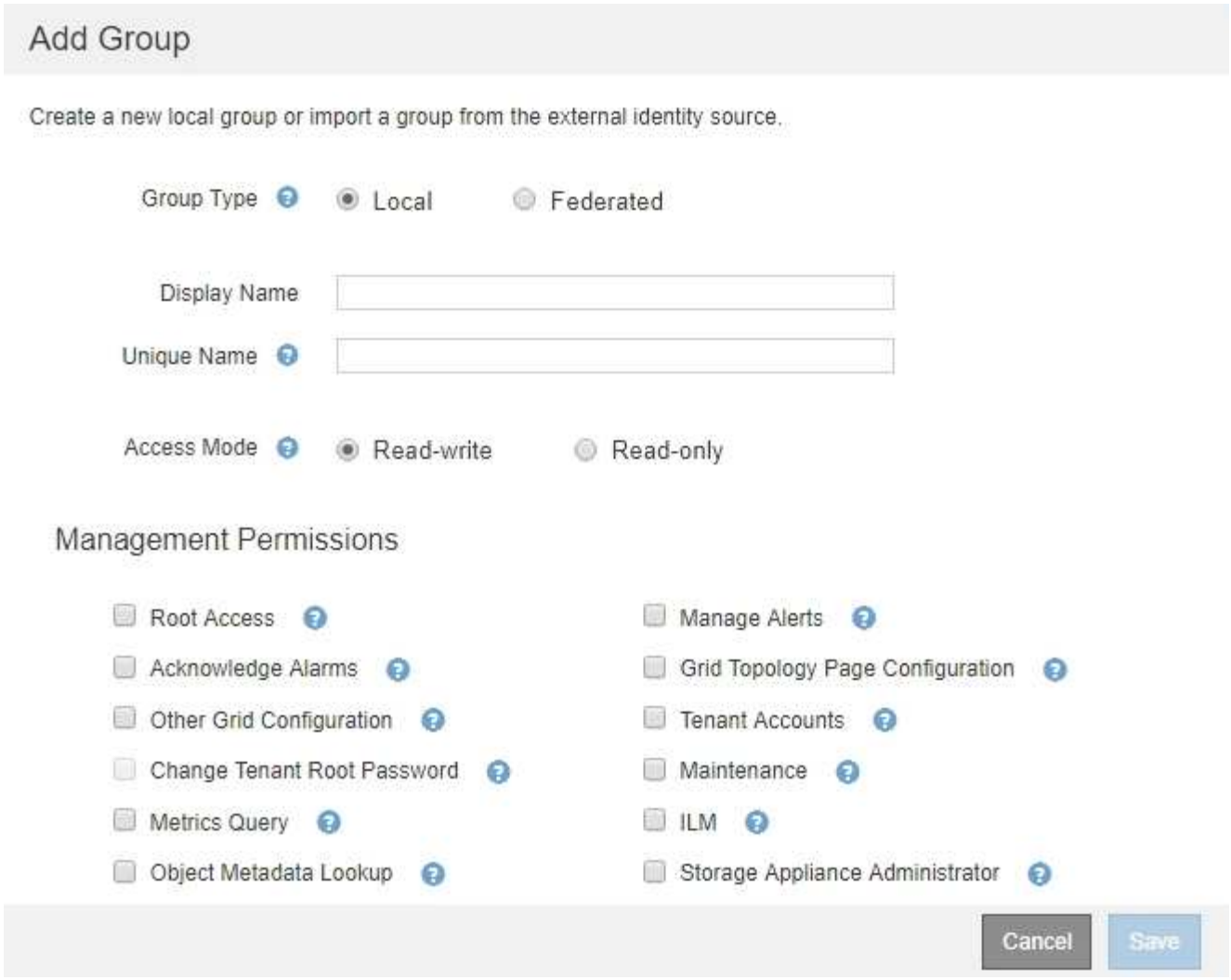
1. Selecione **Configuration** > **Access Control** > **Admin Groups**.

   A página grupos de administração é exibida e lista todos os grupos de administração existentes.



2. Selecione **Adicionar**.

   A caixa de diálogo Adicionar grupo é exibida.



3. Para tipo de grupo, selecione **local** se quiser criar um grupo que será usado somente no StorageGRID ou selecione **federado** se quiser importar um grupo da origem de identidade.
4. Se você selecionou **local**, digite um nome de exibição para o grupo. O nome de exibição é o nome que aparece no Gerenciador de Grade. Por exemplo, "'usuários de Manutenção'" ou "'Administradores de ILM.'"
5. Introduza um nome exclusivo para o grupo.
   - **Local**: Digite o nome exclusivo que você deseja. Por exemplo, "'Administradores ILM.'"
   - **Federated**: Insira o nome do grupo exatamente como ele aparece na origem de identidade configurada.
6. 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.

7. Selecione uma ou mais permissões de gerenciamento.

   Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes ao grupo não poderão entrar no StorageGRID.

8. Selecione **Guardar**.

   O novo grupo é criado. Se este for um grupo local, agora você pode adicionar um ou mais usuários. Se este for um grupo federado, a fonte de identidade gerencia quais usuários pertencem ao grupo.

Informações relacionadas

"Gerenciamento de usuários locais"

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.

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
- Veja o Dashboard
- Exibir as páginas de nós
- Monitore a topologia da grade
- Ver alertas atuais e resolvidos
- Visualizar alarmes atuais e históricos (sistema legado)
- Alterar sua própria senha (somente usuários locais)
- Visualize determinadas informações nas páginas Configuração e Manutenção

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 de acesso root.

Acesso à raiz

Essa permissão fornece acesso a todos os recursos de administração de grade.

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.

Reconhecer alarmes (sistema legado)

Esta permissão fornece acesso para reconhecer e responder a alarmes (sistema legado). Todos os usuários conetados podem visualizar alarmes atuais e históricos.

Se você quiser que um usuário monitore a topologia da grade e reconheça somente alarmes, você deve atribuir essa permissão.

Configuração da página de topologia da grelha

Esta permissão fornece acesso às seguintes opções de menu:

- Guias de configuração disponíveis nas páginas em **suporte** > **Ferramentas** > **topologia de grade**.
- **Redefinir contagens de eventos** na guia **nós** > **Eventos**.

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 de Configuração de Página de topologia de Grade.

- **Alarmes** (sistema legado):
  - Alarmes globais
  - Configuração de e-mail legado
- **ILM**:
  - Pools de armazenamento
  - Classes de armazenamento
- **Configuração** > **Configurações de rede**
  - Custo da ligação
- **Configuração** > **Configurações do sistema**:
  - Opções de exibição
  - Opções de grelha
  - Opções de armazenamento
- **Configuração** > **Monitoramento**:
  - Eventos
- **Suporte**:
  - AutoSupport

Contas de inquilino

Esta permissão fornece acesso à página **tenants** > **Tenant Accounts**.

> A versão 1 da API Grid Management (que foi obsoleta) usa essa permissão para gerenciar políticas de grupo de locatários, redefinir senhas de administrador Swift e gerenciar chaves de acesso S3 do usuário raiz.

Altere a senha raiz do locatário

Essa permissão fornece acesso à opção **alterar senha de root** na página Contas de locatário, permitindo que você controle quem pode alterar a senha para o usuário raiz local do locatário. Os usuários que não têm essa permissão não podem ver a opção **alterar senha de root**.

> Você deve atribuir a permissão Contas do locatário ao grupo antes de poder atribuir essa permissão.

Manutenção

Esta permissão fornece acesso às seguintes opções de menu:

- **Configuração** > **Configurações do sistema**:
  - Nomes de domínio*
  - Certificados de servidor*
- **Configuração** > **Monitoramento**:
  - Auditoria*
- **Configuração** > **Controle de Acesso**:
  - Senhas de grade
- **Manutenção** > **tarefas de manutenção**
  - Descomissionar
  - Expansão
  - Recuperação
- **Manutenção** > **rede**:
  - Servidores DNS*
  - Rede de rede*
  - Servidores NTP*
- **Manutenção** > **sistema**:
  - Licença*
  - Pacote de recuperação
  - Atualização de software
- **Suporte** > **Ferramentas**:
  - Registos
- Os usuários que não têm a permissão Manutenção podem exibir, mas não editar, as páginas marcadas com um asterisco.

Consulta de métricas

Esta permissão fornece acesso à página **suporte** > **Ferramentas** > **métricas**. Essa permissão também fornece acesso a consultas de métricas personalizadas do Prometheus usando a seção **Metrics** da API Grid Management.

ILM

Esta permissão fornece acesso às seguintes opções de menu **ILM**:

- **Codificação de apagamento**
- **Regras**
- **Políticas**
- **Regiões**

> O acesso às opções de menu **ILM** > **Storage Pools** e **ILM** > **Storage grades** é controlado pelas outras permissões de Configuração de Grade e topologia de Grade Page Configuration.

Pesquisa de metadados de objetos

Esta permissão fornece acesso à opção de menu **ILM** > **Object Metadata Lookup**.

Administrador do dispositivo de armazenamento

Essa permissão fornece acesso ao Gerenciador de sistemas do e-Series SANtricity em dispositivos de storage por meio do Gerenciador de Grade.

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.

Desativando recursos da API de Gerenciamento de Grade

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. A desativação de um recurso é a única maneira de impedir que o usuário raiz ou os usuários que pertencem a grupos de administração com a permissão de acesso root 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 **Change Tenant Root Password** no Gerenciador de Grade (tanto a UI quanto a API), a empresa A pode garantir que nenhum usuário Admin - incluindo o usuário root e usuários pertencentes a grupos com a permissão de acesso root - pode alterar a senha para o usuário root de qualquer conta de locatário.*

Reativando as 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.

Para obter detalhes, consulte as instruções para a implementação de aplicativos cliente S3 ou Swift.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade.
2. Localize o endpoint Deactivate Features
3. Para desativar um recurso, como **alterar 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 de senha raiz do locatário de alteração não aparece mais na interface do usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário falhará com "'403 Forbidden.'"

4. Para reativar todos os recursos, envie um corpo para a API assim:

```
{ "grid": null }
```

Quando esta solicitação estiver concluída, todos os recursos, incluindo o recurso alterar senha de root do locatário, são reativados. A permissão de gerenciamento de senha de raiz do locatário de alteração agora aparece na interface do usuário e qualquer solicitação de API que tente alterar a senha de raiz de um locatário será bem-sucedida, assumindo que o usuário tenha a permissão de gerenciamento de senha de raiz do locatário ou altere a permissão de gerenciamento de senha de raiz 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 raiz do locatário e continuar a desativar o recurso de reconhecimento de alarme, envie esta SOLICITAÇÃO DE COMPRA:

```
{ "grid": { "alarmAcknowledgment": true } }
```

Informações relacionadas

"Usando a API de gerenciamento de grade"

Modificando um grupo de administração

Você pode modificar um grupo de administração para alterar as permissões associadas ao grupo. Para grupos de administração locais, também é possível atualizar o nome de exibição.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Groups**.
2. Selecione o grupo.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Editar**.
4. Opcionalmente, para grupos locais, digite o nome do grupo que aparecerá para os usuários, por exemplo, "'usuários de Manutenção.'"

   Não é possível alterar o nome exclusivo, que é o nome do grupo interno.

5. Opcionalmente, altere o modo de acesso do grupo.
   - **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.

6. Opcionalmente, adicione ou remova permissões de grupo.

   Consulte informações sobre as permissões do grupo de administração.

7. Selecione **Guardar**.

Informações relacionadas

Permissões do grupo de administração

Eliminar um grupo de administração

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 quaisquer usuários de administrador do grupo, mas não exclui os usuários de administrador.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Quando você exclui um grupo, os usuários atribuídos a esse grupo perderão todos os Privileges de Acesso ao Gerenciador de Grade, a menos que sejam concedidos Privileges por um grupo diferente.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Groups**.
2. Selecione o nome do grupo.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Selecione **Remover**.
4. Selecione **OK**.

Gerenciamento de usuários locais

Você pode criar usuários locais e atribuí-los a grupos de administração locais para determinar quais recursos do Gerenciador de Grade esses usuários podem acessar.

O Gerenciador de Grade inclui um usuário local predefinido, chamado "root". Embora você possa adicionar e remover usuários locais, não é possível remover o usuário root.

Se o logon único (SSO) tiver sido ativado, os usuários locais não poderão fazer login no StorageGRID.

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Criando um usuário local

Se tiver criado grupos de administração locais, pode criar um ou mais utilizadores locais e atribuir cada utilizador a um ou mais grupos. As permissões do grupo controlam quais recursos do Gerenciador de Grade o usuário pode acessar.

Sobre esta tarefa

Você só pode criar usuários locais e só pode atribuir esses usuários a grupos de administração locais. Usuários federados e grupos federados são gerenciados usando a fonte de identidade externa.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Clique em **criar**.
3. Introduza o nome de apresentação do utilizador, o nome exclusivo e a palavra-passe.
4. Atribua o usuário a um ou mais grupos que governam as permissões de acesso.

   A lista de nomes de grupos é gerada a partir da tabela grupos.

5. Clique em **Salvar**.

Informações relacionadas

"Gerenciando grupos de administradores"

Modificando a conta de um usuário local

Você pode modificar a conta de um usuário de administrador local para atualizar o nome de exibição do usuário ou a associação de grupo. Você também pode impedir temporariamente que um usuário acesse o sistema.

Sobre esta tarefa

Só pode editar utilizadores locais. Os detalhes do usuário federados são sincronizados automaticamente com a fonte de identidade externa.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Selecione o utilizador que pretende editar.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Editar**.
4. Opcionalmente, faça alterações no nome ou na associação ao grupo.
5. Opcionalmente, para impedir que o usuário acesse o sistema temporariamente, marque **Negar acesso**.
6. Clique em **Salvar**.

   As novas configurações são aplicadas da próxima vez que o usuário sair e, em seguida, voltar a entrar no Gerenciador de Grade.

Eliminar a conta de um utilizador local

Você pode excluir contas de usuários locais que não precisam mais de acesso ao Gerenciador de Grade.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Selecione o utilizador local que pretende eliminar.

   Não é possível eliminar o utilizador local raiz predefinido.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Remover**.
4. Clique em **OK**.

Alterar a palavra-passe de um utilizador local

Os usuários locais podem alterar suas próprias senhas usando a opção **alterar senha** no banner do Gerenciador de Grade. Além disso, os usuários que têm acesso à página usuários administradores podem

alterar senhas para outros usuários locais.

Sobre esta tarefa

Você pode alterar senhas apenas para usuários locais. Os usuários federados devem alterar suas próprias senhas na fonte de identidade externa.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Na página usuários, selecione o usuário.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **alterar senha**.
4. Introduza e confirme a palavra-passe e clique em **Guardar**.

Usando logon único (SSO) para StorageGRID

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0). Quando o SSO está ativado, 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 utilizadores locais não podem iniciar sessão no StorageGRID.

- "Como o single sign-on funciona"
- "Requisitos para o uso de logon único"
- "Configurando logon único"

Como o single sign-on funciona

Antes de ativar o SSO (logon único), verifique como os processos de login e logout do StorageGRID são afetados quando o SSO está ativado.

Iniciar sessão quando o SSO está 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.

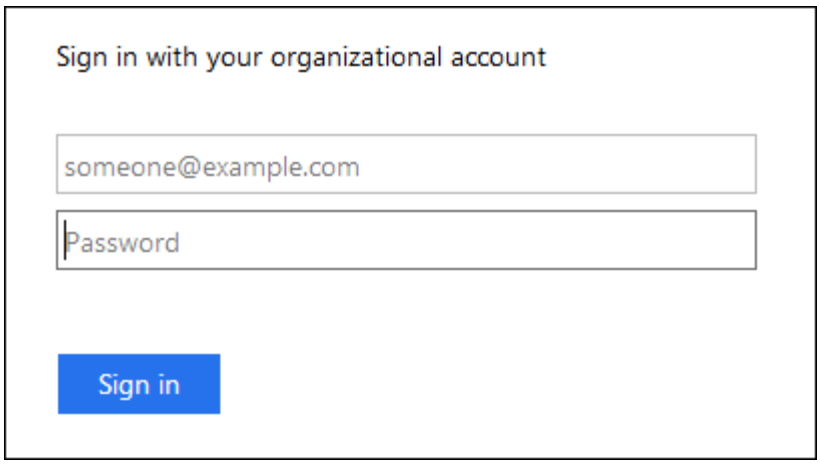
   - Se esta for a primeira vez que você acessou o URL neste navegador, será solicitado um ID de conta:

- 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. Clique em **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 que tenha permissão de acesso adequada, você será conetado ao Gerenciador de Grade ou ao Gerente do locatário, dependendo da conta selecionada.

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.

Terminar sessão quando o SSO está 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. Clique em **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
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

Se você estiver conetado a…	E você sai de…	Você está logado fora de…
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 para o uso de logon único

Antes de ativar o logon único (SSO) para um sistema StorageGRID, revise os requisitos nesta seção.

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.

Requisitos do provedor de identidade

O provedor de identidade (IDP) para SSO deve atender aos seguintes requisitos:

- Uma das seguintes versões do ative Directory Federation Service (AD FS):
  - AD FS 4,0, incluído no Windows Server 2016

    O Windows Server 2016 deve estar usando o "Atualização do KB3201845", ou superior.

  - AD FS 3,0, incluído na atualização do Windows Server 2012 R2 ou superior.
- Transport Layer Security (TLS) 1,2 ou 1,3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Requisitos de certificado do servidor

O StorageGRID usa um certificado de servidor 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 as confianças de parte confiáveis SSO para o StorageGRID no AD FS, você usa o certificado do servidor como o certificado de assinatura para solicitações do StorageGRID para o AD FS.

Se você ainda não tiver instalado um certificado de servidor personalizado para a interface de gerenciamento, você 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 terceiros dependentes do StorageGRID.

O uso do certificado de servidor padrão de um nó Admin na confiança de parte dependente do AD FS não é recomendado. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de poder iniciar sessão no nó recuperado, tem de atualizar a confiança da parte dependente no AD FS 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 .

Informações relacionadas

"Controlar o acesso através de firewalls"

"Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"

Configurando 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.

- "Confirmar que usuários federados podem entrar"
- "Usando o modo sandbox"
- "Criando confianças de parte confiáveis no AD FS"
- "Testando confianças de parte de confiança"
- "Ativar o início de sessão único"
- "Desativação do logon único"
- "Desativando e rehabilitando temporariamente o logon único para um nó de administração"

Confirmar que 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você está usando o ative Directory como fonte de identidade federada e o AD FS como provedor de identidade.

  "Requisitos para o uso de logon único"

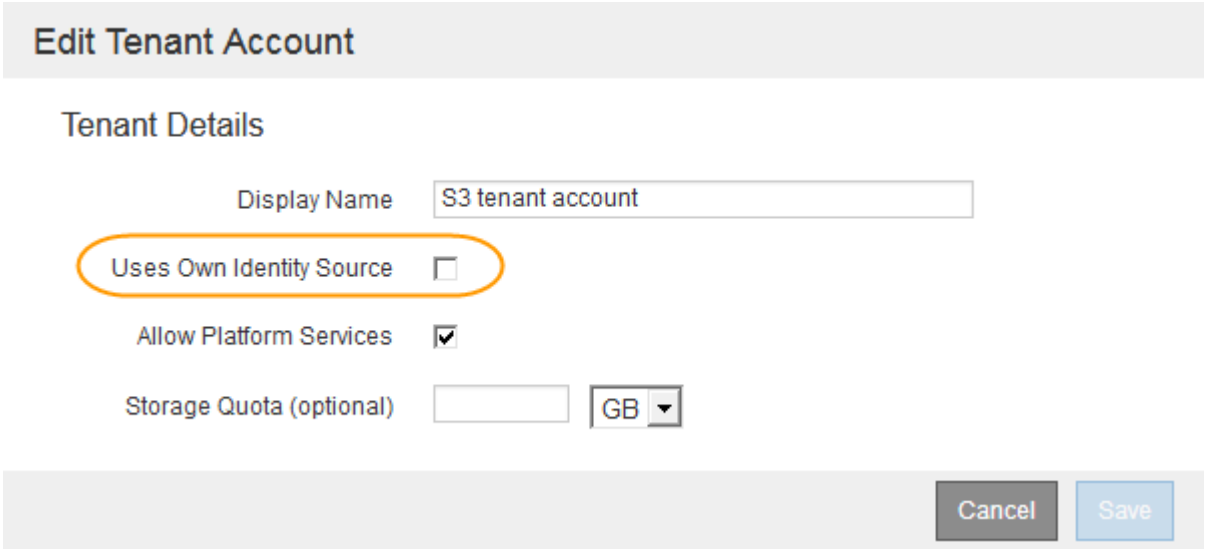
Passos

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 **Access Control** > **Identity Federation**.
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 clique em **Salvar**.

2. Confirme se um usuário federado pode acessar o Gerenciador de Grade:
   a. No Gerenciador de Grade, selecione **Configuração** > **Controle de Acesso** > **grupos de administradores**.
   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 clique em **Editar conta**.
   c. Se a caixa de seleção **usa origem de identidade própria** estiver selecionada, desmarque a caixa e clique em **Salvar**.



   A página Contas do locatário é exibida.
   a. Selecione a conta de locatário, clique em **entrar** e faça login na conta de locatário como usuário raiz local.
   b. No Gerenciador do Locatário, clique em **Controle 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 para o uso de logon único"

"Gerenciando grupos de administradores"

"Use uma conta de locatário"

Usando o modo sandbox

Você pode usar o modo sandbox para configurar e testar as confianças de parte dependentes dos Serviços de Federação do ative Directory (AD FS) antes de aplicar o logon único (SSO) para usuários do StorageGRID. Depois que o SSO estiver ativado, você poderá reativar o modo sandbox para configurar ou testar novos e existentes trusts de terceiros. A reativação do modo sandbox desativa temporariamente o SSO para usuários do StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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 AD FS. Por sua vez, o AD FS envia uma resposta de autenticação de volta ao StorageGRID, indicando se a solicitação de autorização foi bem-sucedida. Para solicitações bem-sucedidas, a resposta inclui um identificador universal exclusivo (UUID) para o usuário.

Para permitir que o StorageGRID (o provedor de serviços) e o AD FS (o provedor de identidade) se comuniquem com segurança sobre solicitações de autenticação de usuário, você deve configurar determinadas configurações no StorageGRID. Em seguida, você deve usar o AD FS para criar uma confiança de parte confiável para cada nó Admin. Finalmente, você deve retornar ao StorageGRID para ativar o SSO.

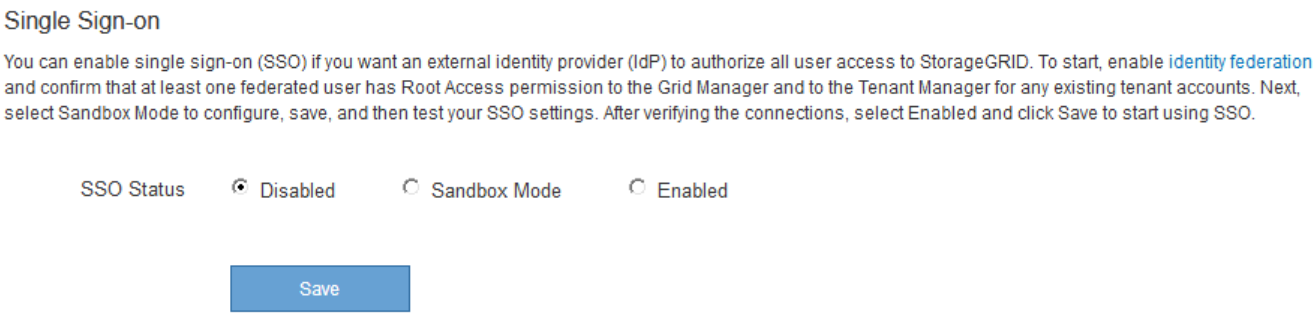
O modo Sandbox facilita a execução desta configuração de back-and-forth e testar todas as suas configurações antes de ativar o SSO.

> O uso do modo sandbox é altamente recomendado, mas não é estritamente necessário. Se você estiver preparado para criar confianças de parte dependentes do AD FS imediatamente após configurar o SSO no StorageGRID e não precisar testar os processos de SSO e logout único (SLO) para cada nó de administrador, clique em **habilitado**, insira as configurações do StorageGRID, crie uma confiança de parte confiável para cada nó de administrador no AD FS e clique em **Salvar** para ativar o SSO.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.

   A página Single Sign-On (Início de sessão único) é exibida, com a opção **Disabled** selecionada.



Se as opções de Status SSO não forem exibidas, confirme se você configurou o ative Directory como a origem de identidade federada. Consulte ""requisitos para utilizar o início de sessão único.""

2. Selecione a opção **Sandbox Mode**.

   As configurações Provedor de identidade e parte dependente aparecem. Na seção Provedor de identidade, o campo **tipo de serviço** é somente leitura. Ele mostra o tipo de serviço de federação de identidade que você está usando (por exemplo, ative Directory).

3. Na seção Provedor de identidade:

   a. Insira o nome do Serviço de Federação, exatamente como aparece no AD FS.

      Para localizar o Nome do Serviço de Federação, vá para Windows Server Manager. 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 se deseja usar a Segurança da camada de Transporte (TLS) 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 e cole o certificado na caixa de texto **certificado CA**.

      - **Não use TLS**: Não use um certificado TLS para proteger a conexão.

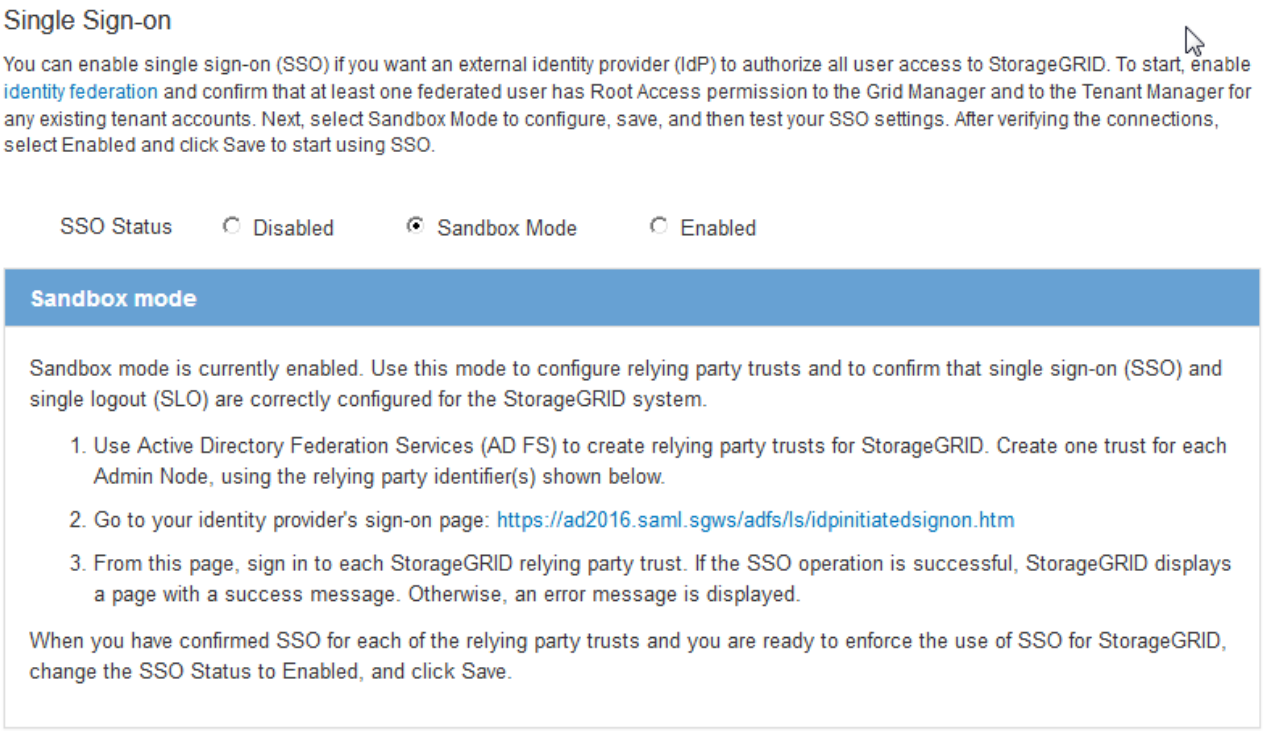
4. Na seção parte dependente, especifique o identificador de parte dependente que você usará para nós de administrador do StorageGRID quando você configurar confianças de parte dependentes.

   - 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 inclui um identificador de parte confiável para cada nó Admin, com base no nome do host do nó. Observação: Você deve criar uma confiança de parte confiável para cada nó de administrador em 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.

5. Clique em **Salvar**.
   - Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

   - O aviso de confirmação do modo Sandbox aparece, confirmando que o modo sandbox está agora ativado. Você pode usar esse modo enquanto usa o AD FS para configurar uma confiança de parte confiável para cada nó Admin e testar os processos de login único (SSO) e logout único (SLO).

Informações relacionadas

"Requisitos para o uso de logon único"

Criando confianças de parte confiáveis 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.

Criando 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.

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.

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.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No menu Iniciar do Windows, clique com o botão direito do Mouse no ícone do PowerShell 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. Clique em **Apply** e clique em **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. Clique em **Adicionar regra**.

d. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.

e. Na página Configurar regra, insira um nome de exibição para essa regra.

   Por exemplo, **ObjectGUID to Name ID**.

f. Para o Attribute Store, selecione **ative Directory**.

g. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.

h. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.

i. Clique em **Finish** e clique em **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 simplesmente 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, regresse ao StorageGRID e "teste todos os trusts de confiança"confirme que estão configurados corretamente.

Criando 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.

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.

  > ⓘ 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.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No Gerenciador do Windows Server, clique em **Ferramentas** e selecione **Gerenciamento do AD FS**.
2. Em ações, clique em **Adicionar confiança de parte dependente**.

3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e clique em **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. Clique em **Adicionar regra**:
   c. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.
   d. Na página Configurar regra, insira um nome de exibição para essa regra.

      Por exemplo, **ObjectGUID to Name ID**.

   e. Para o Attribute Store, selecione **ative Directory**.
   f. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
   g. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
   h. Clique em **Finish** e clique em **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 simplesmente 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, regresse ao StorageGRID e "teste todos os trusts de confiança"confirme que estão configurados corretamente.

Criando uma confiança de parte confiável manualmente

Se você optar por não importar os dados para as partes confiáveis, você poderá inserir os valores

manualmente.

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.

> 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 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.
- 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.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No Gerenciador do Windows Server, clique em **Ferramentas** e selecione **Gerenciamento do AD FS**.
2. Em ações, clique em **Adicionar confiança de parte dependente**.
3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e clique em **Iniciar**.
4. Selecione **Digite os dados sobre a parte confiável manualmente** e clique em **Avançar**.
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, clique em **Adicionar regra**:
   a. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.
   b. Na página Configurar regra, insira um nome de exibição para essa regra.

      Por exemplo, **ObjectGUID to Name ID**.

   c. Para o Attribute Store, selecione **ative Directory**.
   d. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
   e. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
   f. Clique em **Finish** e clique em **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. Clique em **Add 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. Clique em **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.

        Observação: usando o 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. Clique em **Apply** e clique em **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, regresse ao StorageGRID e "teste todos os trusts de confiança"confirme que estão configurados corretamente.

Testando confianças de parte de confiança

Antes de aplicar o uso de logon único (SSO) para StorageGRID, confirme se o logon único e o logout único (SLO) estão configurados corretamente. Se você criou uma confiança de parte confiável para cada nó Admin, confirme que você pode usar SSO e SLO para cada nó Admin.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você configurou uma ou mais confianças de parte confiáveis no AD FS.

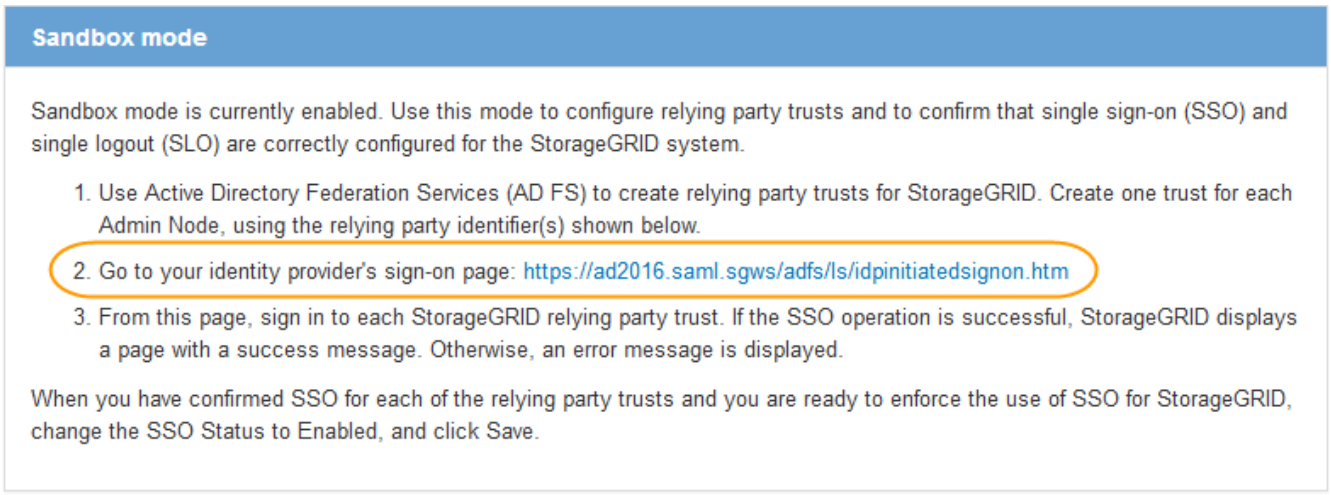
Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.

   A página Single Sign-On (Início de sessão único) é exibida, com a opção **Sandbox Mode** selecionada.

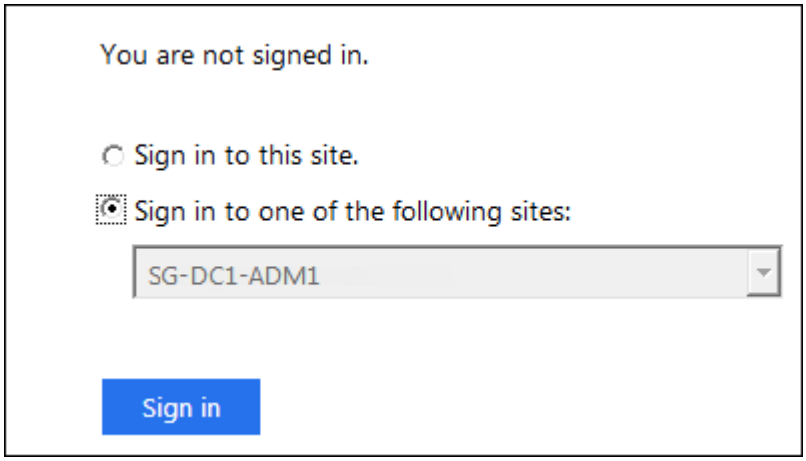
2. Nas instruções para o modo sandbox, localize o link para a página de logon do provedor de identidade.

   O URL é derivado do valor inserido no campo **Nome do serviço federado**.



3. Clique no link ou copie e cole o URL em um navegador para acessar a página de logon do provedor de identidade.
4. 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

clique em **entrar**.



Você é solicitado a digitar seu nome de usuário e senha.

5. 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.

     ✔ 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.
6. Repita as etapas anteriores para confirmar que você pode entrar em qualquer outro nó Admin.

   Se todas as operações de login e logout SSO forem bem-sucedidas, você estará pronto para ativar o SSO.

Ativar o início de sessão único

Depois de usar o modo sandbox para testar todas as suas trusts de terceiros dependentes do StorageGRID, você está pronto para ativar o logon único (SSO).

O que você vai precisar

- Você deve ter importado pelo menos um grupo federado da origem da identidade e atribuído permissões de gerenciamento de acesso raiz ao grupo. Você deve confirmar que pelo menos um usuário federado tem permissão de acesso root ao Gerenciador de Grade e ao Gerente do locatário para quaisquer contas de locatário existentes.
- Você deve ter testado todas as confianças de parte que dependem usando o modo sandbox.

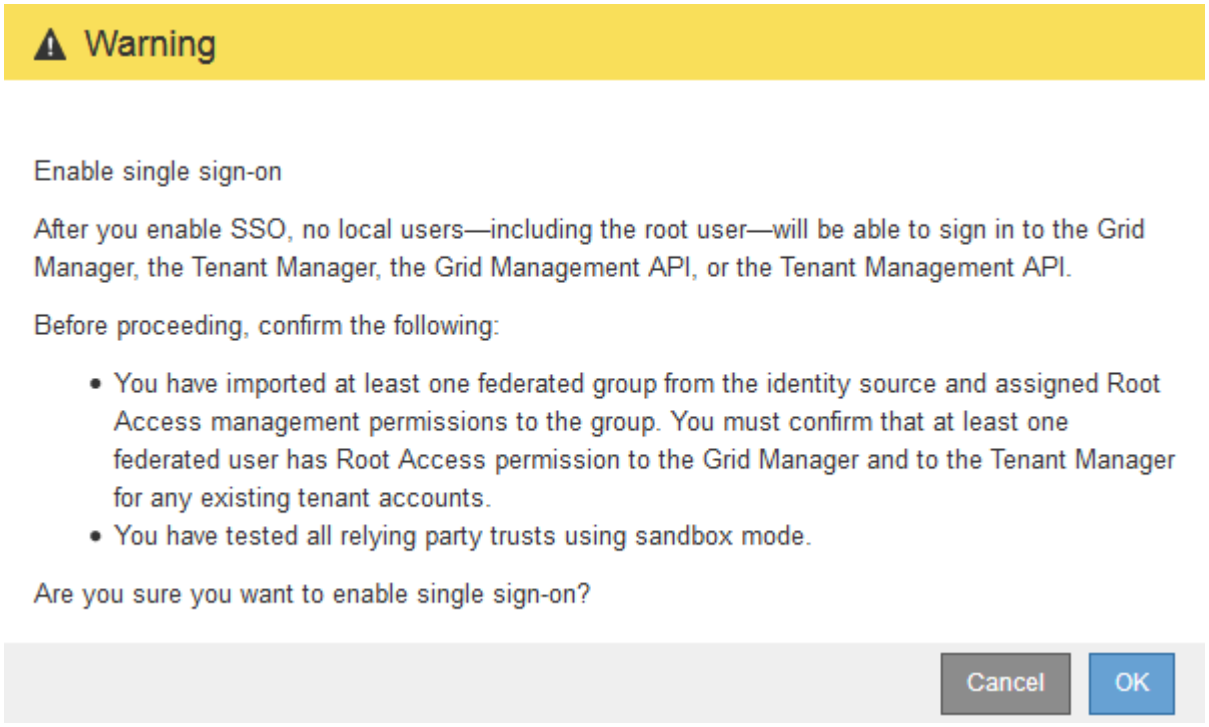
Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.

   A página Single Sign-On (Início de sessão único) aparece com **Sandbox Mode** selecionado.

2. Altere o Status SSO para **Enabled**.
3. Clique em **Salvar**.

É apresentada uma mensagem de aviso.



4. Reveja o aviso e clique em **OK**.

   O início de sessão único está agora ativado.

   Todos os usuários devem usar o SSO para acessar o Gerenciador de Grade, o Gerenciador de Tenant, a API de gerenciamento de grade e a API de gerenciamento de locatário. Os usuários locais não podem mais acessar o StorageGRID.

Desativação do 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

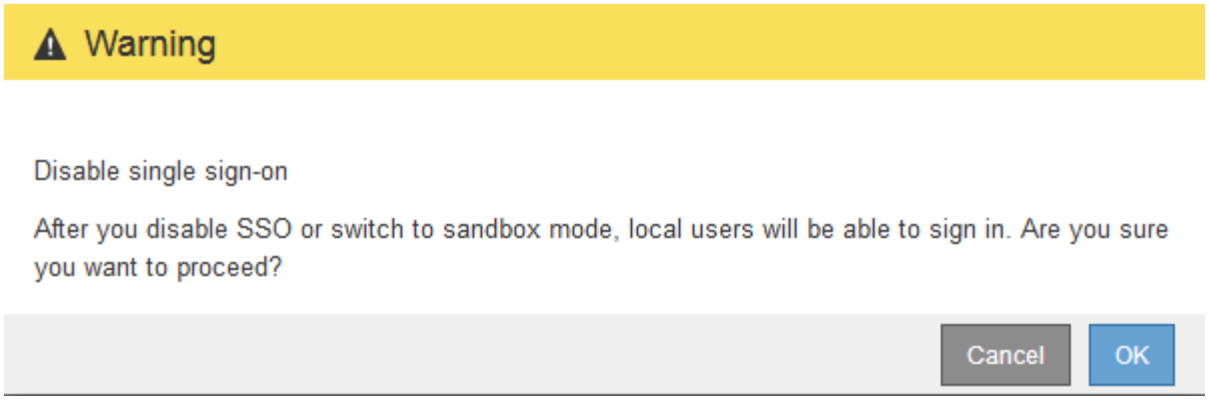
Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.

   É apresentada a página Single Sign-on (Início de sessão único).

2. Selecione a opção **Disabled** (Desativado).
3. Clique em **Salvar**.

   É apresentada uma mensagem de aviso indicando que os utilizadores locais poderão iniciar sessão.



4. Clique em **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.

Desativando e rehabilitando 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.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber 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 **Configuração** > **Controle de Acesso** > **Início de sessão único**.
   b. Altere as configurações de SSO incorretas ou desatualizadas.
   c. Clique em **Salvar**.

      Clicar em **Salvar** na página de logon único reativa automaticamente o SSO para toda a grade.

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. Clique em **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.

Informações relacionadas

"Configurando logon único"

Configurando certificados de cliente de administrador

Você pode usar certificados de cliente para permitir que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. Os certificados de cliente fornecem uma maneira segura de usar ferramentas externas para monitorar 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.

Adicionando certificados de cliente administrador

Para adicionar um certificado de cliente, você pode fornecer seu próprio certificado ou gerar um usando o Gerenciador de Grade.

O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve saber o endereço IP ou o nome de domínio do nó Admin.
- Você deve ter configurado o certificado do servidor de interface de gerenciamento do StorageGRID e ter o pacote de CA correspondente
- Se você quiser carregar seu próprio certificado, a chave pública e a chave privada do certificado devem estar disponíveis no computador local.

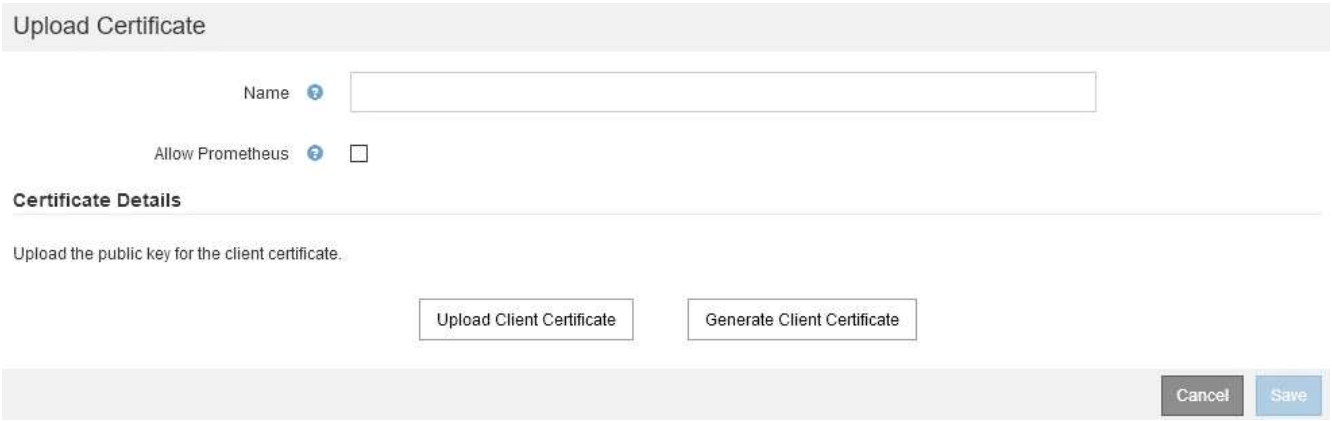
Passos

1. No Gerenciador de Grade, selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

   A página certificados de cliente é exibida.

2. Selecione **Adicionar**.

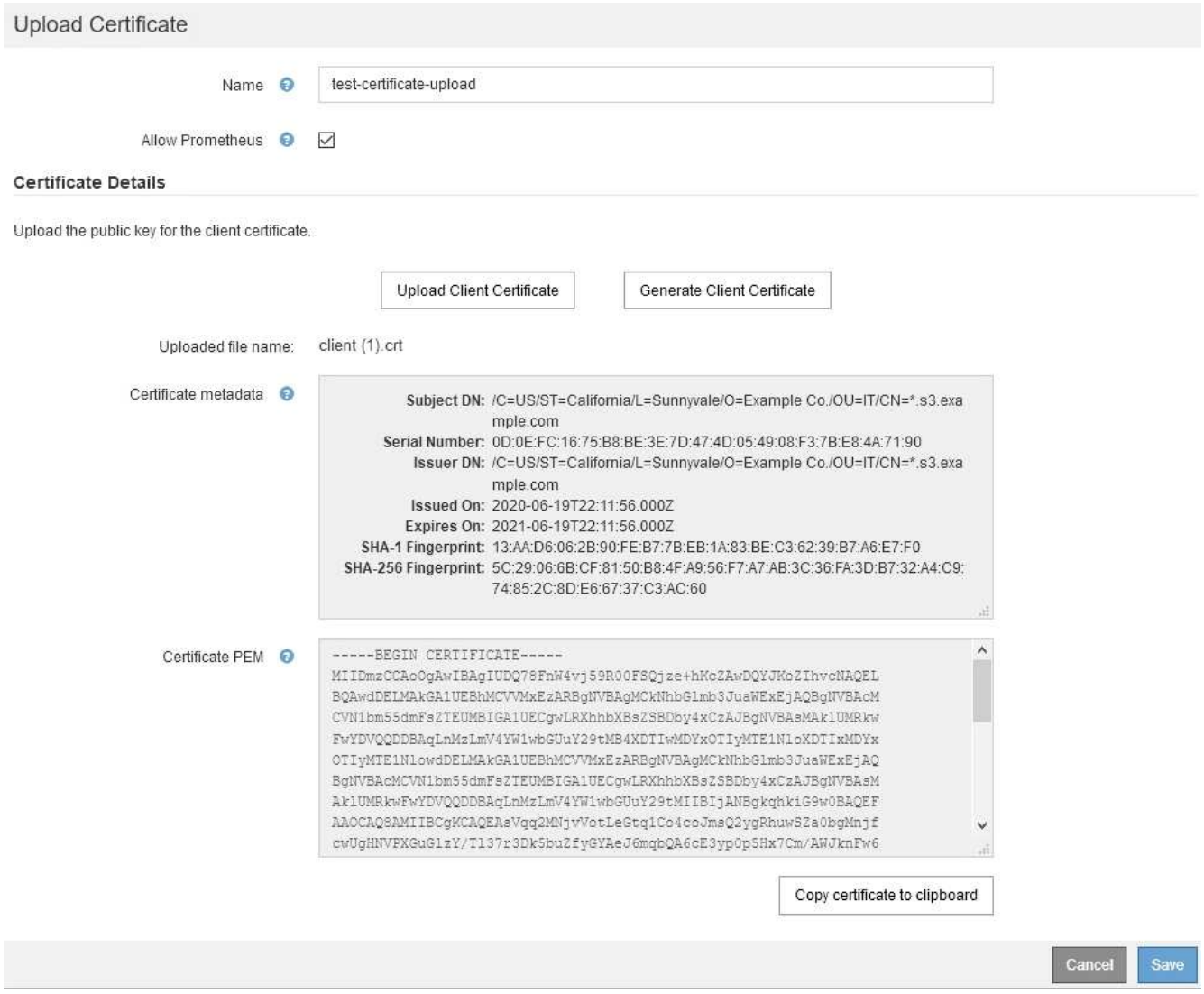
   A página carregar certificado é exibida.



3. Digite um nome entre 1 e 32 carateres para o certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, marque a caixa de seleção **Allow Prometheus**.

5. Carregar ou gerar um certificado:
   a. Para carregar um certificado, vá aqui.
   b. Para gerar um certificado, vá aqui.
6. para carregar um certificado:
   a. Selecione **carregar certificado de cliente**.
   b. Procure a chave pública do certificado.

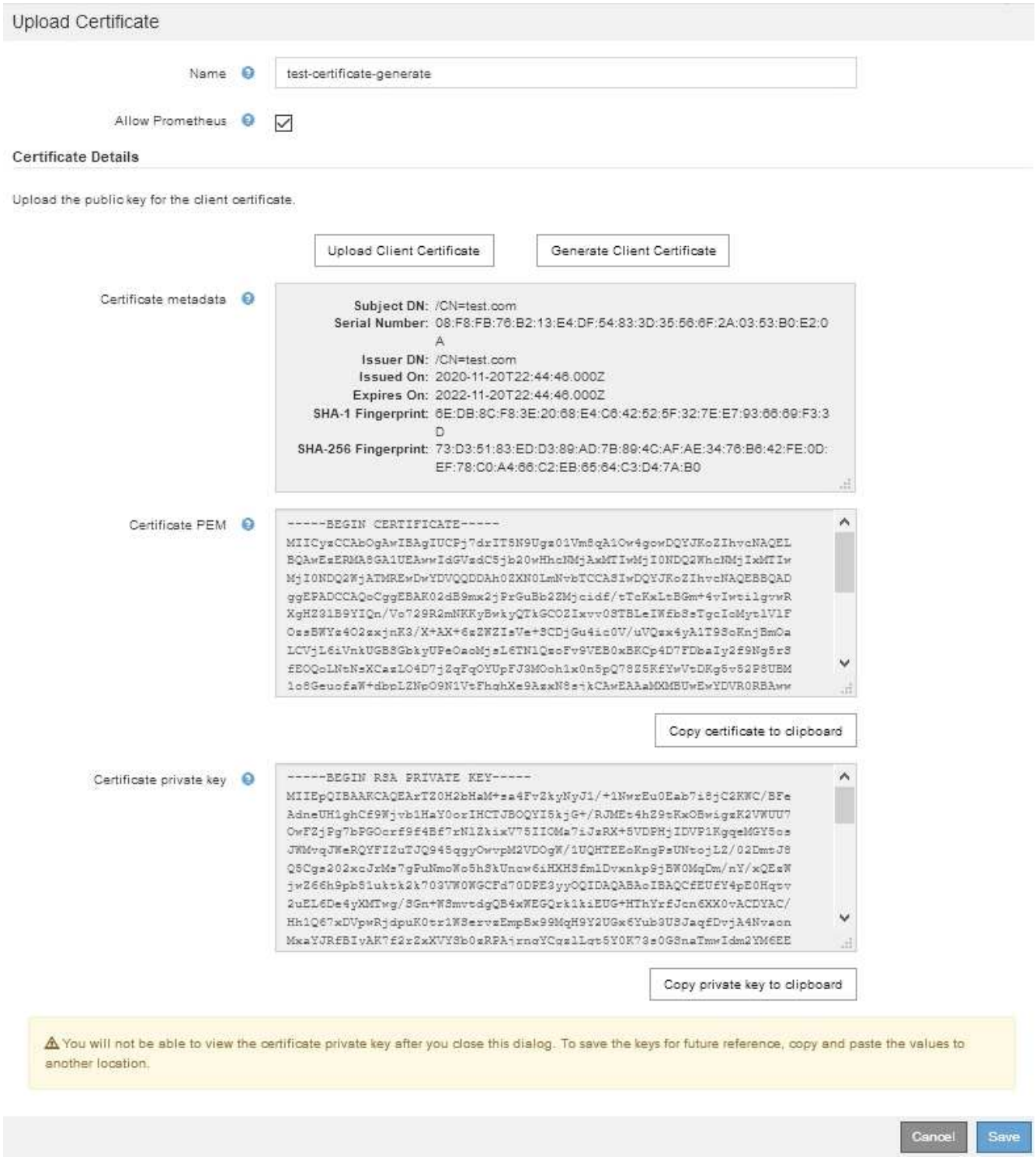
      Depois de carregar a chave pública para o certificado, os campos **metadados do certificado** e **PEM** do certificado são preenchidos.



   a. Selecione **Copiar certificado para a área de transferência** e cole o certificado na ferramenta de monitoramento externa.
   b. Use uma ferramenta de edição para copiar e colar a chave privada na sua ferramenta de monitoramento externo.
   c. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.
7. para gerar um certificado:

a. Selecione **Generate Client Certificate**.
b. Introduza o nome de domínio ou o endereço IP do nó de administração.
c. Opcionalmente, insira um assunto X,509, também chamado de Nome distinto (DN), para identificar o administrador que possui o certificado.
d. Opcionalmente, selecione o número de dias em que o certificado é válido. O padrão é de 730 dias.
e. Selecione **Generate**.

   Os campos **metadados do certificado**, **PEM** do certificado e **chave privada do certificado** são preenchidos.



a. Selecione **Copiar certificado para a área de transferência** e cole o certificado na ferramenta de monitoramento externa.

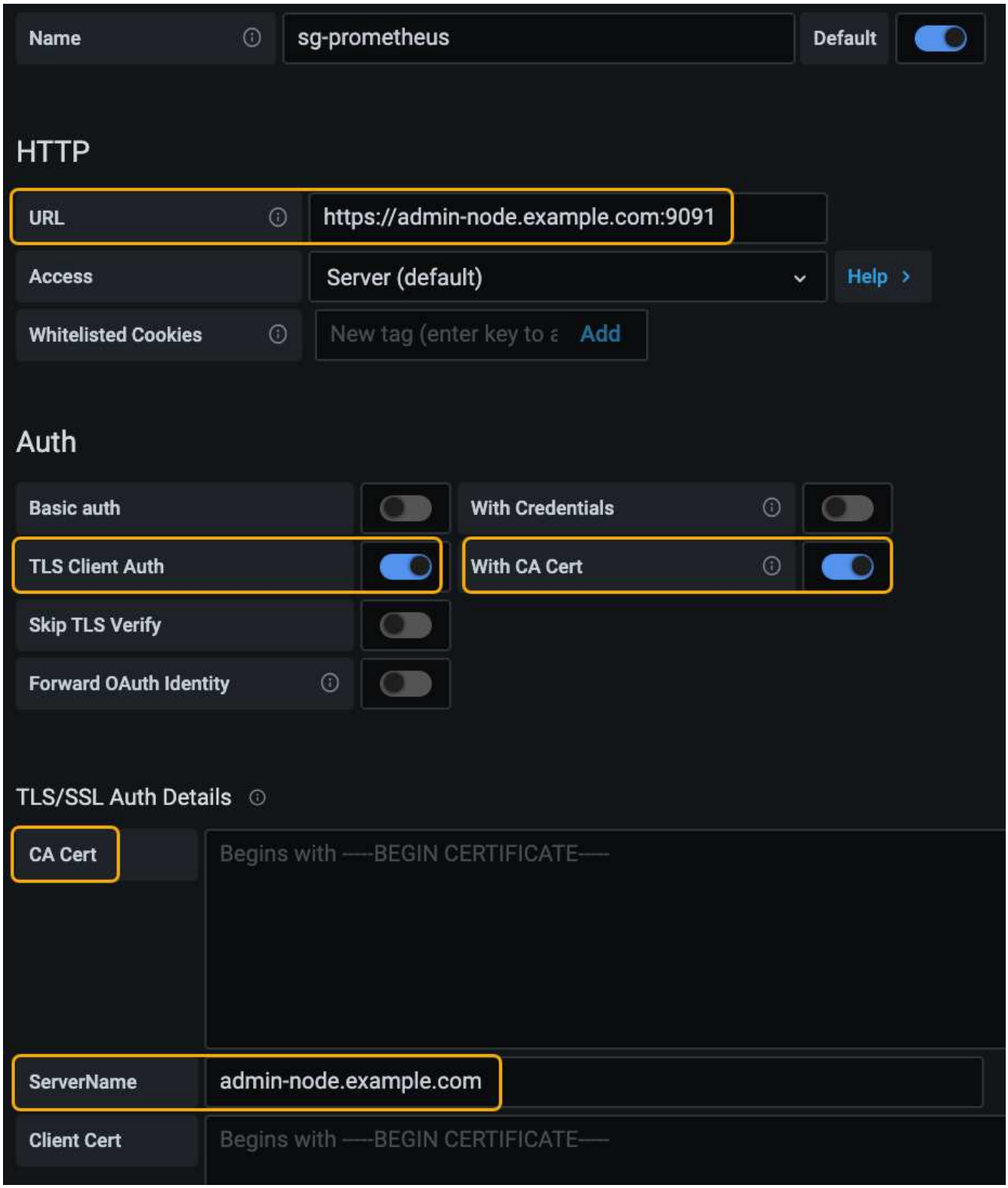
b. Selecione **Copie a chave privada para a área de transferência** e cole a chave na ferramenta de monitoramento externa.

> Não será possível visualizar a chave privada depois de fechar a caixa de diálogo. Copie a chave para um local seguro.

c. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.

8. Configure as seguintes configurações em sua ferramenta de monitoramento externo, como Grafana.

   Um exemplo de Grafana é mostrado na seguinte captura de tela:



   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 Authorization** e **with CA Cert**.

d. Copie e cole o certificado do servidor de interface de gerenciamento ou o pacote CA para **CA Cert** em Detalhes de autenticação TLS/SSL.

e. **ServerName**: Insira o nome de domínio do nó Admin.

   O nome do servidor deve corresponder ao nome de domínio como aparece no certificado do servidor de interface de gerenciamento.

f. 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 as instruções para monitoramento e solução de problemas do StorageGRID.

Informações relacionadas

"Usando certificados de segurança do StorageGRID"

"Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"

"Monitorizar Resolução de problemas"

Editando certificados de cliente do administrador

Você pode editar um certificado para alterar seu nome, ativar ou desativar o acesso Prometheus ou carregar um novo certificado quando o atual expirar.

O que você vai precisar

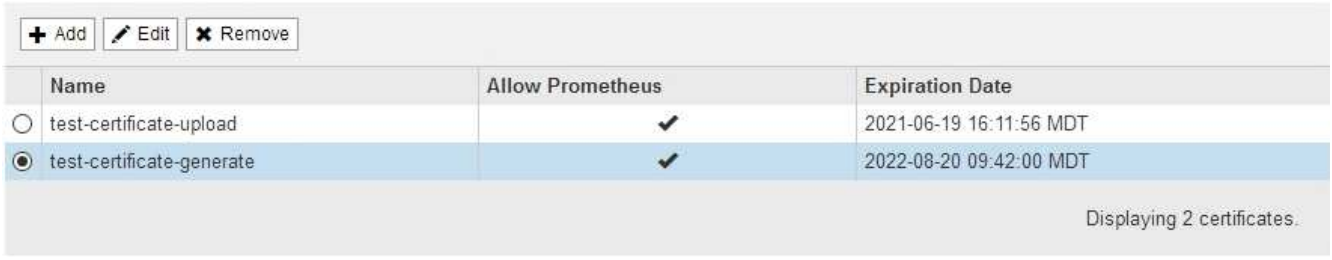
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve saber o endereço IP ou o nome de domínio do nó Admin.
- Se você quiser carregar um novo certificado e uma chave privada, eles devem estar disponíveis no computador local.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

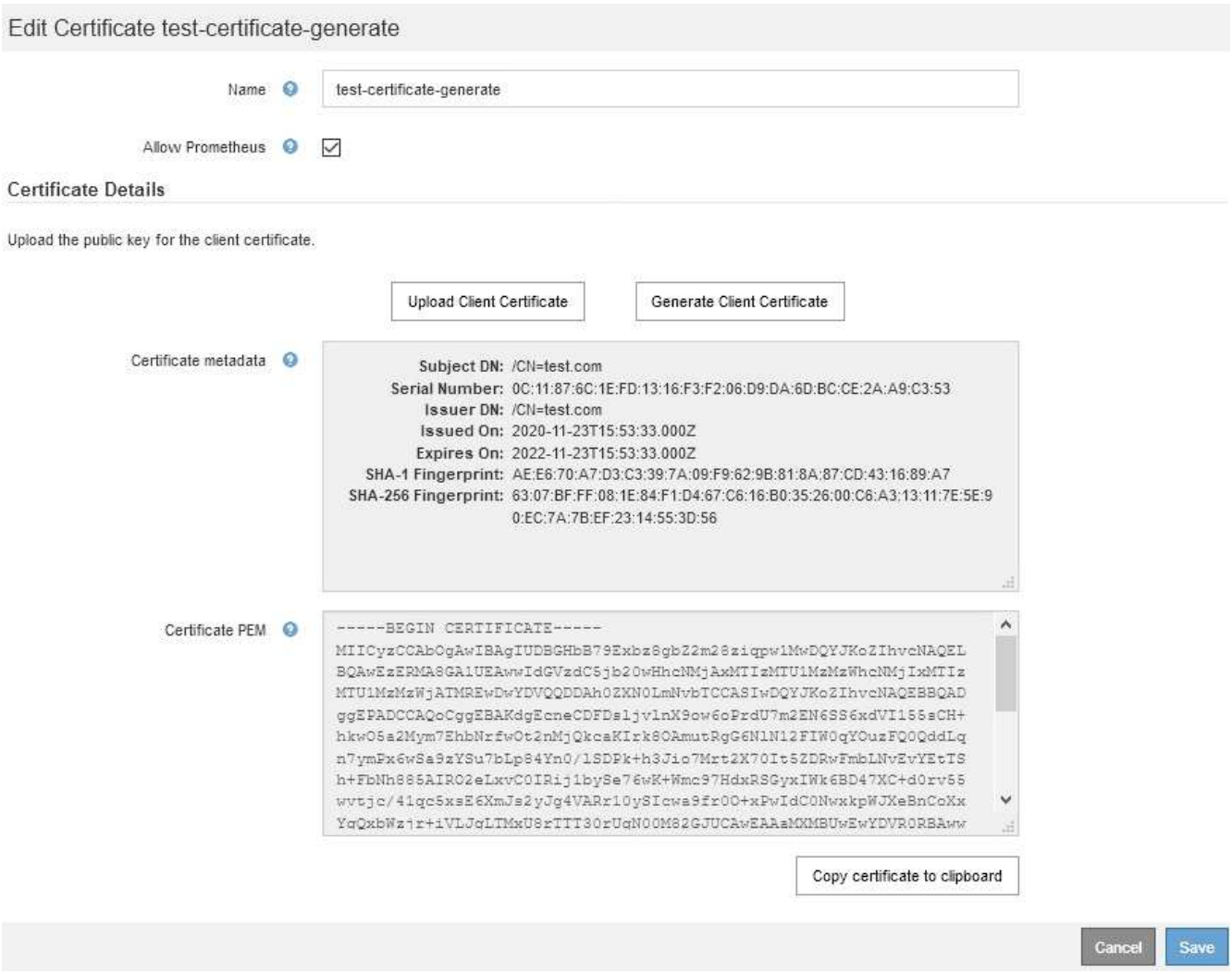
   A página certificados de cliente é exibida. Os certificados existentes são listados.

   As datas de expiração do certificado são 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 botão de opção à esquerda do certificado que deseja editar.
3. Selecione **Editar**.

   A caixa de diálogo Editar certificado é exibida.



4. Faça as alterações desejadas no certificado.
5. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.
6. Se você carregou um novo certificado:
   a. Selecione **Copiar certificado para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.
   b. Use uma ferramenta de edição para copiar e colar a nova chave privada na sua ferramenta de monitoramento externo.

c. Salve e teste o certificado e a chave privada em sua ferramenta de monitoramento externa.

7. Se você gerou um novo certificado:
   a. Selecione **Copiar certificado para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.
   b. Selecione **Copiar chave privada para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.

      Não será possível visualizar ou copiar a chave privada depois de fechar a caixa de diálogo. Copie a chave para um local seguro.

   c. Salve e teste o certificado e a chave privada em sua ferramenta de monitoramento externa.

Removendo certificados de cliente de administrador

Se você não precisar mais de um certificado, você pode removê-lo.

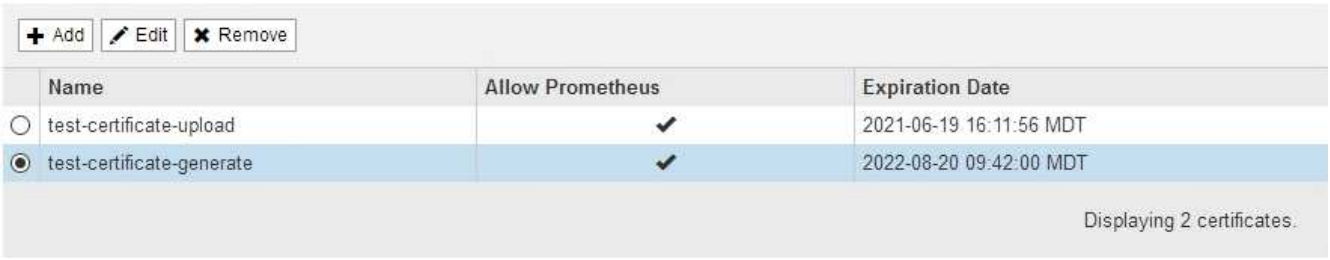
O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

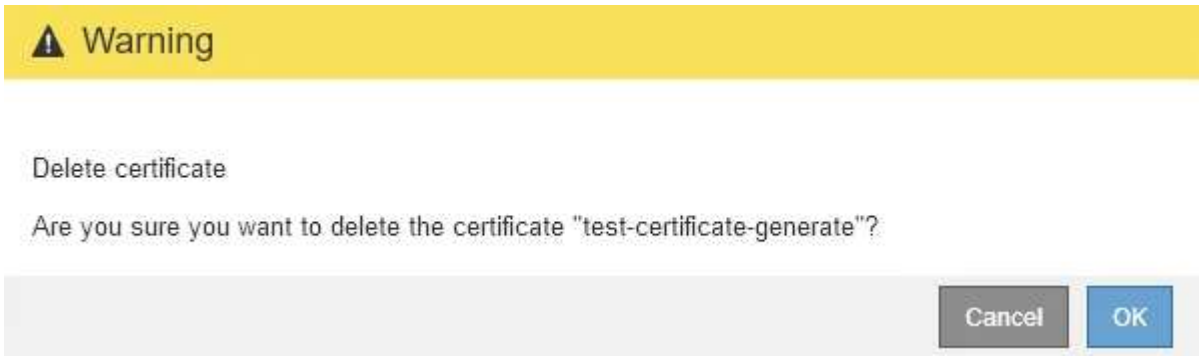
1. Selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

   A página certificados de cliente é exibida. Os certificados existentes são listados.



2. Selecione o botão de opção à esquerda do certificado que deseja remover.
3. Selecione **Remover**.

   É apresentada uma caixa de diálogo de confirmação.



4. Selecione **OK**.

O certificado é removido.

Configurando servidores de gerenciamento de chaves

Você pode configurar um ou mais servidores de gerenciamento de chaves externos (KMS) para proteger os dados em nós de dispositivo especialmente configurados.

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).

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.

Rever os métodos de encriptação StorageGRID

O StorageGRID fornece 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	Configure um servidor de gerenciamento de chaves para o site StorageGRID (**Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**) 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. Pode ser usado com alguns dispositivos de armazenamento e serviços StorageGRID.

Opção de criptografia	Como funciona	Aplica-se a
Conduza a segurança no Gerenciador de sistemas do SANtricity	Se o recurso Segurança da unidade estiver habilitado para um dispositivo de armazenamento, você poderá usar o Gerenciador de sistema do SANtricity 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 FIPS (Federal Information Processing Standard). 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 qualquer dispositivo de serviço. "SG6000 dispositivos de armazenamento" "SG5700 dispositivos de armazenamento" "SG5600 dispositivos de armazenamento"
Opção de grade de criptografia de objetos armazenados	A opção **Stored Object Encryption** pode ser ativada no Grid Manager (**Configuration** > **System Settings** > **Grid Options**). 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 e Swift recém-ingeridos.os objetos armazenados existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados. "Configurando a criptografia de objeto armazenado"
Criptografia de bucket do S3	Você emite uma solicitação de criptografia PUT Bucket para habilitar a criptografia para o bucket. Todos os novos objetos que não são criptografados no nível do objeto são criptografados durante a ingestão.	Apenas dados de objetos S3 recém-ingeridos.a encriptação tem de ser especificada para o intervalo. Os objetos bucket existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados. "Use S3"

Opção de criptografia	Como funciona	Aplica-se a
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 S3"
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 S3"
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.

Opção de criptografia	Como funciona	Aplica-se a
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 desenvolvedor: Protegendo dados usando criptografia do lado do cliente"

Usando vários métodos de criptografia

Dependendo dos seus requisitos, você pode usar mais de um método de criptografia de cada vez. Por exemplo:

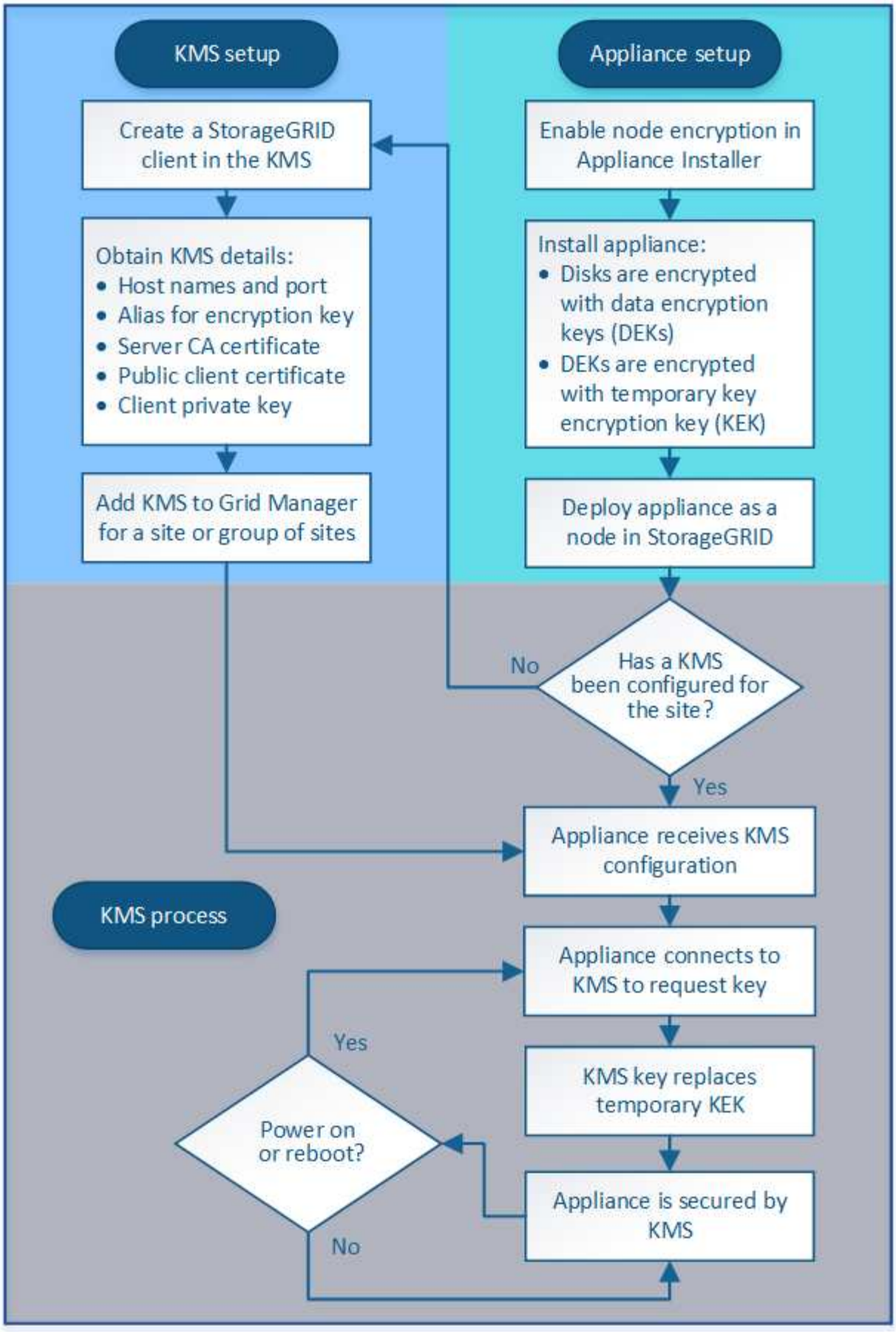
- Você pode usar um KMS para proteger os nós do dispositivo e também usar o recurso de segurança da unidade no Gerenciador de sistema do SANtricity para "criptografar" os dados nas unidades de autocriptografia nos mesmos dispositivos.
- Você pode usar um KMS para proteger dados nos nós do dispositivo e também usar a opção de grade criptografia de objetos armazenados 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.

Visão geral do KMS e da configuração do appliance

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.

Configurando 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.	"Configurando o StorageGRID como um cliente no KMS"
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configurando 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)"

Configurar 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.

Para obter detalhes, consulte o seguinte:

- "Aparelhos de serviços SG100 SG1000"
- "SG6000 dispositivos de armazenamento"
- "SG5700 dispositivos de armazenamento"
- "SG5600 dispositivos de armazenamento"

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.

Quais são os requisitos do KMIP?

O StorageGRID é compatível com KMIP versão 1,4.

"Especificação do protocolo de interoperabilidade de gerenciamento de chaves versão 1,4"

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID é compatível com as seguintes cifras TLS v1,2 para KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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.

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.

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 os seguintes dispositivos e nós de dispositivo StorageGRID:

Aparelho	Tipo de nó
Dispositivo de serviços SG1000	Nó de administração ou nó de gateway
Dispositivo de serviços SG100	Nó de administração ou nó de gateway
SG6000 dispositivo de armazenamento	Nó de storage
SG5700 dispositivo de armazenamento	Nó de storage
SG5600 dispositivo de armazenamento	Nó de storage

Você não pode usar o KMS configurado para nós baseados em software (não-dispositivo), incluindo o seguinte:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados em contentores do Docker 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.

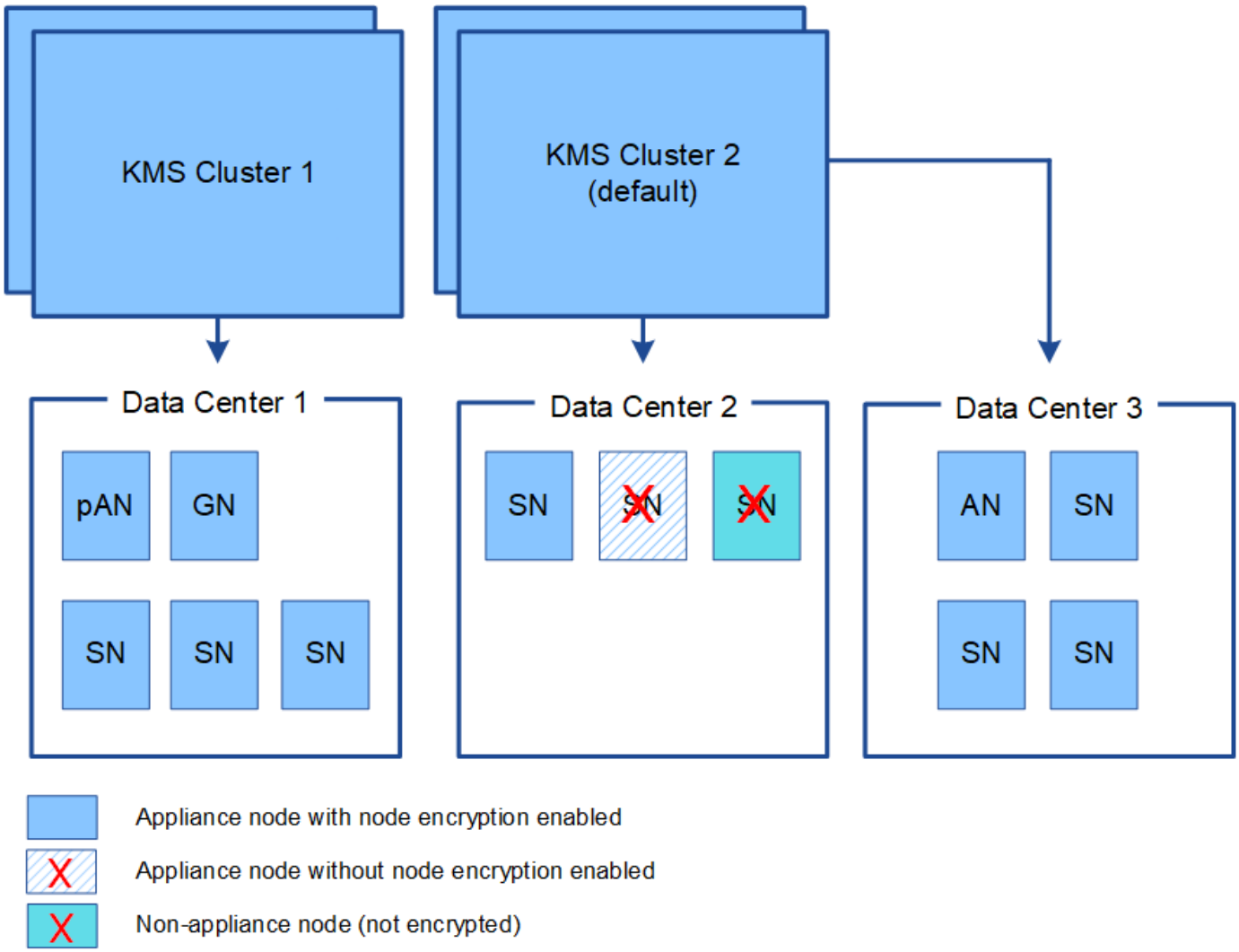
Quantos servidores de gerenciamento de chaves eu preciso?

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 você não pode 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 prática recomendada de segurança, você deve girar periodicamente a chave de criptografia usada por cada KMS configurado.

Ao girar a chave de criptografia, use o software KMS para girar 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 no Gerenciador de Grade. Em vez disso, gire a chave atualizando a versão da chave no software KMS. Use o mesmo alias de chave para novas chaves que foi usado para chaves anteriores. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados.

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** será 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 limpar 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.

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

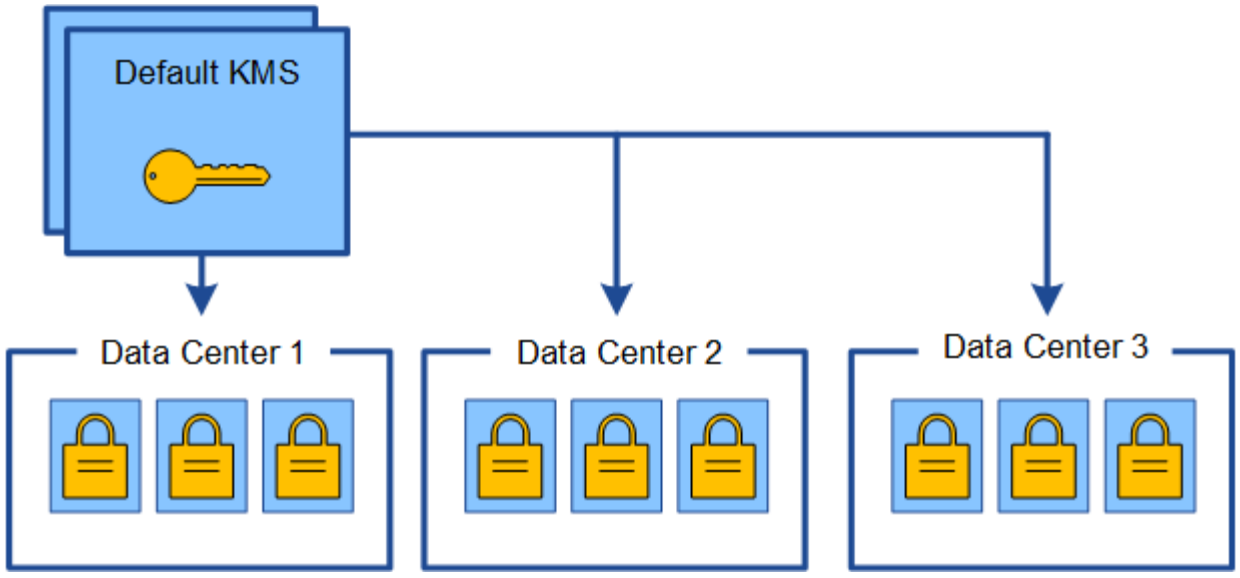
Considerações para alterar o KMS para um site

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.

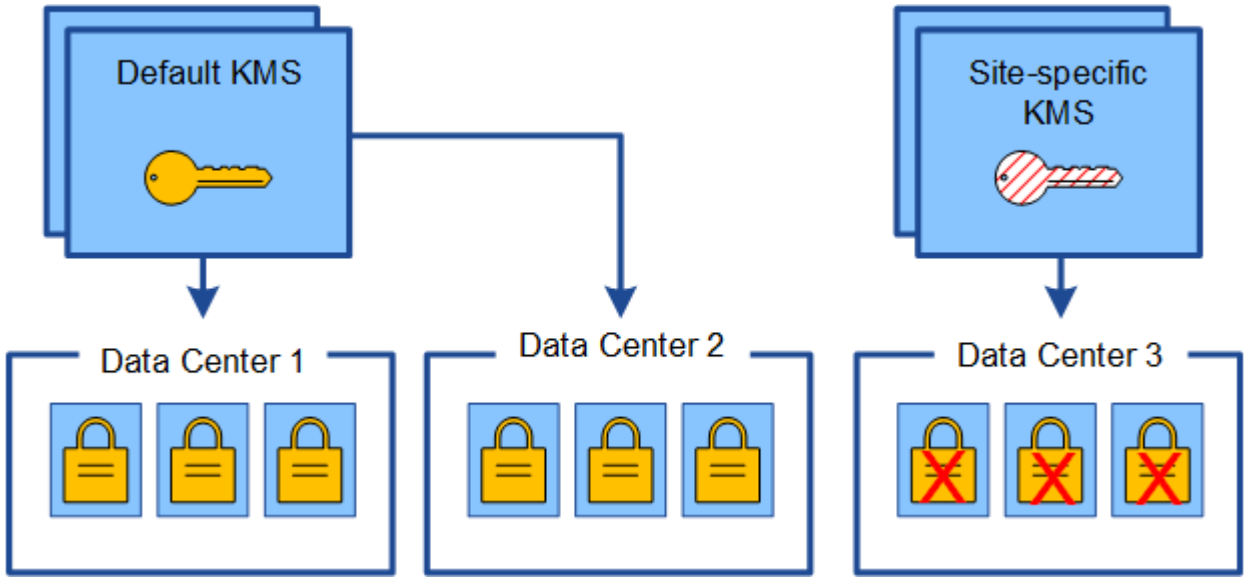
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS. Você deve garantir que o KMS tenha a chave correta para descriptografar os nós de dispositivo criptografado no local.

Por exemplo:

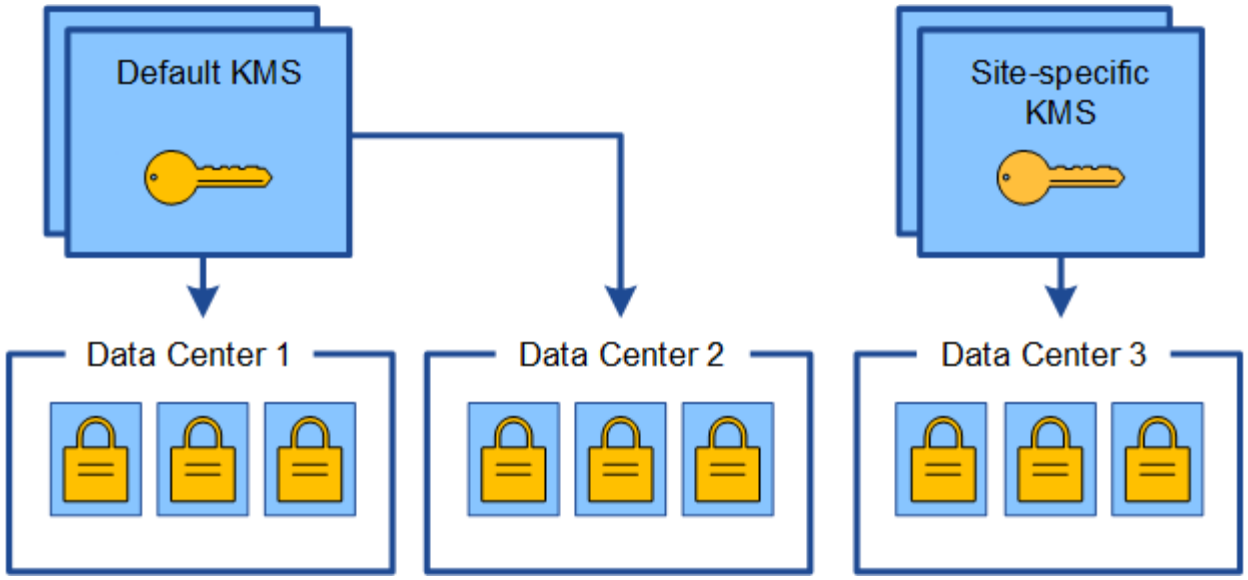
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar 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 deseja 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)"

Caso de uso para alterar o KMS de um site	Passos necessários
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)"

Configurando 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.

Sobre esta tarefa

Estas instruções aplicam-se ao Thales CipherTrust Manager k170v, versões 2,0, 2,1 e 2,2. Se tiver dúvidas sobre o uso de um servidor de gerenciamento de chaves diferente com o StorageGRID, entre em Contato com o suporte técnico.

"Thales CipherTrust Manager"

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. A partir do software KMS, crie uma chave de criptografia AES para cada cluster KMS ou KMS.

   A chave de criptografia precisa ser exportável.

3. Registre as seguintes informações para cada cluster KMS ou KMS.

   Você precisa dessas informações quando você adiciona 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.

   > ⓘ A chave de criptografia já deve existir no KMS. O StorageGRID não cria nem gerencia chaves 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.

Adicionar um servidor de gerenciamento de chaves (KMS)

Você usa o assistente do servidor de gerenciamento de chaves do StorageGRID para adicionar cada cluster KMS ou KMS.

O que você vai precisar

- Tem de ter revisto a "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você deve ter "Configurado o StorageGRID como um cliente no KMS", e você deve ter as informações necessárias para cada cluster KMS ou KMS
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

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"

Passos

1. "Passo 1: Insira os detalhes do KMS"
2. "Passo 2: Carregar certificado de servidor"
3. "Passo 3: Faça o upload de certificados de cliente"

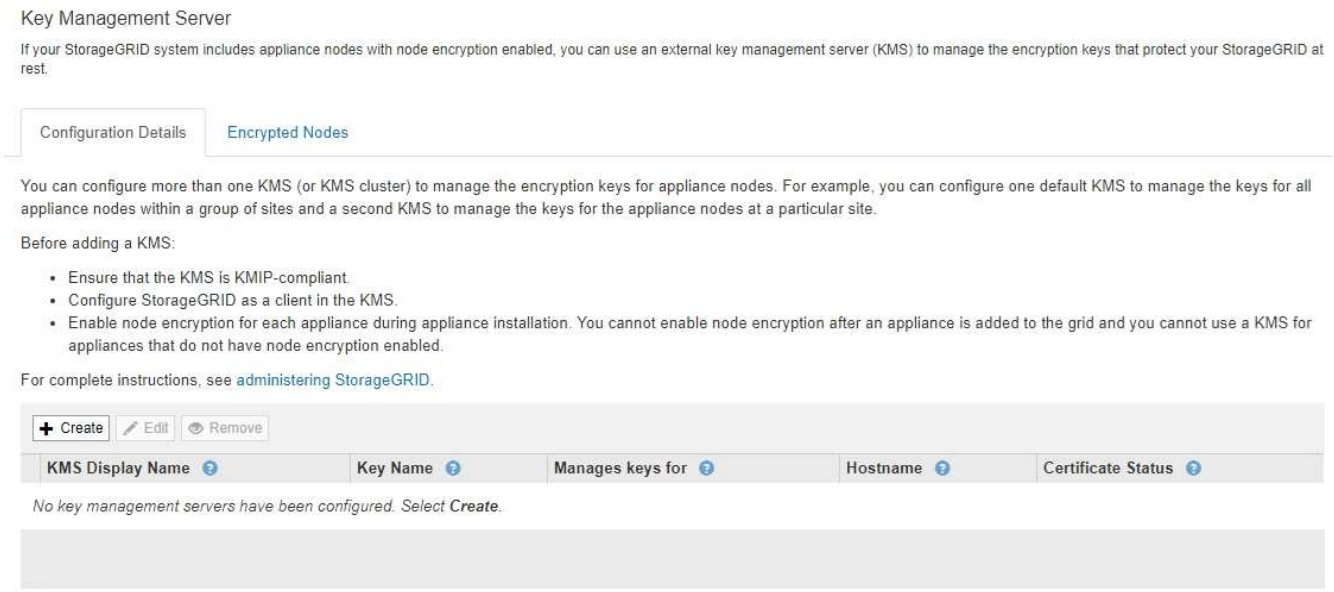
Passo 1: Insira os detalhes do KMS

Na Etapa 1 (Inserir detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves, você fornece detalhes sobre o cluster KMS ou KMS.

Passos

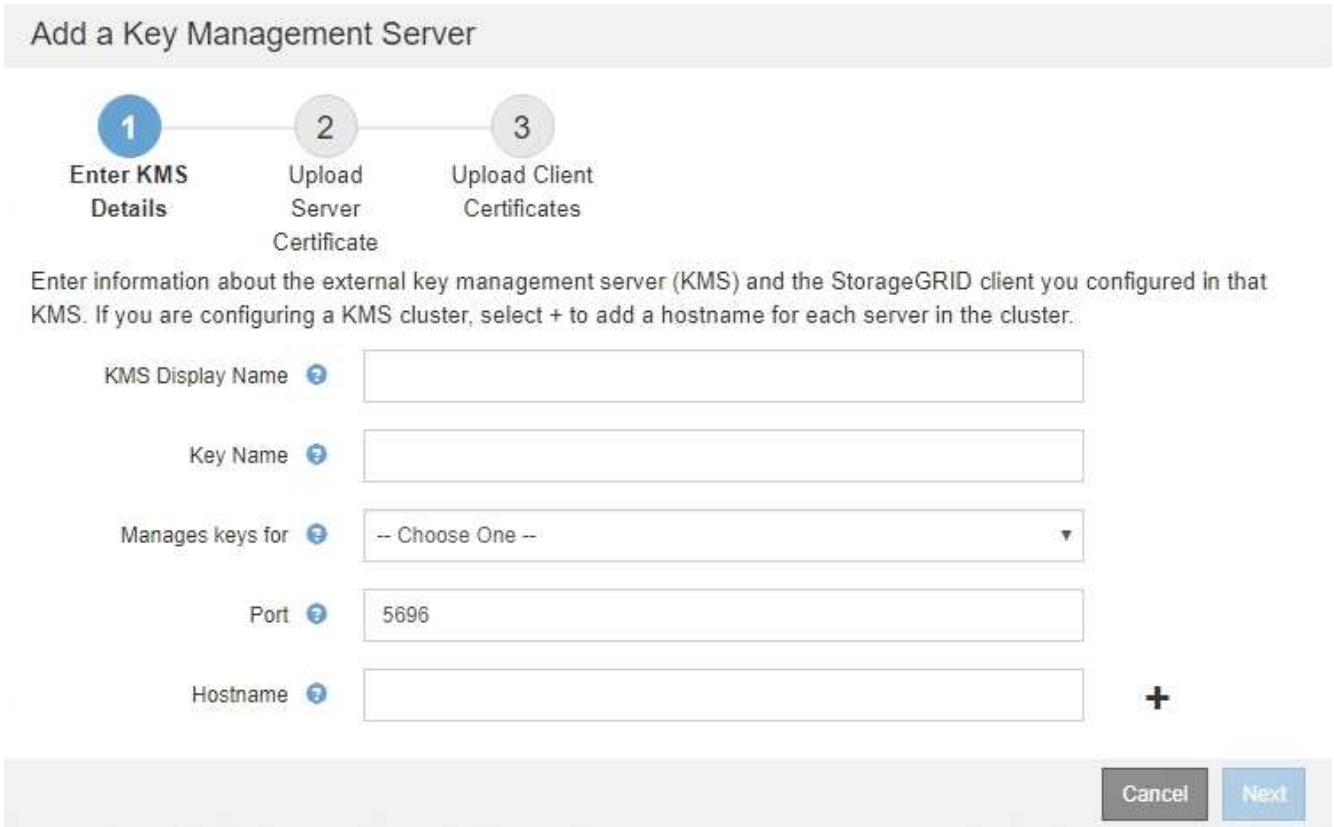
1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida com a guia Configuration Details (Detalhes da configuração) selecionada.



2. Selecione **criar**.

   O passo 1 (Digite os detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves é exibido.



3. Insira as seguintes informações para o KMS e o cliente StorageGRID que você configurou nesse KMS.

Campo	Descrição
Nome de exibição de KMS	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.
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. **Observação:** o campo SAN 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 usando um cluster KMS, selecione o sinal de mais ➕para adicionar um nome de host para cada servidor no cluster.
5. Selecione **seguinte**.

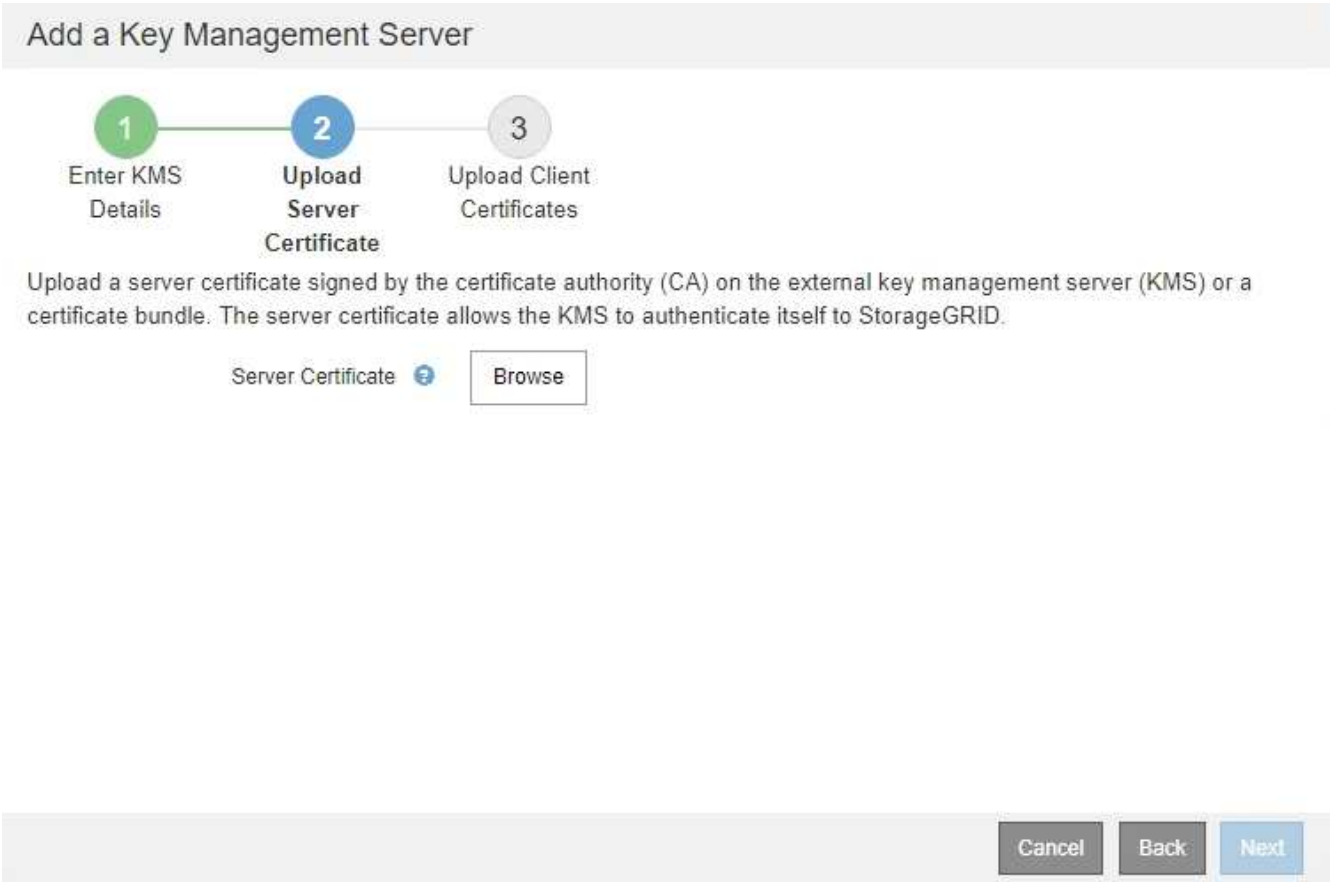
A etapa 2 (carregar certificado do servidor) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

Passo 2: Carregar certificado de 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.

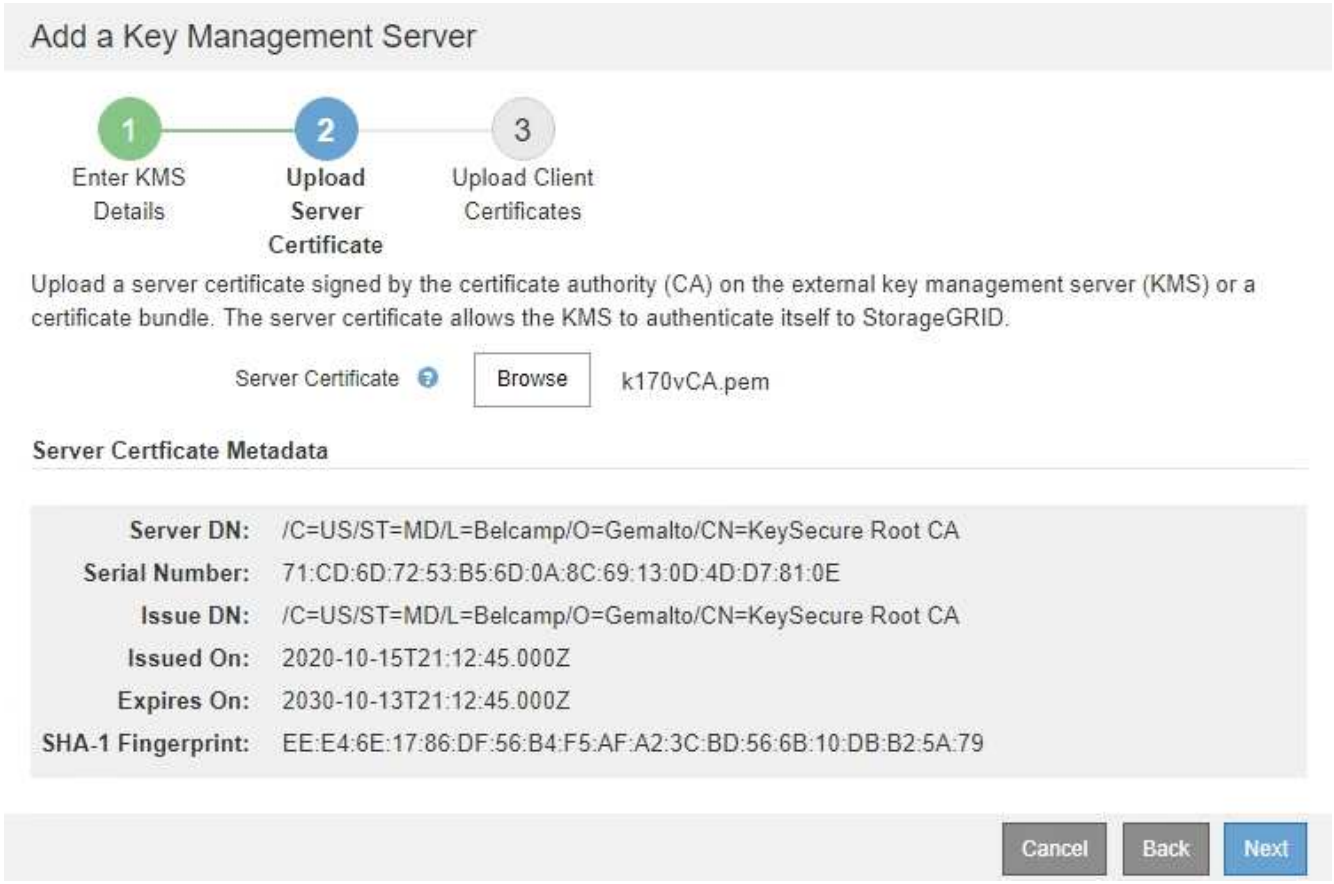
Passos

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 **seguinte**.

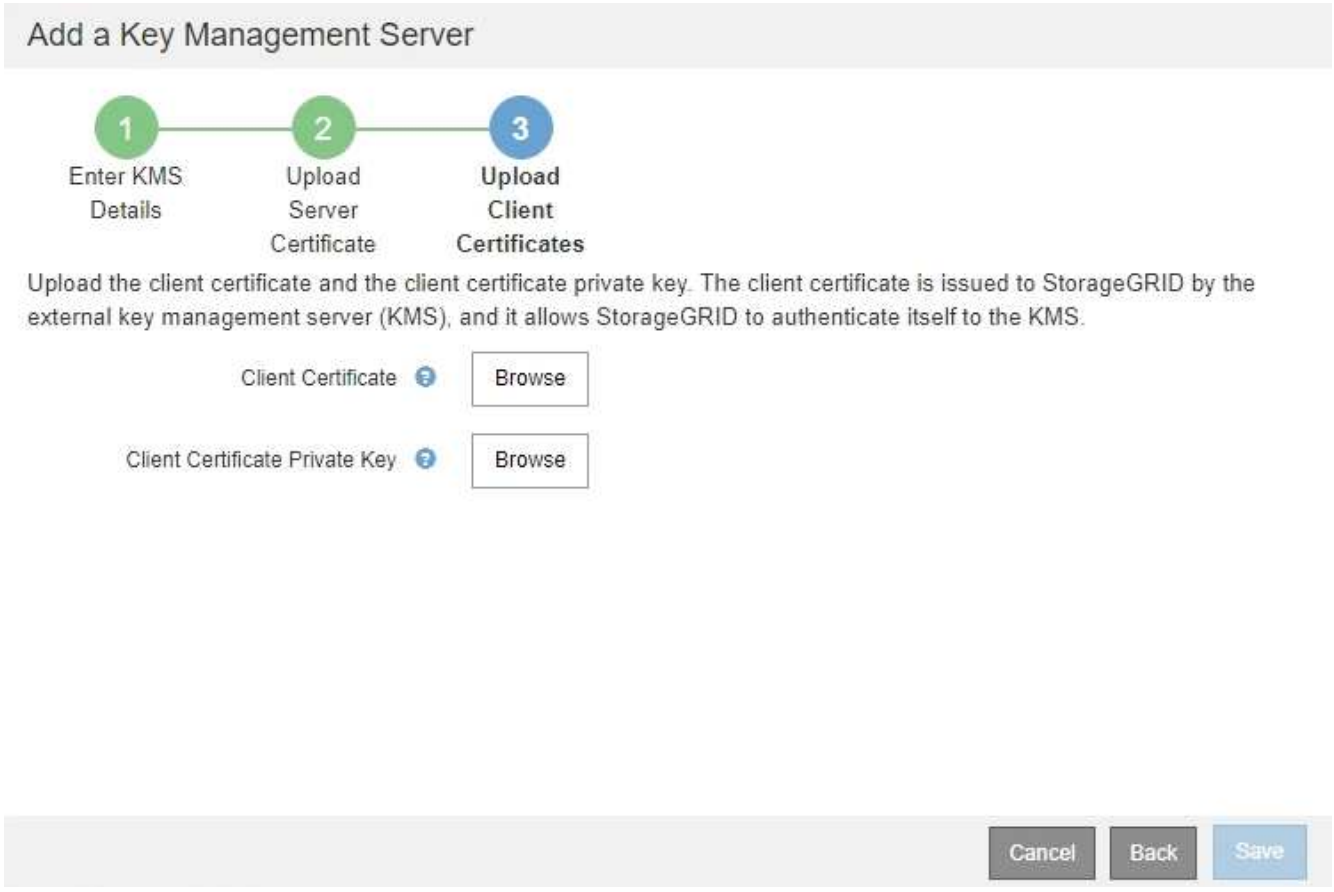
   A etapa 3 (carregar certificados de cliente) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

Passo 3: Faça o upload de 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 do **passo 3 (carregar certificados de cliente)**, navegue até a localização do certificado de cliente.

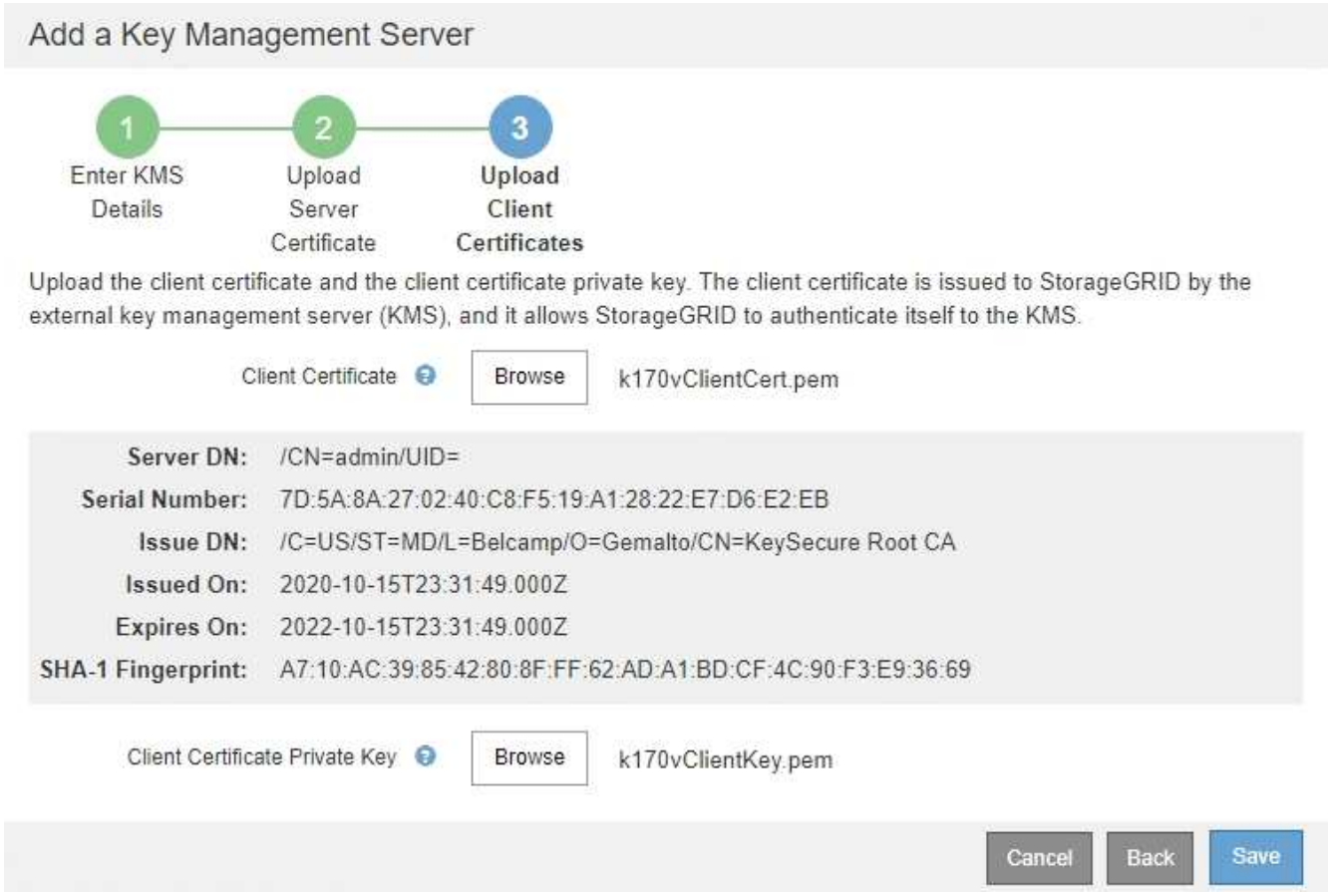


2. Carregue o ficheiro de certificado do cliente.

   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.

   Os metadados do certificado de cliente e da chave privada do certificado de cliente são exibidos.



5. Selecione **Guardar**.

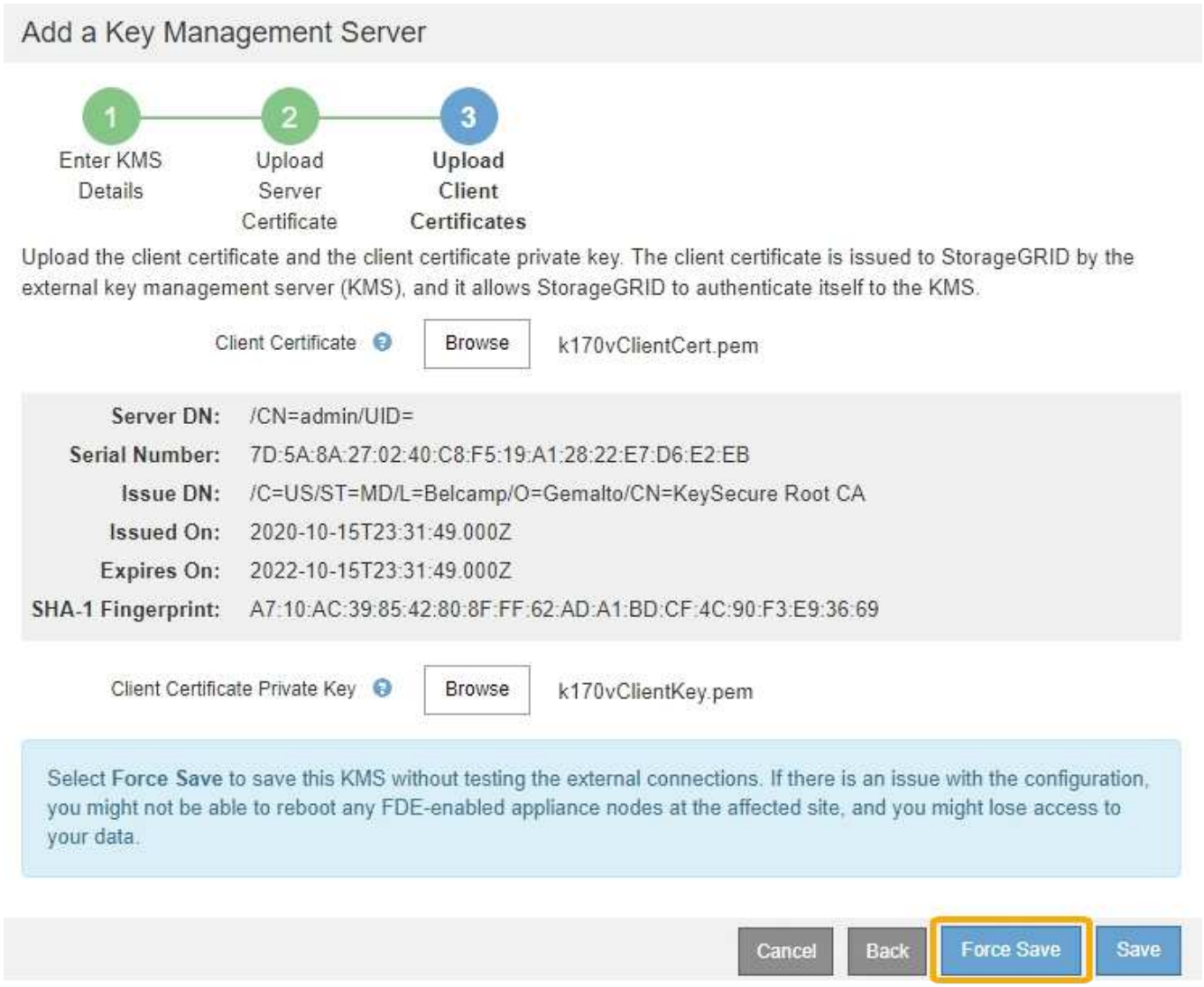
   As conexões entre o servidor de gerenciamento de chaves e os nós do dispositivo são testadas. Se todas as conexões forem válidas e a chave correta for encontrada no KMS, o novo servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.

   > 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 **Salvar**, revise os detalhes da mensagem e selecione **OK**.

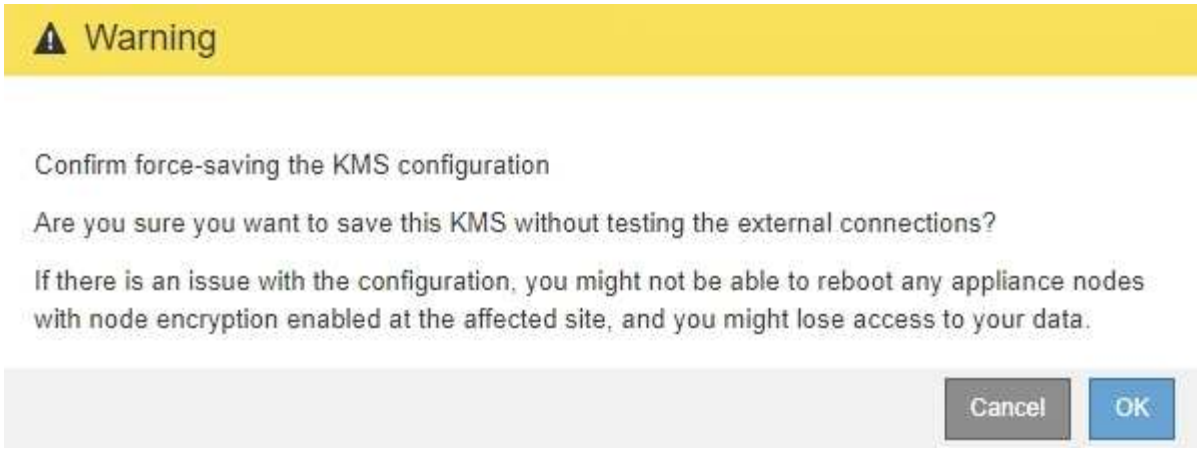
   Por exemplo, você pode receber um erro de entidade 422: Não processável se um teste de conexão falhar.

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.

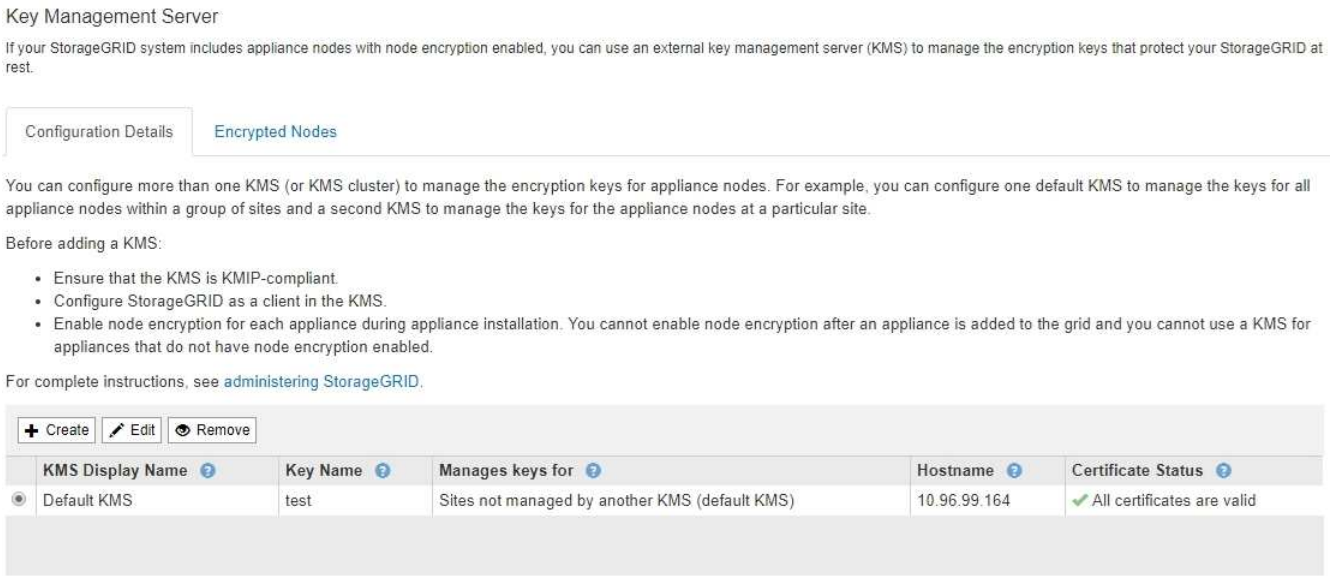
Visualizar detalhes do KMS

Você pode exibir informações sobre cada servidor de gerenciamento de chaves (KMS) em seu sistema StorageGRID, incluindo o status atual do servidor e dos certificados de cliente.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   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 configurados.



2. Reveja as informações na tabela para cada KMS.

Campo	Descrição
Nome de exibição de KMS	O nome descritivo do KMS.

Campo	Descrição
Nome da chave	O alias de chave para o cliente StorageGRID no KMS.
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 exibir todos os nomes de host em um cluster, selecione um KMS e, em seguida, selecione **Editar**.
Estado do certificado	Estado atual do certificado do servidor, do certificado da CA opcional e do certificado do cliente: Válido, expirado, próximo da expiração ou desconhecido. **Nota:** pode demorar StorageGRID até 30 minutos para obter atualizações do status do certificado. Você deve atualizar o navegador da Web para ver os valores atuais.

3. Se o Status do certificado for desconhecido, aguarde até 30 minutos e, em seguida, atualize o navegador da Web.

> 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 real.

4. Se a coluna Status do certificado indicar que um certificado expirou ou está prestes a expirar, solucione o problema o mais rápido possível.

   Consulte as ações recomendadas para os alertas **expiração do certificado KMS CA**, **expiração do**

certificado do cliente KMS e **expiração do certificado do servidor KMS** nas instruções para monitoramento e solução de problemas do StorageGRID.

> Você deve resolver quaisquer problemas de certificado o mais rápido possível para manter o acesso aos dados.

Informações relacionadas

"Monitorizar Resolução de problemas"

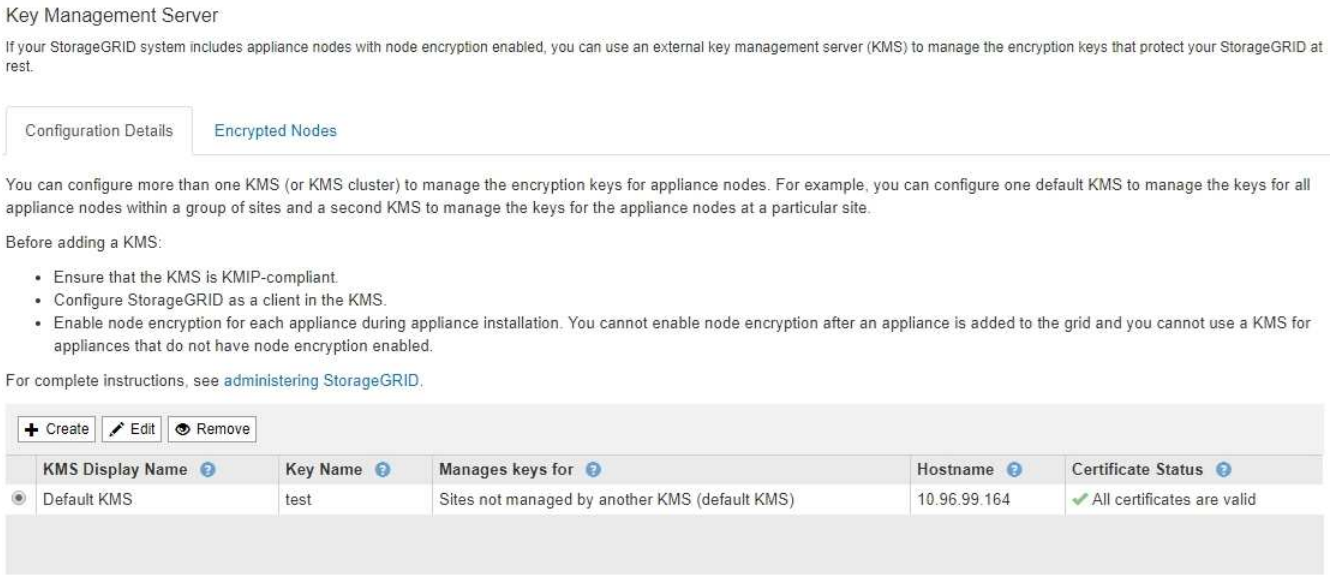
Exibindo nós criptografados

Você pode exibir informações sobre os nós do dispositivo no seu sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

Passos

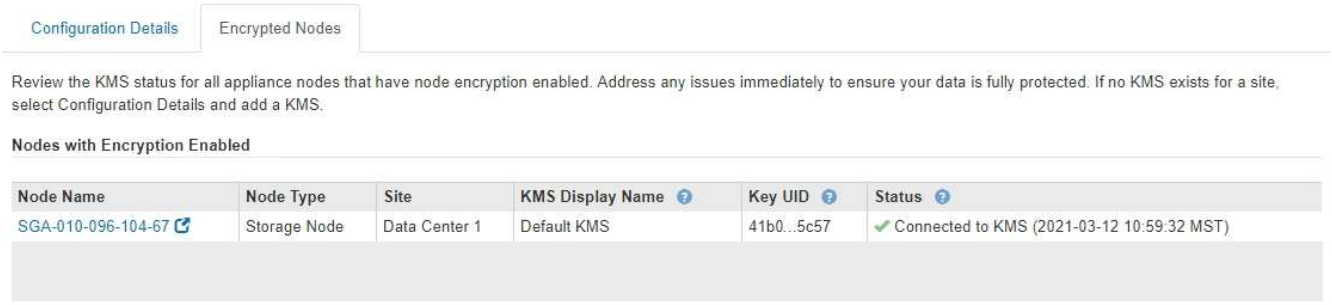
1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   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 nó	O tipo de nó: Storage, Admin ou Gateway.
Local	O nome do site do StorageGRID onde o nó está instalado.
Nome de exibição de KMS	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)"
UID da chave	O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do dispositivo. Para exibir um UID de chave inteiro, passe o cursor sobre a célula. 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:** você deve atualizar 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
- O KMS não está configurado consulte as ações recomendadas para esses alertas nas instruções para monitoramento e solução de problemas do StorageGRID.

> Você deve resolver quaisquer problemas imediatamente para garantir que seus dados estejam totalmente protegidos.

Informações relacionadas

"Monitorizar Resolução de problemas"

Editar um servidor de gerenciamento de chaves (KMS)

Talvez seja necessário editar a configuração de um servidor de gerenciamento de chaves, por exemplo, se um certificado estiver prestes a expirar.

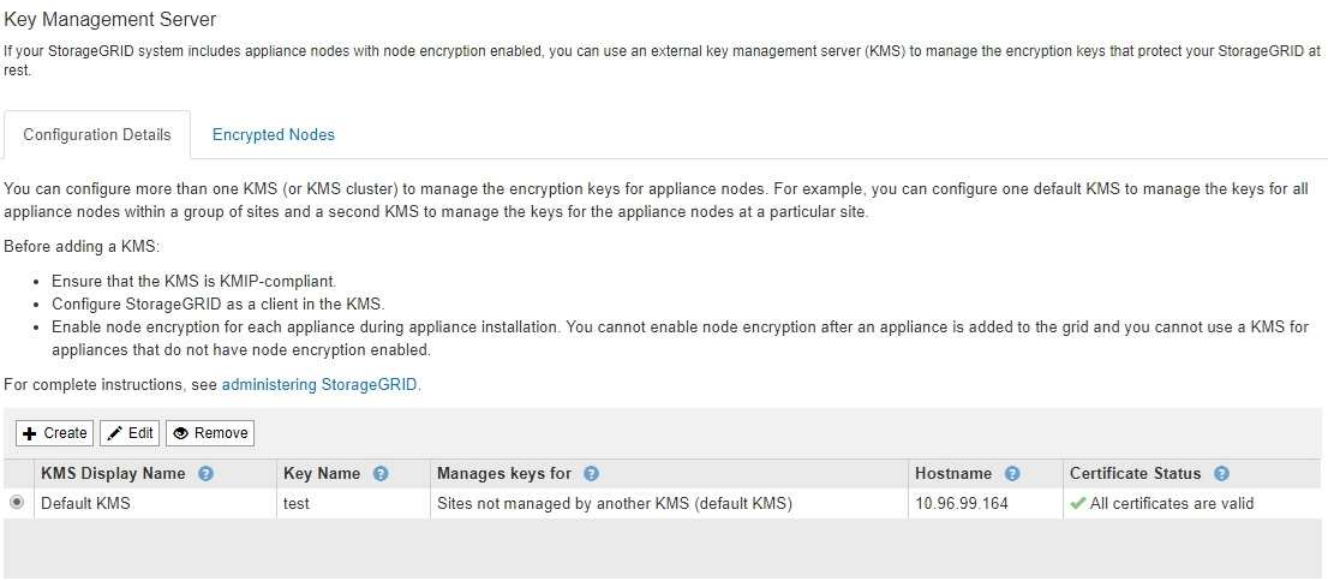
O que você vai precisar

- Tem de ter revisto a "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Se pretende atualizar o local selecionado para um KMS, tem de ter revisto o "Considerações para alterar o KMS para um site".
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   A página Key Management Server (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 **Editar**.
3. Opcionalmente, atualize os detalhes em **Etapa 1 (Inserir detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

Campo	Descrição
Nome de exibição de KMS	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. Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS. Em vez disso, gire a chave atualizando a versão da chave no software 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. "Considerações e requisitos para usar um servidor de gerenciamento de chaves"
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 poderá 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.

Campo	Descrição
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Observação:** o campo SAN 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 o sinal de mais ➕para adicionar um nome de host para cada servidor no cluster.
5. Selecione **seguinte**.

   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 **seguinte**.

   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 **Guardar**.

   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**.

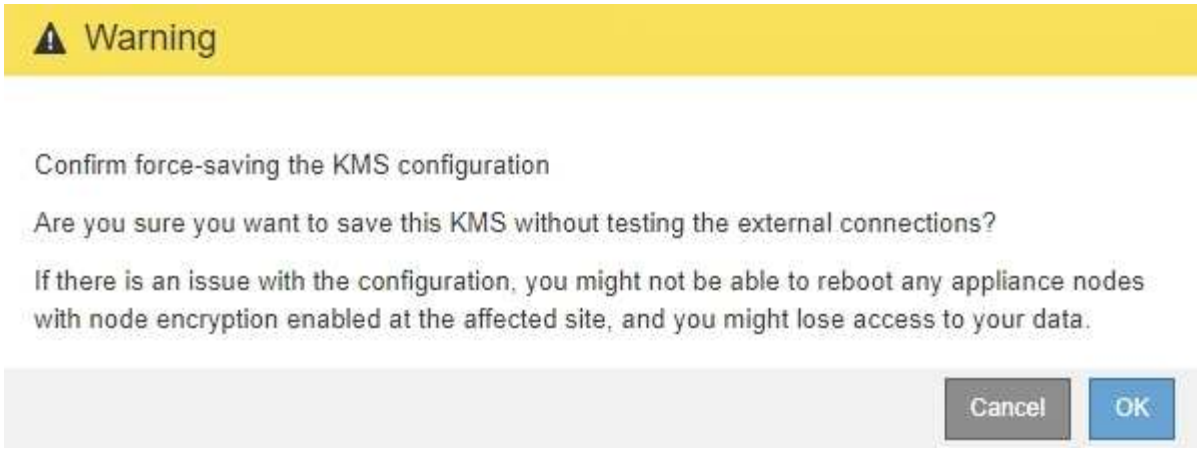
    Por exemplo, você pode receber um erro de entidade 422: Não processável se o site selecionado para este KMS já for gerenciado por outro KMS, ou se um teste de conexão falhou.

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.

O que você vai precisar

- Tem de ter revisto a "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

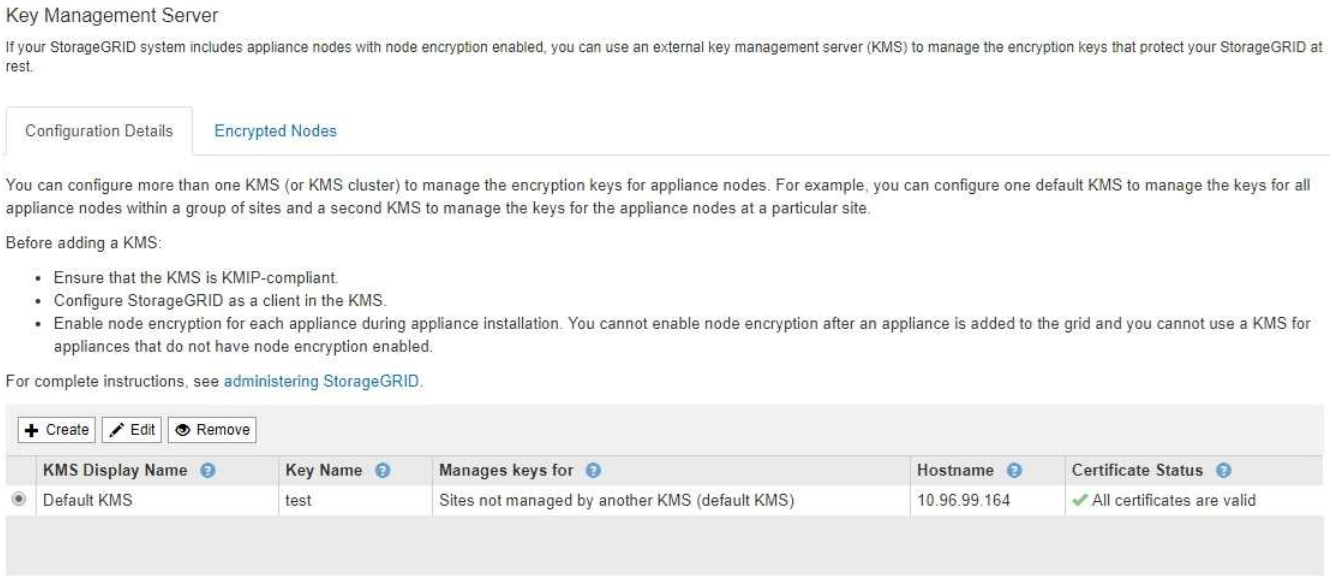
Você pode remover um KMS nestes casos:

- 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.

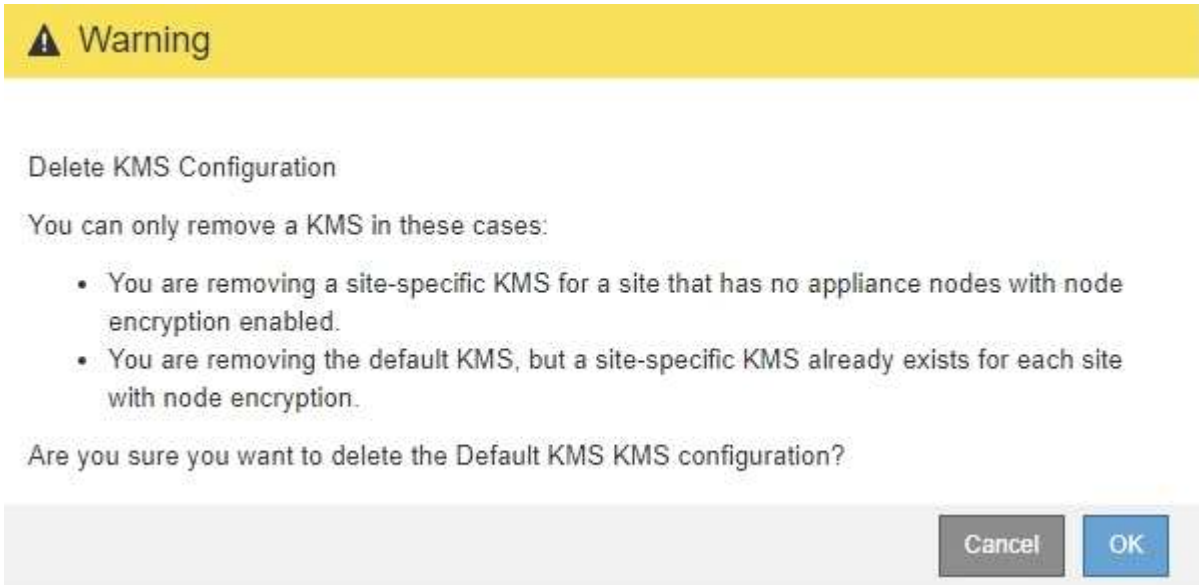
Passos

1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.



2. Selecione o botão de opção para o KMS que deseja remover e selecione **Remover**.
3. Reveja as considerações na caixa de diálogo de aviso.



4. Selecione **OK**.

   A configuração do KMS é removida.

Gerenciamento de locatários

Como administrador de grade, você cria e gerencia as contas de locatário que os clientes S3 e Swift usam para armazenar e recuperar objetos, monitorar o uso do armazenamento e gerenciar as ações que os clientes podem executar usando seu sistema StorageGRID.

Quais são as contas de inquilino

As contas de locatário permitem que aplicativos clientes que usam a API REST do Simple Storage Service (S3) ou a API REST Swift armazenem e recuperem objetos no StorageGRID.

Cada conta de locatário suporta o uso de um único protocolo, que você especifica quando você cria a conta. Para armazenar e recuperar objetos em um sistema StorageGRID com ambos os protocolos, você deve criar duas contas de locatário: Uma para buckets e objetos do S3 e outra para contentores e objetos do Swift. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários autorizados, buckets ou containers e objetos.

Opcionalmente, você pode criar contas de locatário adicionais se quiser segregar os objetos armazenados em seu sistema por diferentes entidades. Por exemplo, você pode configurar várias contas de locatário em 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, você pode simplesmente 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 para implementar aplicativos cliente 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.

Criando e configurando contas de inquilino

Ao criar uma conta de locatário, você especifica as seguintes informações:

- Nome de exibição da conta de locatário.
- Qual protocolo de cliente será usado pela conta de locatário (S3 ou Swift).
- Para contas de locatário do S3: Se a conta de locatário tem permissão para usar serviços de plataforma com buckets do S3. Se você permitir que as contas de inquilino usem serviços de plataforma, você deve garantir que a grade esteja configurada para suportar seu uso. Consulte ""Gerenciando serviços de plataforma.""
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. Se a cota for excedida, o locatário não poderá criar novos objetos.

  > A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).

- Se a federação de identidade estiver ativada para o sistema StorageGRID, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.
- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.

Depois que uma conta de locatário for criada, você poderá executar as seguintes tarefas:

- **Gerenciar serviços de plataforma para a grade**: Se você habilitar serviços de plataforma para contas de locatários, certifique-se de entender como as mensagens de serviços de plataforma são entregues e os requisitos de rede que o uso de serviços de plataforma coloca na implantação do StorageGRID.
- **Monitorar o uso de armazenamento de uma conta de locatário**: Depois que os locatários começam a usar suas contas, você pode usar o Grid Manager para monitorar quanto armazenamento cada locatário consome.

  Se você tiver definido cotas para locatários, poderá ativar o alerta **uso alto da cota do locatário** para determinar se os locatários estão consumindo suas cotas. Se ativado, esse alerta é acionado quando um locatário usou 90% de sua cota. Para obter mais informações, consulte a referência de alertas nas instruções para monitoramento e solução de problemas do StorageGRID.

- **Configurar operações do cliente**: Você pode configurar se alguns tipos de operações do cliente são proibidos.

Configurando S3 locatários

Depois que uma conta de locatário do S3 for criada, os usuários do locatário poderão acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e criando grupos e usuários locais
- Gerenciando chaves de acesso S3
- Criação e gerenciamento de buckets do S3
- Monitoramento do uso do storage
- Usando serviços de plataforma (se ativado)

> Os usuários de locatários do S3 podem criar e gerenciar chaves de acesso do S3 e buckets com o Gerenciador de locatários, mas devem usar um aplicativo cliente do S3 para obter e gerenciar objetos.

Configurando os locatários Swift

Depois que uma conta de locatário Swift for criada, o usuário raiz do locatário poderá acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e criando grupos e usuários locais
- Monitoramento do uso do storage

> Os usuários Swift devem ter a permissão de acesso root para acessar o Gerenciador do locatário. No entanto, a permissão de acesso root não permite que os usuários se autentiquem na API REST do Swift para criar contentores e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

Informações relacionadas

"Use uma conta de locatário"

Criando uma conta de locatário

Você deve criar pelo menos uma conta de locatário para controlar o acesso ao storage no sistema StorageGRID.

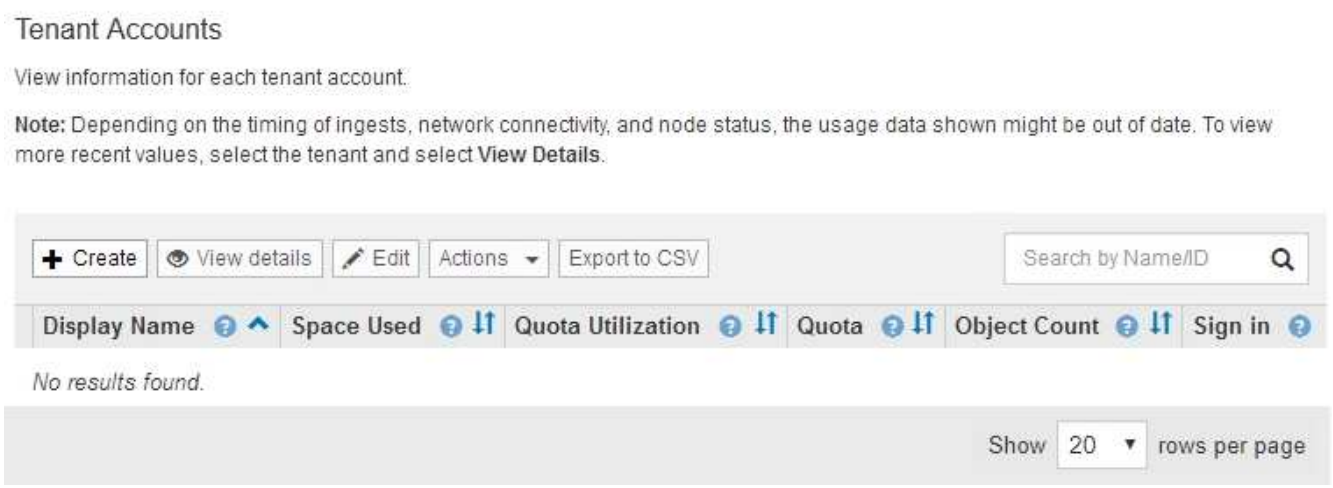
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **tenants**.

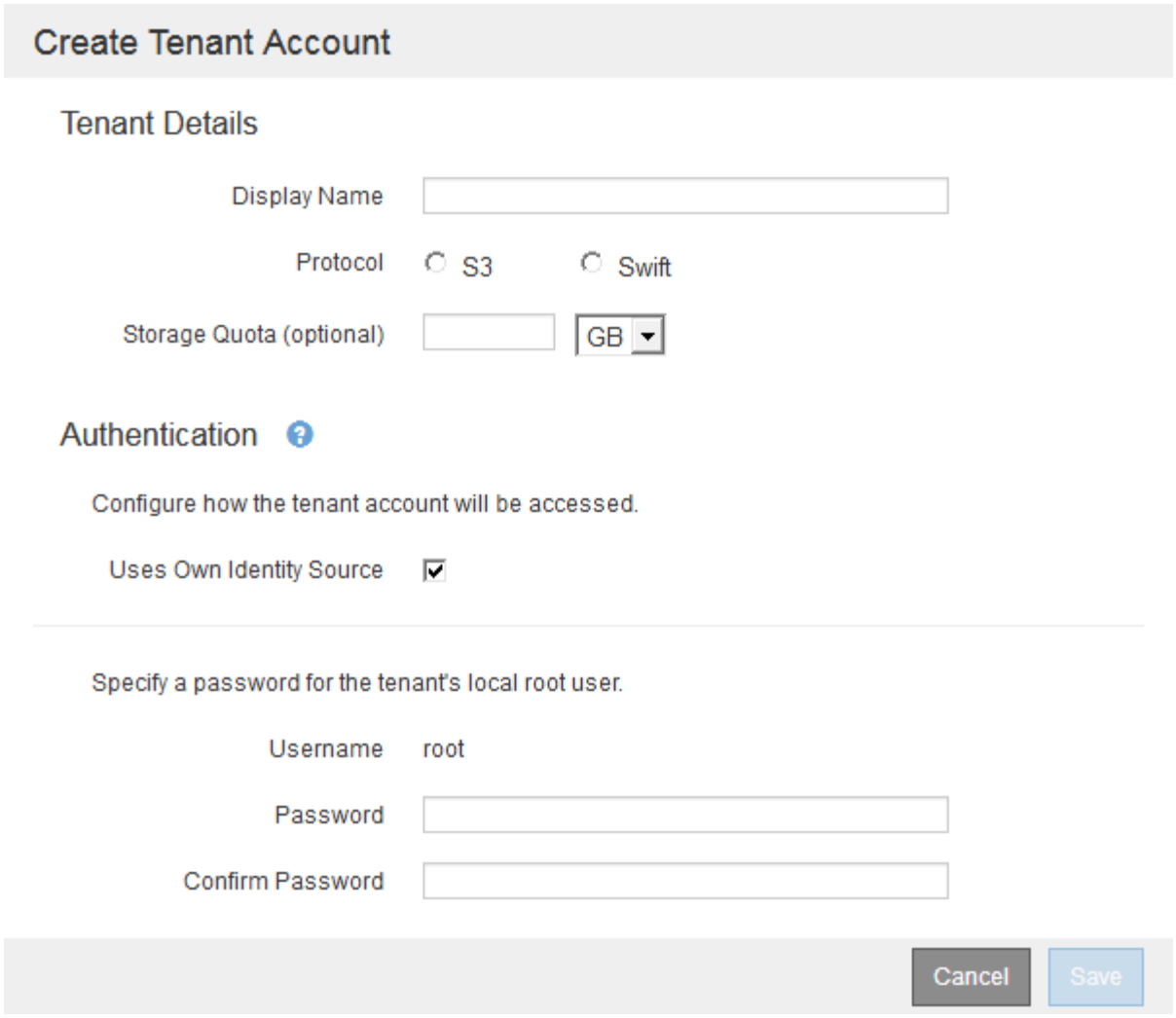
   A página Contas do locatário é exibida e lista todas as contas de locatário existentes.



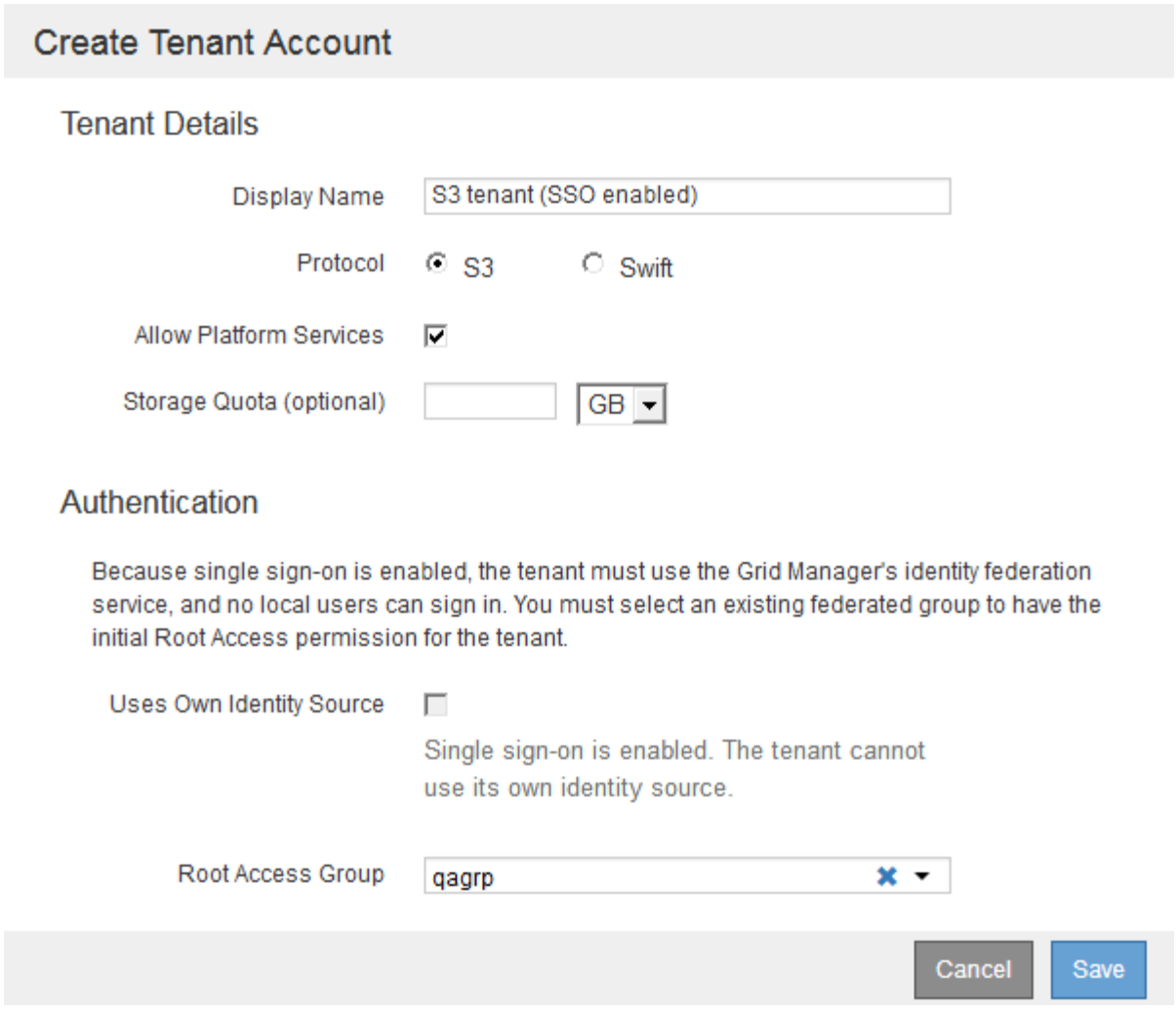
2. Selecione **criar**.

   A página criar conta de locatário é exibida. Os campos incluídos na página dependem se o logon único (SSO) foi ativado para o sistema StorageGRID.

   - Se o SSO não estiver sendo usado, a página criar conta do locatário será assim.



- Se o SSO estiver ativado, a página criar conta do locatário será assim.



Informações relacionadas

"Usando a federação de identidade"

"Configurando logon único"

Criando uma conta de locatário se o StorageGRID não estiver usando SSO

Quando você cria uma conta de locatário, você especifica um nome, um protocolo de cliente e, opcionalmente, uma cota de armazenamento. Se o StorageGRID não estiver usando logon único (SSO), você também deve especificar se a conta de locatário usará sua própria origem de identidade e configurar a senha inicial para o usuário raiz local do locatário.

Sobre esta tarefa

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 deve ter importado esse grupo federado para o Gerenciador de Grade. Você não precisa atribuir nenhuma permissão do Gerenciador de Grade a esse grupo de administradores. Consulte as instruções para "gerenciando grupos de administradores".

Passos

1. Na caixa de texto **Nome de exibição**, insira um nome de exibição para essa conta de locatário.

   Os nomes de exibição não precisam ser exclusivos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.

2. Selecione o protocolo de cliente que será usado por esta conta de locatário, seja **S3** ou **Swift**.
3. Para contas de locatário do S3, mantenha a caixa de seleção **permitir Serviços de Plataforma** selecionada, a menos que você não queira que esse locatário use serviços de plataforma para buckets do S3.

   Se os serviços de plataforma estiverem ativados, um locatário poderá usar recursos, como a replicação do CloudMirror, que acessam serviços externos. Talvez você queira desativar o uso desses recursos para limitar a quantidade de largura de banda da rede ou outros recursos que um locatário consome. Consulte ""Gerenciando serviços de plataforma.""

4. Na caixa de texto **cota de armazenamento**, insira opcionalmente o número máximo de gigabytes, terabytes ou petabytes que você deseja disponibilizar para os objetos desse locatário. Em seguida, selecione as unidades na lista suspensa.

   Deixe esse campo em branco se você quiser que esse locatário tenha uma cota ilimitada.

   > A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco). As cópias ILM e a codificação de apagamento não contribuem para a quantidade de cota usada. Se a cota for excedida, a conta de locatário não poderá criar novos objetos.

   > Para monitorar o uso de armazenamento de cada conta de locatário, selecione **uso**. As contas de locatário também podem monitorar seu próprio uso de storage no Dashboard no Gerenciador do locatário ou com a API de gerenciamento do locatário. Observe que os valores de uso de storage de um locatário podem ficar desatualizados se os nós forem isolados de outros nós na grade. Os totais serão atualizados quando a conetividade de rede for restaurada.

5. Se o locatário gerenciar seus próprios grupos e usuários, siga estas etapas.
   a. Marque a caixa de seleção **usa a própria fonte de identidade** (padrão).

      > Se esta caixa de verificação estiver selecionada e pretender utilizar a federação de identidade para grupos de inquilinos e utilizadores, o inquilino tem de configurar a sua própria origem de identidade. Consulte as instruções para usar contas de locatário.

   b. Especifique uma senha para o usuário raiz local do locatário.
6. Se o locatário usar os grupos e usuários configurados para o Gerenciador de Grade, siga estas etapas.
   a. Desmarque a caixa de seleção **usa a própria fonte de identidade**.
   b. Faça um ou ambos os procedimentos a seguir:
      - No campo Grupo de Acesso raiz, selecione um grupo federado existente no Gerenciador de Grade que deve ter a permissão de acesso raiz inicial para o locatário.

        > Se você tiver permissões adequadas, os grupos federados existentes do Gerenciador de Grade serão listados quando você clicar no campo. Caso contrário, introduza o nome exclusivo do grupo.

- Especifique uma senha para o usuário raiz local do locatário.

7. Clique em **Salvar**.

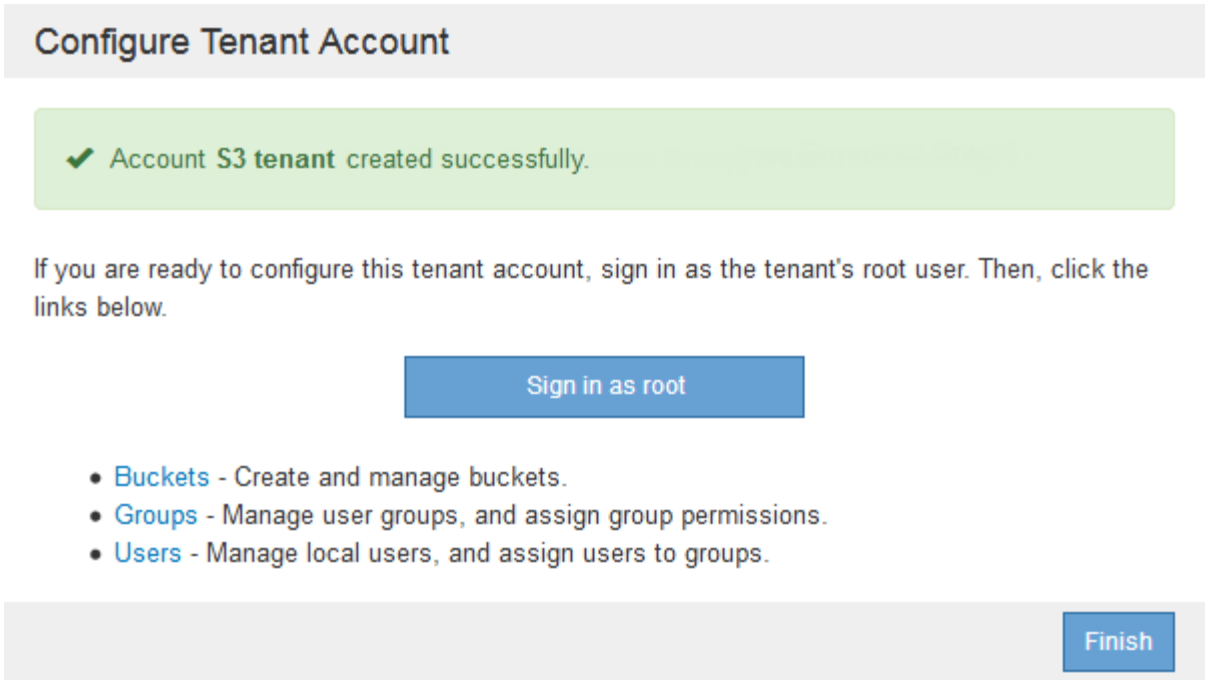
   A conta de locatário é criada.

8. Opcionalmente, acesse o novo locatário. Caso contrário, vá para a etapa acessando o locatário mais tardede .

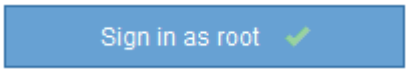
Se você é…	Faça isso…
Acessando o Gerenciador de Grade em uma porta restrita	Clique em **restrito** para saber mais sobre como acessar essa conta de locatário. O URL do Gerenciador do Locatário tem este formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *FQDN_or_Admin_Node_IP* 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
Acessando o Gerenciador de Grade na porta 443, mas você não definiu uma senha para o usuário raiz local	Clique em **entrar** e insira as credenciais de um usuário no grupo federado de acesso root.
Acessando o Gerenciador de Grade na porta 443 e você define uma senha para o usuário raiz local	Vá para a próxima etapa para faça login como root.

9. Faça login no locatário como root:

   a. Na caixa de diálogo Configurar conta de locatário, clique no botão **entrar como root**.



Uma marca de seleção verde aparece no botão, indicando que você agora está conetado à conta de locatário como usuário raiz.



a. Clique nos links para configurar a conta de locatário.

   Cada link abre a página correspondente no Gerenciador do Locatário. Para concluir a página, consulte as instruções para usar contas de locatário.

b. Clique em **Finish**.

10. para acessar o locatário mais tarde:

Se você estiver usando…	Faça um destes…
Porta 443	• No Gerenciador de Grade, selecione **tenants** e clique em **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

Se você estiver usando…	Faça um destes…
Uma porta restrita	• No Gerenciador de Grade, selecione **tenants** e clique em **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

Informações relacionadas

"Controlar o acesso através de firewalls"

"Gerenciamento de serviços de plataforma para contas de locatários do S3"

"Use uma conta de locatário"

Criando uma conta de locatário se o SSO estiver habilitado

Quando você cria uma conta de locatário, você especifica um nome, um protocolo de cliente e, opcionalmente, uma cota de armazenamento. Se o logon único (SSO) estiver ativado para o StorageGRID, você também especificará qual grupo federado tem permissão de acesso root para configurar a conta de locatário.

Passos

1. Na caixa de texto **Nome de exibição**, insira um nome de exibição para essa conta de locatário.

   Os nomes de exibição não precisam ser exclusivos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.

2. Selecione o protocolo de cliente que será usado por esta conta de locatário, seja **S3** ou **Swift**.
3. Para contas de locatário do S3, mantenha a caixa de seleção **permitir Serviços de Plataforma** selecionada, a menos que você não queira que esse locatário use serviços de plataforma para buckets do S3.

   Se os serviços de plataforma estiverem ativados, um locatário poderá usar recursos, como a replicação do CloudMirror, que acessam serviços externos. Talvez você queira desativar o uso desses recursos para limitar a quantidade de largura de banda da rede ou outros recursos que um locatário consome. Consulte ""Gerenciando serviços de plataforma.""

4. Na caixa de texto **cota de armazenamento**, insira opcionalmente o número máximo de gigabytes, terabytes ou petabytes que você deseja disponibilizar para os objetos desse locatário. Em seguida, selecione as unidades na lista suspensa.

Deixe esse campo em branco se você quiser que esse locatário tenha uma cota ilimitada.

> A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco). As cópias ILM e a codificação de apagamento não contribuem para a quantidade de cota usada. Se a cota for excedida, a conta de locatário não poderá criar novos objetos.

> Para monitorar o uso de armazenamento de cada conta de locatário, selecione **uso**. As contas de locatário também podem monitorar seu próprio uso de storage no Dashboard no Gerenciador do locatário ou com a API de gerenciamento do locatário. Observe que os valores de uso de storage de um locatário podem ficar desatualizados se os nós forem isolados de outros nós na grade. Os totais serão atualizados quando a conetividade de rede for restaurada.

5. Observe que a caixa de seleção **usa a própria fonte de identidade** está desmarcada e desativada.

   Como o SSO está habilitado, o locatário deve usar a origem de identidade que foi configurada para o Gerenciador de Grade. Nenhum usuário local pode entrar.

6. No campo **Root Access Group**, selecione um grupo federado existente no Gerenciador de Grade para ter a permissão de acesso raiz inicial para o locatário.

   > Se você tiver permissões adequadas, os grupos federados existentes do Gerenciador de Grade serão listados quando você clicar no campo. Caso contrário, introduza o nome exclusivo do grupo.

7. Clique em **Salvar**.

   A conta de locatário é criada. A página Contas do locatário é exibida e inclui uma linha para o novo locatário.

8. Se você for um usuário no grupo de acesso root, opcionalmente clique no link **entrar** para que o novo locatário acesse imediatamente o Gerenciador de Locatário, onde você pode configurar o locatário. Caso contrário, forneça o URL do link **entrar** para o administrador da conta do locatário. (O URL de um locatário é o nome de domínio totalmente qualificado ou o endereço IP de qualquer nó Admin, seguido de `/?accountId=`*`20-digit-account-id`*.)

   > Uma mensagem de acesso negado será exibida se você clicar em **entrar**, mas você não pertencer ao grupo de acesso raiz da conta de locatário.

Informações relacionadas

"Configurando logon único"

"Gerenciamento de serviços de plataforma para contas de locatários do S3"

"Use uma conta de locatário"

Alterando a senha do usuário raiz local de um locatário

Talvez seja necessário alterar a senha do usuário raiz local de um locatário se o usuário raiz estiver bloqueado para fora da conta.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

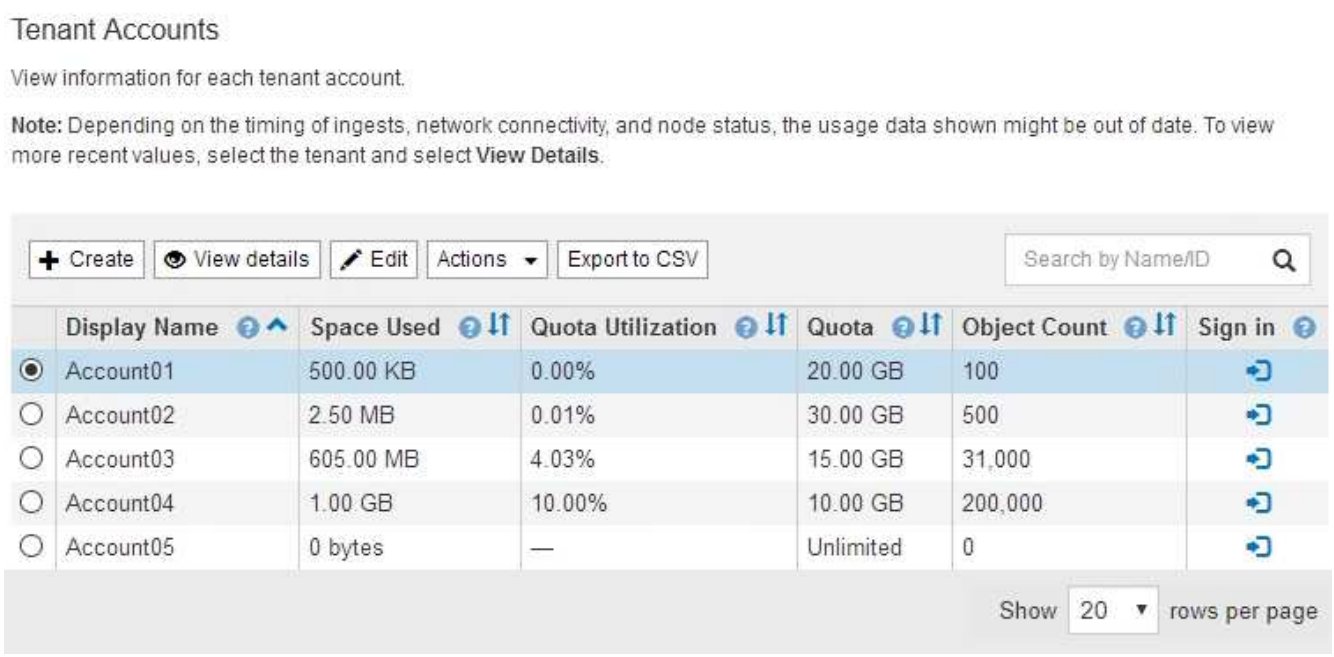
Sobre esta tarefa

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**.

   A página Contas do locatário é exibida e lista todas as contas de locatário existentes.

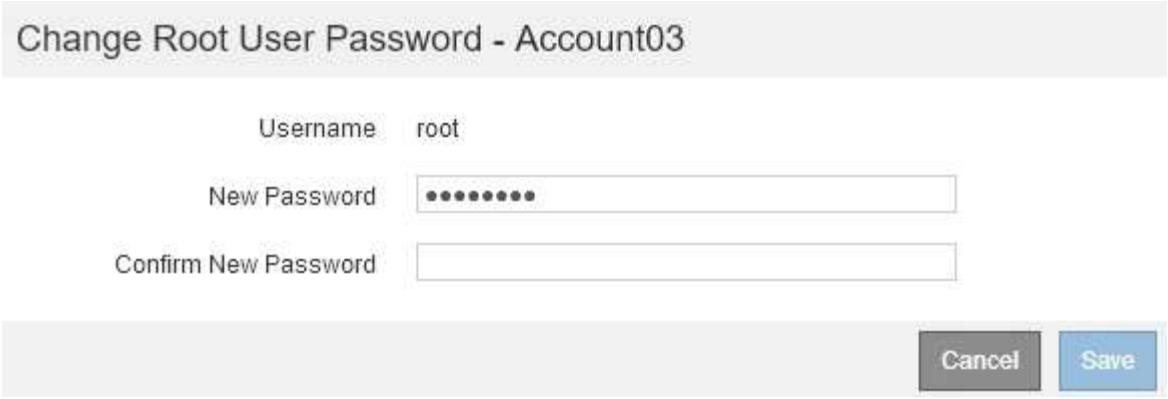


2. Selecione a conta de locatário que você deseja editar.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Use a caixa de pesquisa para procurar uma conta de locatário por nome de exibição ou ID de locatário.

   Os botões Ver Detalhes, Editar e ações ficam ativados.

3. Na lista suspensa **ações**, selecione **alterar senha de root**.



4. Introduza a nova palavra-passe para a conta de locatário.
5. Selecione **Guardar**.

Informações relacionadas

"Controlar o acesso do administrador ao StorageGRID"

Editando uma conta de locatário

Você pode editar uma conta de locatário para alterar o nome de exibição, alterar a configuração de origem de identidade, permitir ou desativar serviços de plataforma ou inserir uma cota de armazenamento.

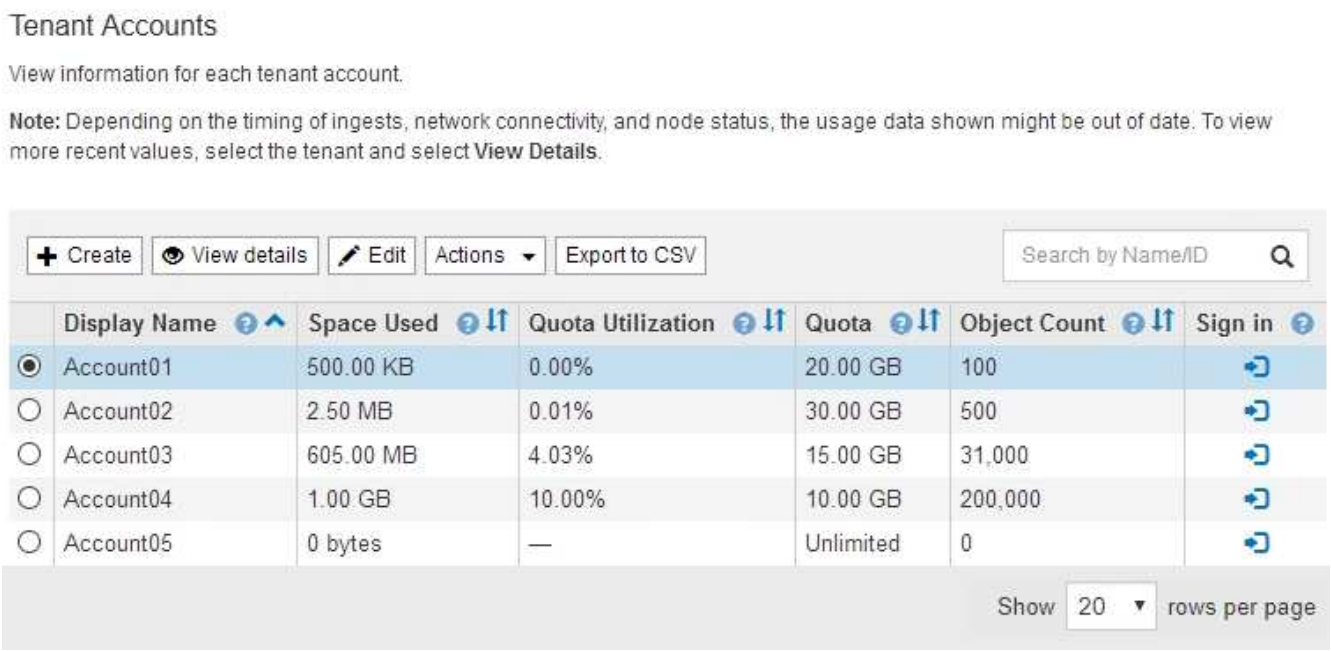
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **tenants**.

   A página Contas do locatário é exibida e lista todas as contas de locatário existentes.

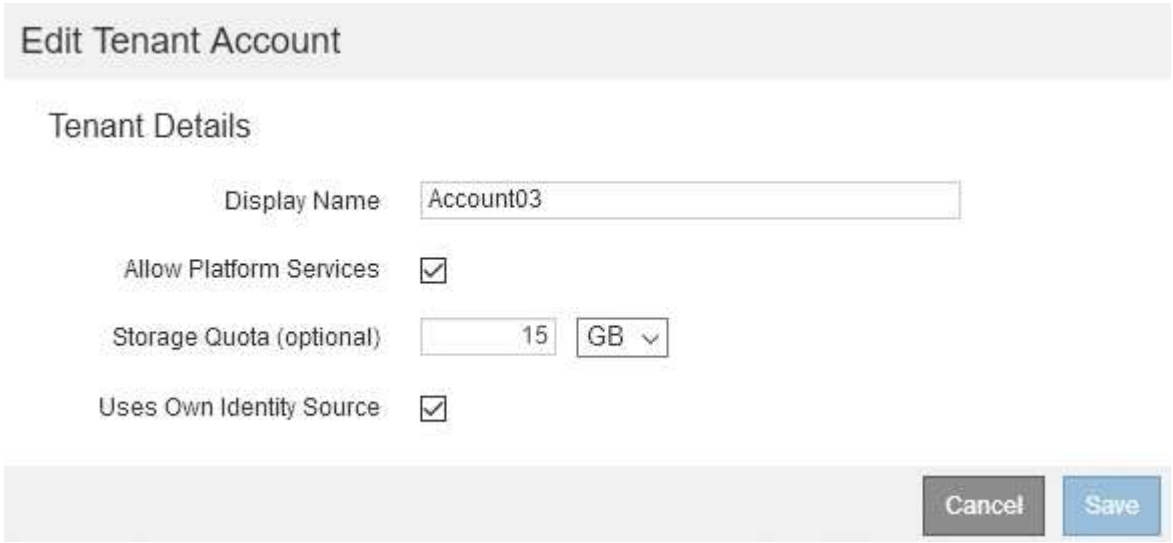


2. Selecione a conta de locatário que você deseja editar.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Use a caixa de pesquisa para procurar uma conta de locatário por nome de exibição ou ID de locatário.

3. Selecione **Editar**.

   A página Editar conta do locatário é exibida. Este exemplo é para uma grade que não usa logon único (SSO). Essa conta de locatário não configurou sua própria origem de identidade.



4. Altere os valores dos campos conforme necessário.
   a. Altere o nome de exibição dessa conta de locatário.
   b. Altere a configuração da caixa de seleção **permitir Serviços de Plataforma** para determinar se a conta de locatário pode usar serviços de plataforma para seus buckets do S3.

      Se você desabilitar os 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.

   c. Para **cota de armazenamento**, altere o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos desse locatário ou deixe o campo em branco se desejar que esse locatário tenha uma cota ilimitada.

      A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco). As cópias ILM e a codificação de apagamento não contribuem para a quantidade de cota usada.

Para monitorar o uso de armazenamento de cada conta de locatário, selecione **uso**. As contas de inquilino também podem monitorar seu próprio uso no Dashboard no Gerenciador do locatário ou com a API de gerenciamento do locatário. Observe que os valores de uso de storage de um locatário podem ficar desatualizados se os nós forem isolados de outros nós na grade. Os totais serão atualizados quando a conetividade de rede for restaurada.

d. Altere a configuração da caixa de seleção **usa a própria origem de identidade** para determinar se a conta de locatário usará sua própria origem de identidade ou a origem de identidade que foi configurada para o Gerenciador de Grade.

Se a caixa de verificação **usa a própria fonte de identidade** for:

- Desativado e verificado, 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 desmarcado, SSO está ativado para o sistema StorageGRID. O locatário deve usar a fonte de identidade que foi configurada para o Gerenciador de Grade.

5. Selecione **Guardar**.

Informações relacionadas

"Gerenciamento de serviços de plataforma para contas de locatários do S3"

"Use uma conta de locatário"

Excluindo uma conta de locatário

Você pode excluir uma conta de locatário se quiser remover permanentemente o acesso do locatário ao sistema.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter removido todos os buckets (S3), contentores (Swift) e objetos associados à conta de locatário.

Passos

1. Selecione **tenants**.
2. Selecione a conta de locatário que deseja excluir.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Use a caixa de pesquisa para procurar uma conta de locatário por nome de exibição ou ID de locatário.

3. Na lista suspensa **ações**, selecione **Remover**.
4. Selecione **OK**.

Informações relacionadas

"Controlar o acesso do administrador ao StorageGRID"

Gerenciamento de serviços de plataforma para contas de locatários do S3

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.

- "Quais são os serviços de plataforma"
- "Rede e portas para serviços de plataforma"
- "Entrega por local de mensagens de serviços de plataforma"
- "Solução de problemas de serviços da plataforma"

Quais são os serviços de plataforma

Os serviços de plataforma incluem replicação do CloudMirror, notificações de eventos e o serviço de integração de pesquisa.

Esses serviços permitem que os locatários usem a seguinte funcionalidade com seus buckets do S3:

- **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 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 Amazon Simple Notification Service (SNS) externo especificado.

  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 objetos 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 de plataforma, você deve estar ciente das seguintes recomendações:

- 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.
- 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.

Informações relacionadas

"Use uma conta de locatário"

"Configurando as configurações de proxy de armazenamento"

"Monitorizar Resolução de problemas"

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 Simple Notification Service (SNS)
- 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
- **443**: Para URIs de endpoint que começam com https

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 configurar as configurações de proxy de armazenamento para permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet.

Informações relacionadas

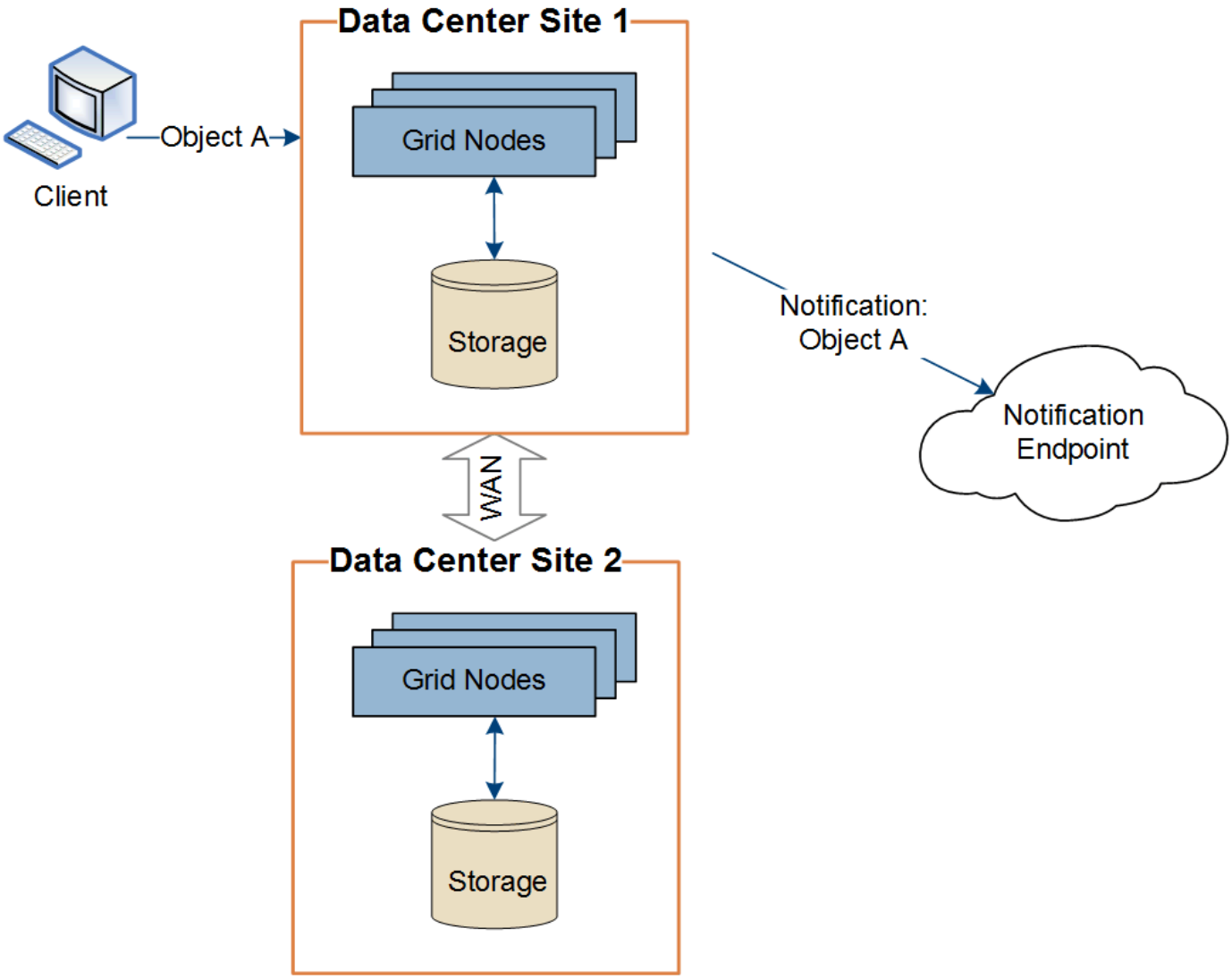
"Configurando as configurações de proxy de armazenamento"

"Use uma conta de locatário"

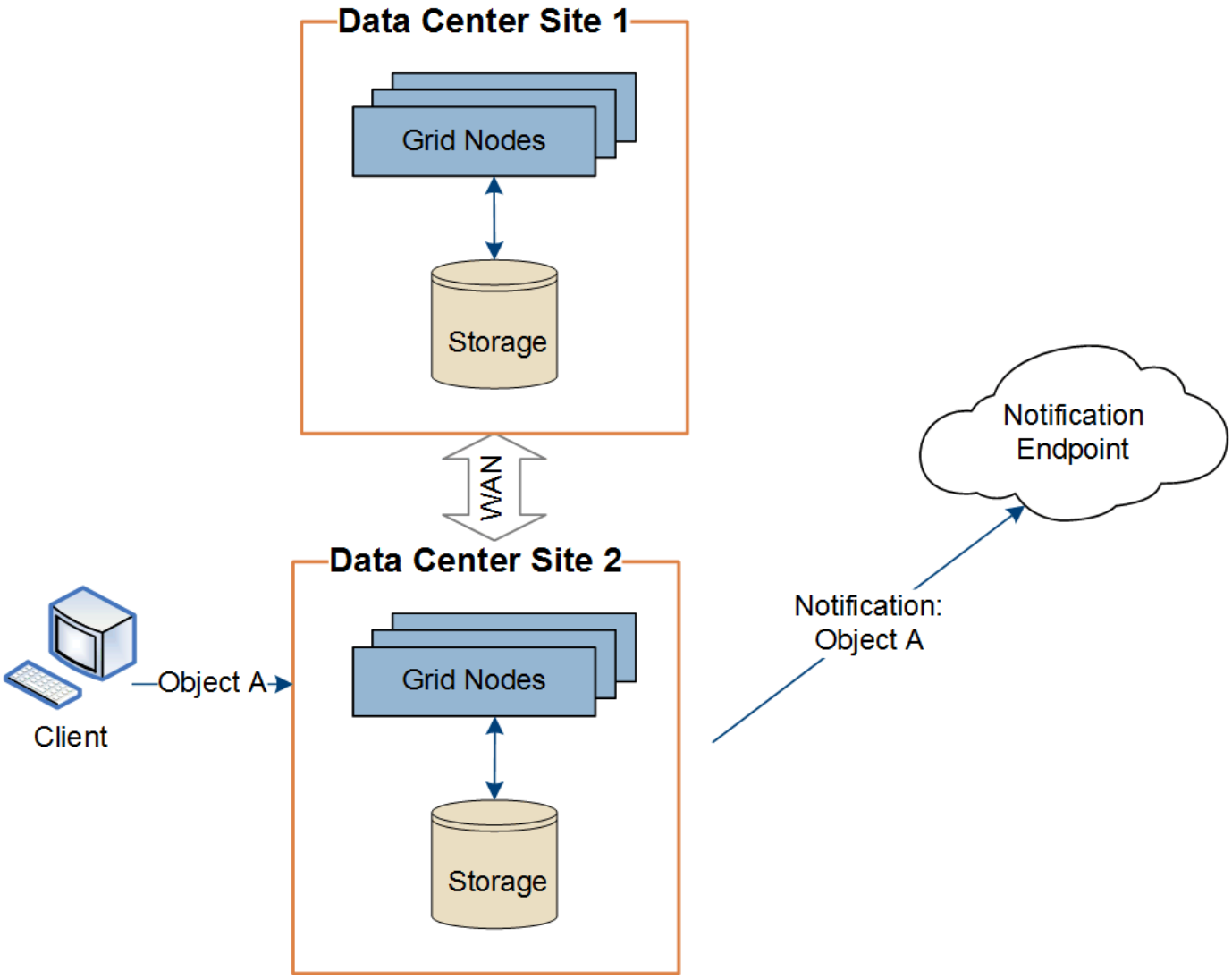
Entrega por local de mensagens de serviços de plataforma

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.

Solução de problemas de serviços da 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 serviço de notificação simples 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.

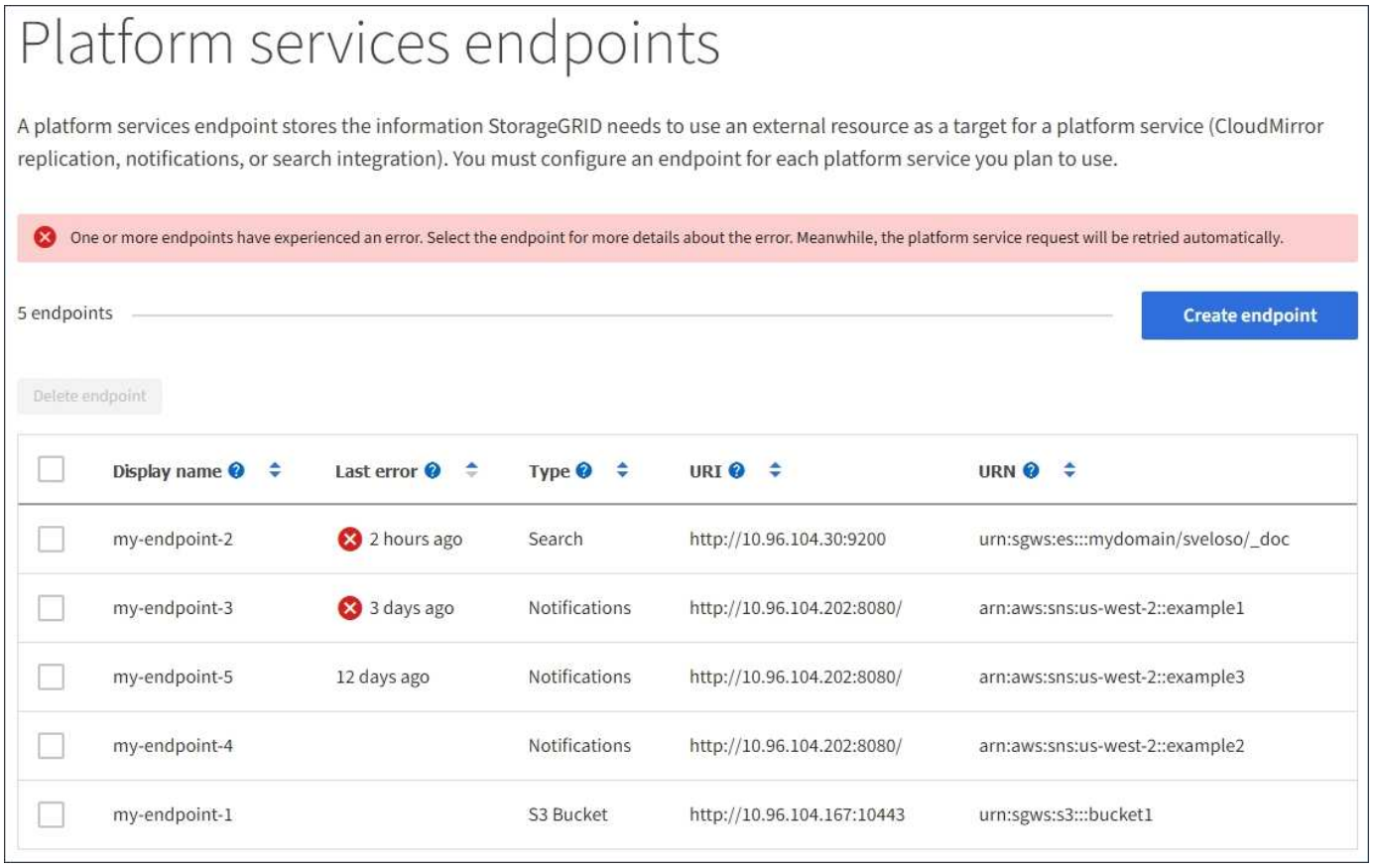
> A criação do endpoint falhará se os serviços da plataforma não estiverem habilitados para a conta do locatário.

Problemas com endpoints existentes

Se ocorrer um erro quando o StorageGRID tenta alcançar um endpoint existente, uma mensagem é exibida no Dashboard no Gerenciador de locatário.

> One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

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 de 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.

Determinar se ocorreu um erro

Se algum erro de endpoint tiver ocorrido nos últimos 7 dias, o Dashboard 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, o alarme de Eventos totais (SMTT) é acionado no Gerenciador de Grade. Para visualizar o alarme Total de Eventos:

1. Selecione **nós**.
2. Selecione ***site*** > ***grid node*** > **Eventos**.
3. Veja o último evento na parte superior da tabela.

   As mensagens de evento também são listadas em `/var/local/log/bycast-err.log`.

4. Siga as orientações fornecidas no conteúdo do alarme SMTT para corrigir o problema.
5. Clique em **Redefinir contagens de eventos**.
6. Notificar o locatário dos objetos cujas mensagens de serviços da plataforma não foram entregues.
7. Instrua o locatário a reativar a replicação ou notificação com falha atualizando os metadados ou as tags do

objeto.

O locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

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.

Se as mensagens dos serviços da plataforma não puderem ser entregues devido a um erro irrecuperável, o alarme de Eventos totais (SMTT) é acionado no Gerenciador de Grade.

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 **nós**.
2. Selecione ***site*** > **Serviços de Plataforma**.
3. Veja o gráfico taxa de falha 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 sobre a solução de problemas de endpoints de serviços de plataforma, consulte as instruções para o uso de contas de locatário.

"Use uma conta de locatário"

Informações relacionadas

"Monitorizar Resolução de problemas"

"Configurando as configurações de proxy de armazenamento"

Configurando conexões de cliente S3 e Swift

Como administrador de grade, você gerencia as opções de configuração que controlam como os locatários S3 e Swift podem conetar aplicativos clientes ao seu sistema StorageGRID para armazenar e recuperar dados. Existem várias opções diferentes para atender a diferentes requisitos de cliente e locatário.

Os aplicativos clientes podem armazenar ou recuperar objetos conetando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway, ou, opcionalmente, o endereço IP virtual de um grupo de alta disponibilidade (HA) de nós de administração ou nós de gateway
- O serviço CLB em nós de Gateway, ou, opcionalmente, o endereço IP virtual de um grupo de nós de gateway de alta disponibilidade

  O serviço CLB está obsoleto. Os clientes configurados antes da versão do StorageGRID 11,3 podem continuar a usar o serviço CLB nos nós de gateway. Todos os outros aplicativos clientes que dependem do StorageGRID para fornecer balanceamento de carga devem se conetar usando o serviço de balanceamento de carga.

- Nós de storage, com ou sem um balanceador de carga externo

Opcionalmente, você pode configurar os seguintes recursos em seu sistema StorageGRID:

- **Serviço de balanceamento de carga**: Você permite que os clientes usem o serviço de balanceamento de carga criando pontos de extremidade do balanceador de carga para conexões de cliente. Ao criar um endpoint de balanceador de carga, você especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).
- **Rede Cliente não confiável**: Você pode tornar a rede Cliente mais segura configurando-a como não confiável. Quando a rede do cliente não é confiável, os clientes só podem se conetar usando pontos de extremidade do balanceador de carga.
- **Grupos de alta disponibilidade**: Você pode criar um grupo de HA de nós de Gateway ou nós de administrador para criar uma configuração de backup ativo ou usar DNS de round-robin ou um balanceador de carga de terceiros e vários grupos de HA para obter uma configuração ativo-ativo. As conexões de cliente são feitas usando os endereços IP virtuais de grupos HA.

Você também pode habilitar o uso de HTTP para clientes que se conetam ao StorageGRID diretamente aos nós de armazenamento ou usando o serviço CLB (obsoleto), e você pode configurar nomes de domínio de endpoint de API S3 para clientes S3.

Resumo: Endereços IP e portas para conexões de clientes

Os aplicativos clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de grade e o número da porta de um serviço nesse nó. Se os grupos de alta disponibilidade (HA) estiverem configurados, os aplicativos clientes poderão se conetar usando o endereço IP virtual do grupo HA.

Sobre esta tarefa

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. As instruções descrevem como localizar essas informações no Gerenciador de Grade se os pontos de extremidade do balanceador de carga e os grupos de alta disponibilidade (HA) já estiverem configurados.

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 de extremidade do balanceador de carga
Grupo HA	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas S3 padrão: • HTTPS: 8082 • HTTP: 8084 Portas Swift padrão: • HTTPS:8083 • HTTP:8085
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	• Porta de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	• Porta de extremidade do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Nó de gateway	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP do nó de gateway **Nota:** por padrão, as portas HTTP para CLB e LDR não estão ativadas.	Portas S3 padrão: • HTTPS: 8082 • HTTP: 8084 Portas Swift padrão: • HTTPS:8083 • HTTP:8085
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084 Portas Swift padrão: • HTTPS: 18083 • HTTP:18085

Exemplos

Para conetar um cliente S3 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 de um endpoint do balanceador de carga S3 for 10443, um cliente S3 poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.5:10443`

Para conetar um cliente Swift ao endpoint 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 192.0.2.6 e o número da porta de um endpoint do Swift Load Balancer for 10444, um cliente Swift poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.6:10444`

É possível configurar um nome DNS para o endereço IP que os clientes usam para se conetar ao StorageGRID. Contacte o administrador da rede local.

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.

2. Para localizar o endereço IP de um nó de grade:
   a. Selecione **nós**.
   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. Clique em **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 **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.
   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 Settings** > **Load Balancer Endpoints**.

      A página Load Balancer Endpoints é exibida, mostrando a lista de endpoints que já foram configurados.

   b. Selecione um endpoint e clique em **Editar endpoint**.

      A janela Editar ponto final abre-se e apresenta detalhes adicionais sobre o ponto final.

   c. Confirme se o endpoint selecionado está configurado para uso com o protocolo correto (S3 ou Swift) e, em seguida, clique em **Cancelar**.
   d. Observe o número da porta do endpoint que você deseja usar para uma conexão de cliente.

      > Se o número da porta for 80 ou 443, o endpoint será configurado apenas em nós de Gateway, uma vez que essas portas estão reservadas em nós de administração. Todas as outras portas são configuradas nos nós de Gateway e nos de Admin.

Gerenciamento do balanceamento de carga

Você pode usar as funções de balanceamento de carga do StorageGRID para lidar com cargas de trabalho de ingestão e recuperação de clientes S3 e Swift. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo cargas de trabalho e conexões entre vários nós de storage.

Você pode obter balanceamento de carga em seu sistema StorageGRID das seguintes maneiras:

- Use o serviço Load Balancer, que é instalado em nós de administração e nós de gateway. O serviço Load Balancer fornece balanceamento de carga de camada 7 e executa o encerramento TLS das solicitações do cliente, inspeciona as solicitações e estabelece novas conexões seguras aos nós de storage. Este é o mecanismo de balanceamento de carga recomendado.
- Use o serviço CLB (Connection Load Balancer), que é instalado somente em nós de Gateway. O serviço CLB fornece balanceamento de carga da camada 4 e suporta custos de link.

  O serviço CLB está obsoleto.

- Integre um balanceador de carga de terceiros. Entre em Contato com o representante da sua conta NetApp para obter detalhes.

Como funciona o balanceamento de carga - Serviço do Load Balancer

O serviço Load Balancer distribui conexões de rede recebidas de aplicativos clientes para nós de storage. Para ativar o balanceamento de carga, você deve configurar pontos de extremidade do balanceador de carga usando o Gerenciador de Grade.

Você pode configurar pontos de extremidade do balanceador de carga somente para nós de administrador ou nós de gateway, uma vez que esses tipos de nó contêm o serviço Load Balancer. Não é possível configurar pontos de extremidade para nós de storage ou nós de arquivamento.

Cada ponto de extremidade do balanceador de carga especifica uma porta, um protocolo (HTTP ou HTTPS), um tipo de serviço (S3 ou Swift) e um modo de encadernação. Os endpoints HTTPS requerem um certificado de servidor. Os modos de vinculação permitem restringir a acessibilidade das portas de endpoint a:

- Endereços IP virtuais (VIPs) específicos de alta disponibilidade (HA)
- Interfaces de rede específicas de nós específicos

Considerações de porta

Os clientes podem acessar qualquer um dos pontos de extremidade que você configurar em qualquer nó executando o serviço Load Balancer, com duas exceções: As portas 80 e 443 são reservadas em nós de administração, portanto, os pontos de extremidade configurados nessas portas suportam operações de balanceamento de carga somente em nós de Gateway.

Se você tiver remapeado quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Você pode criar endpoints usando portas remapeadas, mas esses endpoints serão remapeados para as portas e serviços CLB originais, não para o serviço Load Balancer. Siga as etapas nas instruções de recuperação e manutenção para remover os remapas de portas.

O serviço CLB está obsoleto.

Disponibilidade da CPU

O serviço Load Balancer em cada nó de administração e nó de gateway opera independentemente ao encaminhar tráfego S3 ou Swift 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.

Informações relacionadas

"Manter recuperar"

Configuração dos pontos de extremidade do balanceador de carga

Você pode criar, editar e remover pontos de extremidade do balanceador de carga.

Criação de pontos de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga especifica uma porta, um protocolo de rede (HTTP ou HTTPS) e um tipo de serviço (S3 ou Swift). Se criar um endpoint HTTPS, tem de carregar ou gerar um certificado de servidor.

O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Se você tiver anteriormente as portas remapeadas que pretende usar para o serviço Load Balancer, você deve ter removido os remapes.

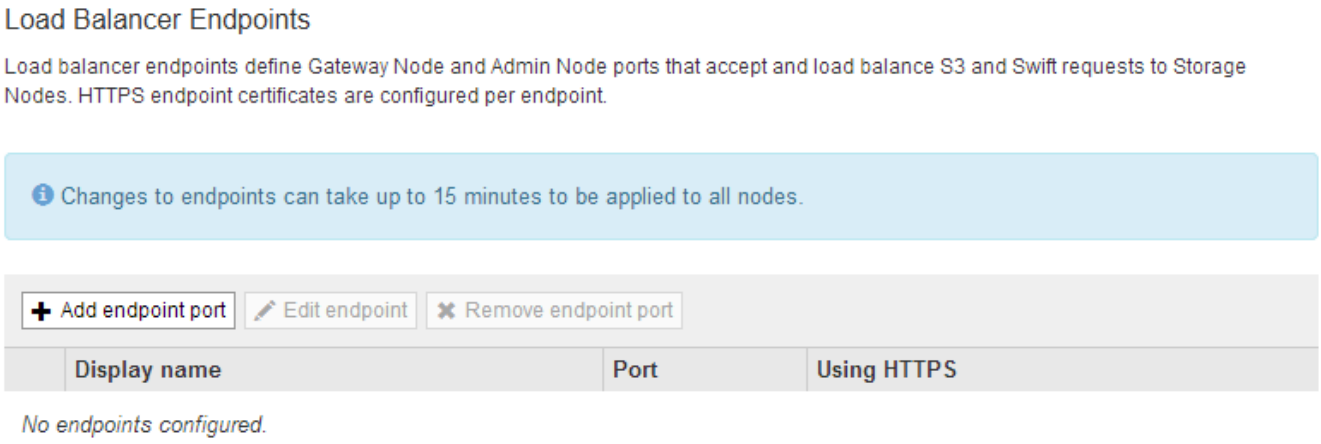
> Se você tiver remapeado quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Você pode criar endpoints usando portas remapeadas, mas esses endpoints serão remapeados para as portas e serviços CLB originais, não para o serviço Load Balancer. Siga as etapas nas instruções de recuperação e manutenção para remover os remapas de portas.

> O serviço CLB está obsoleto.

Passos

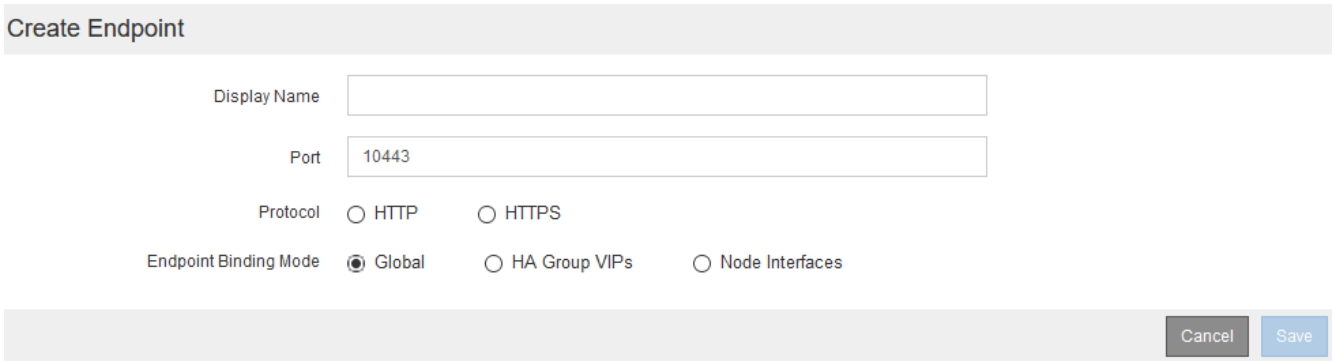
1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida.



2. Selecione **Adicionar endpoint**.

A caixa de diálogo criar ponto final é exibida.



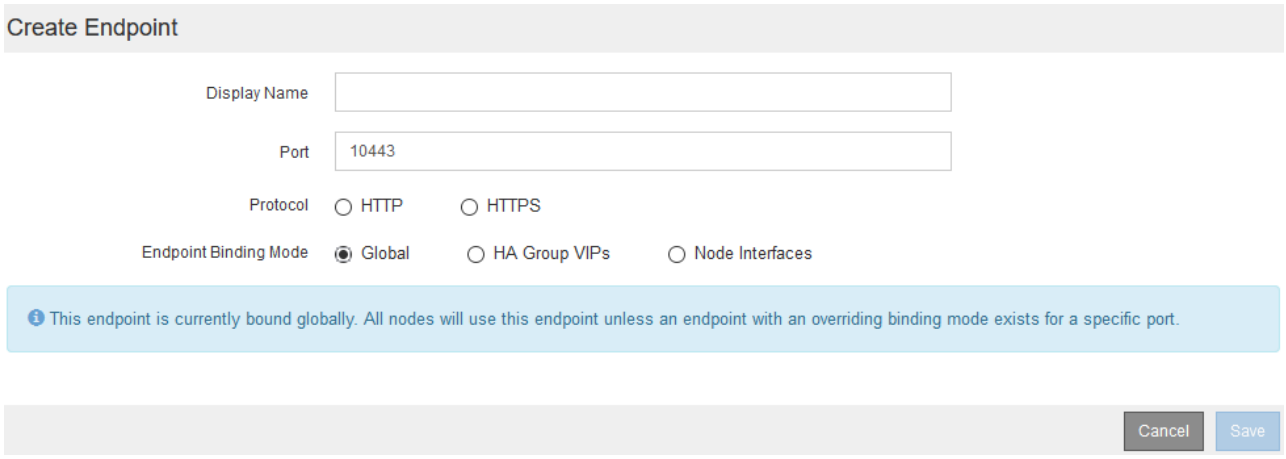
3. Insira um nome de exibição para o endpoint, que aparecerá na lista na página Load Balancer Endpoints.
4. Introduza um número de porta ou deixe o número de porta pré-preenchido como está.

   Se você inserir o número da porta 80 ou 443, o endpoint será configurado somente nos nós do Gateway, uma vez que essas portas serão reservadas nos nós de administração.

   > As portas usadas por outros serviços de grade não são permitidas. Consulte as diretrizes de rede para obter uma lista de portas usadas para comunicações internas e externas.

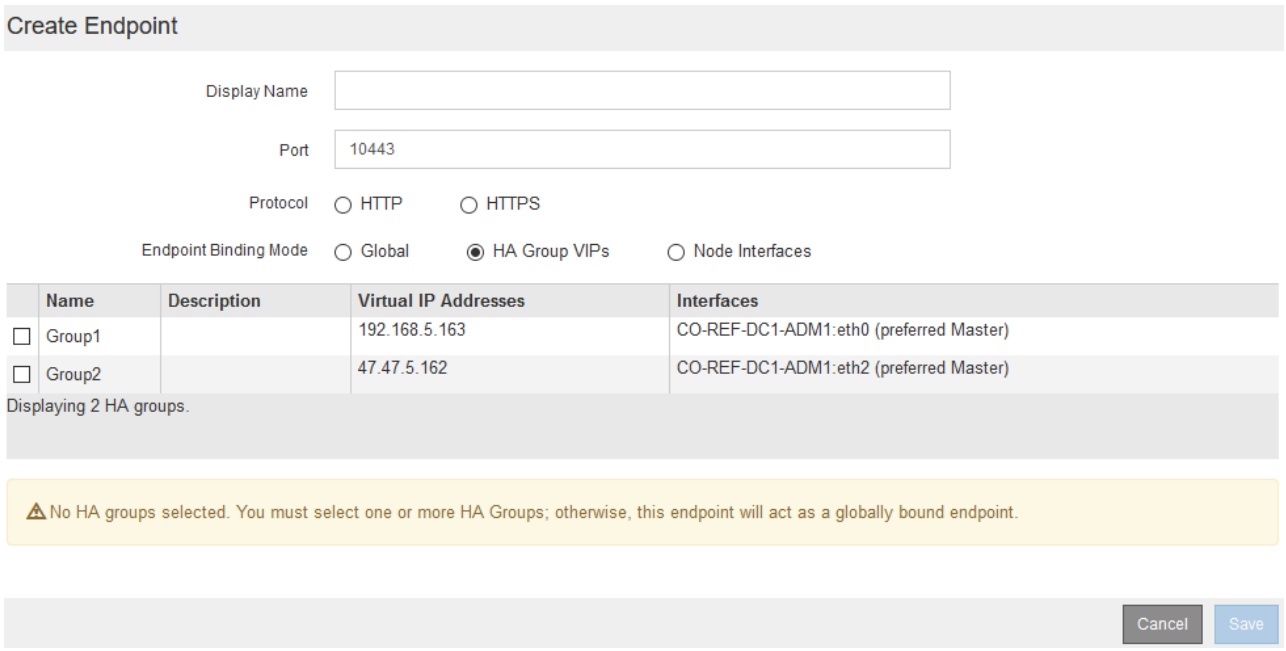
5. Selecione **HTTP** ou **HTTPS** para especificar o protocolo de rede para este endpoint.
6. Selecione um modo de encadernação de endpoint.

   - **Global** (padrão): O endpoint está acessível em todos os nós de Gateway e nós de Admin no número de porta especificado.



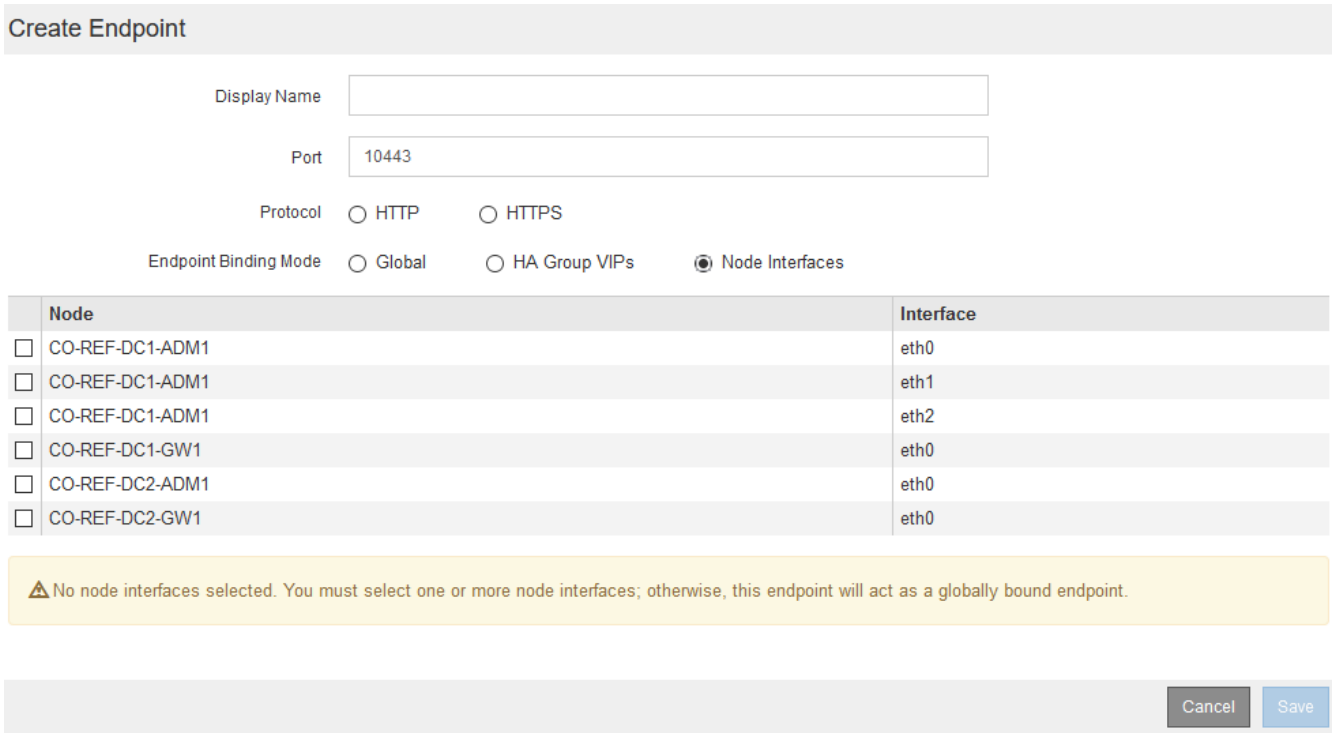
   - **VIPs do grupo HA**: O endpoint só pode ser acessado através dos endereços IP virtuais definidos para os grupos de HA selecionados. Os endpoints definidos neste modo podem reutilizar o mesmo número de porta, desde que os grupos de HA definidos por esses endpoints não se sobreponham entre si.

     Selecione os grupos de HA com os endereços IP virtuais onde deseja que o endpoint apareça.



- * Interfaces de nó*: O ponto de extremidade é acessível apenas nos nós designados e interfaces de rede. Os endpoints definidos neste modo podem reutilizar o mesmo número de porta desde que essas interfaces não se sobreponham umas às outras.

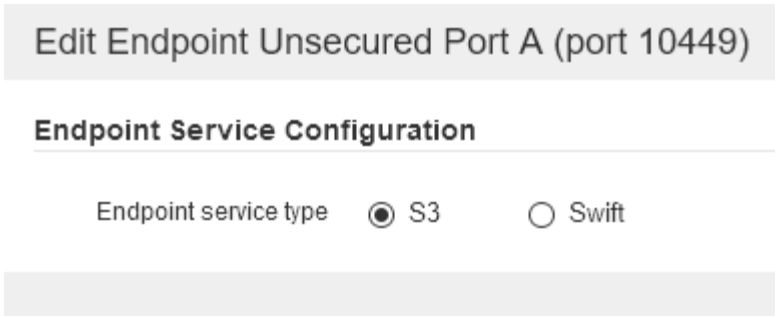
  Selecione as interfaces de nó em que você deseja que o endpoint apareça.



7. Selecione **Guardar**.

   A caixa de diálogo Editar ponto final é exibida.

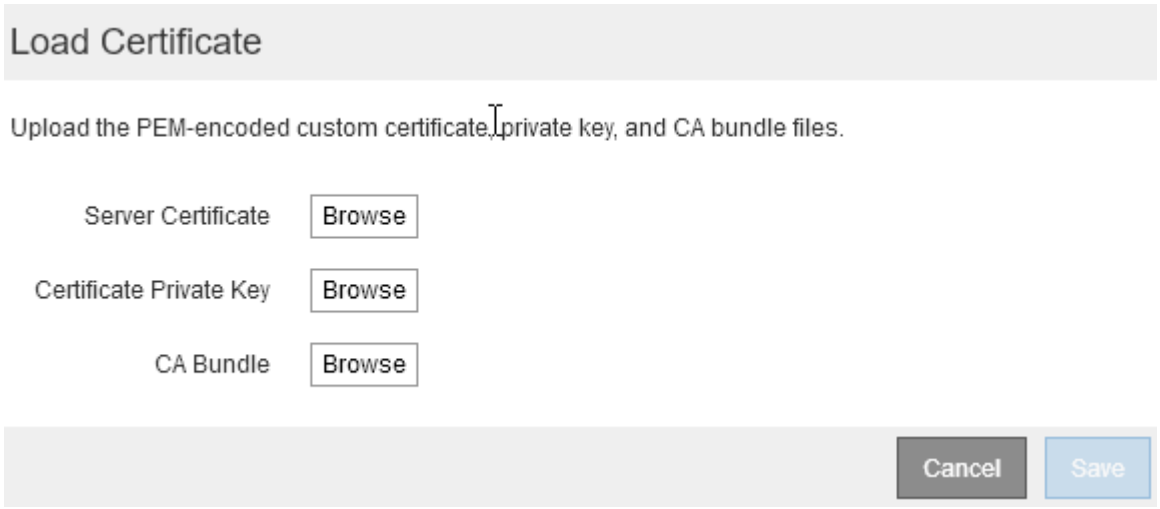
8. Selecione **S3** ou **Swift** para especificar o tipo de tráfego que este endpoint irá servir.



9. Se você selecionou **HTTP**, selecione **Salvar**.

   O ponto final não protegido é criado. A tabela na página Load Balancer Endpoints lista o nome de exibição, o número da porta, o protocolo e o ID do endpoint.

10. Se selecionou **HTTPS** e pretende carregar um certificado, selecione **carregar certificado**.



    a. Procure o certificado do servidor e a chave privada do certificado.

       Para permitir que os clientes S3 se conetem usando um nome de domínio de endpoint da API S3, use um certificado de domínio multidomínio ou curinga que corresponda a todos os nomes de domínio que o cliente possa usar para se conetar à grade. Por exemplo, o certificado do servidor pode usar o nome de domínio `*.example.com` .

"Configurando nomes de domínio de endpoint da API S3"

    a. Opcionalmente, procure um pacote de CA.
    b. Selecione **Guardar**.

       Os dados de certificado codificados em PEM para o endpoint são exibidos.

11. Se você selecionou **HTTPS** e deseja gerar um certificado, selecione **Generate Certificate**.

a. Introduza um nome de domínio ou um endereço IP.

   Você pode usar wildcards para representar os nomes de domínio totalmente qualificados de todos os nós de administrador e nós de gateway que executam o serviço Load Balancer. Por exemplo, `*.sgws.foo.com` usa o caractere curinga * para representar `gn1.sgws.foo.com` e `gn2.sgws.foo.com`.

"Configurando nomes de domínio de endpoint da API S3"

a. ➕Selecione para adicionar outros nomes de domínio ou endereços IP.

   Se você estiver usando grupos de alta disponibilidade (HA), adicione os nomes de domínio e endereços IP dos IPs virtuais de HA.

b. Opcionalmente, insira um assunto X,509, também chamado de Nome distinto (DN), para identificar quem possui o certificado.
c. Opcionalmente, selecione o número de dias em que o certificado é válido. O padrão é de 730 dias.
d. Selecione **Generate**.

   Os metadados do certificado e os dados do certificado codificados em PEM para o endpoint são exibidos.

12. Clique em **Salvar**.

    O endpoint é criado. A tabela na página Load Balancer Endpoints lista o nome de exibição, o número da porta, o protocolo e o ID do endpoint.

Informações relacionadas

"Manter recuperar"

"Diretrizes de rede"

"Gerenciamento de grupos de alta disponibilidade"

"Gerenciando redes de clientes não confiáveis"

Editar pontos de extremidade do balanceador de carga

Para um endpoint não protegido (HTTP), você pode alterar o tipo de serviço de endpoint entre S3 e Swift. Para um endpoint seguro (HTTPS), você pode editar o tipo de serviço de endpoint e exibir ou alterar o certificado de segurança.

O que você vai precisar

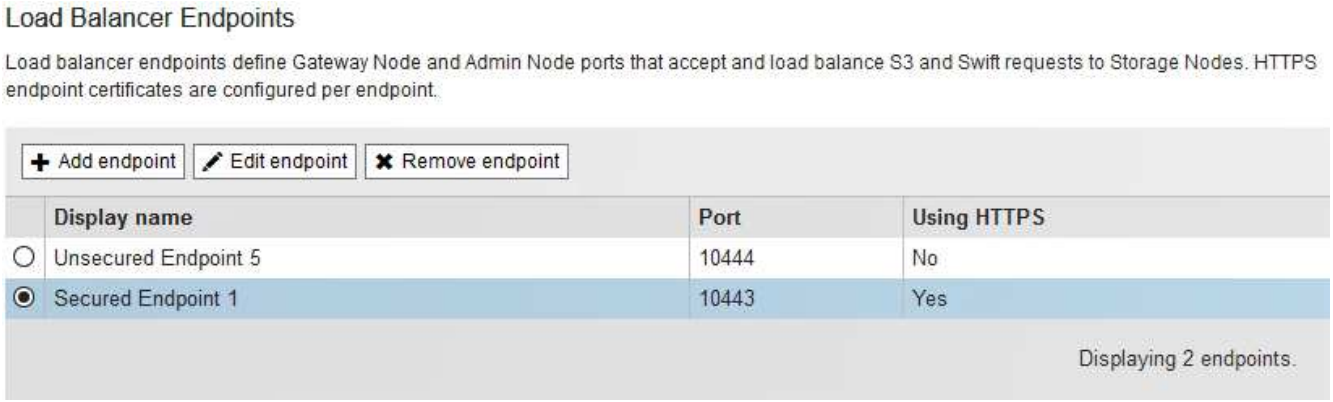
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida. Os endpoints existentes são listados na tabela.

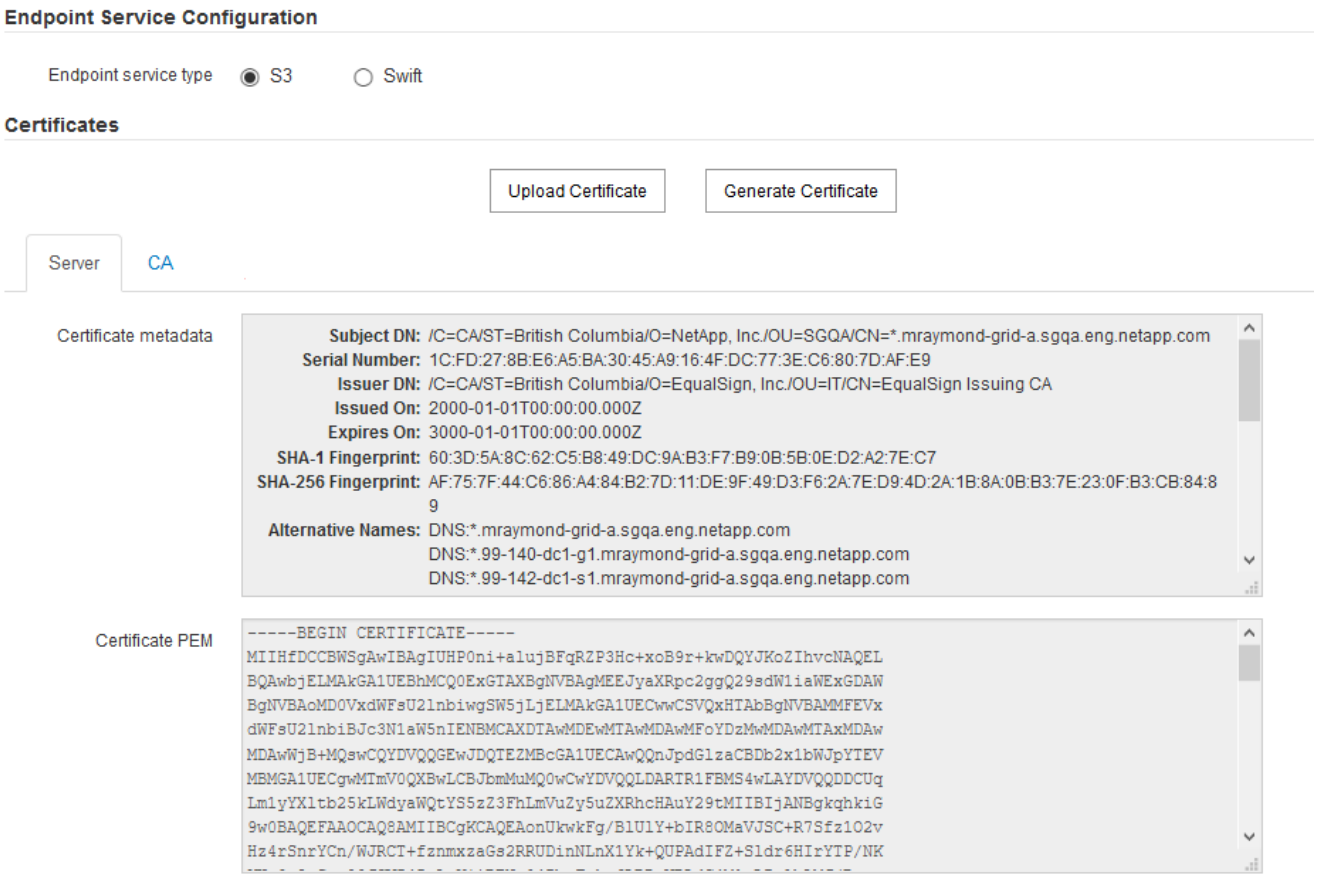
   Endpoints com certificados que expirarão em breve são identificados na tabela.



2. Selecione o ponto de extremidade que pretende editar.
3. Clique em **Editar endpoint**.

   A caixa de diálogo Editar ponto final é exibida.

   Para um ponto de extremidade não protegido (HTTP), apenas a secção Configuração do serviço de extremidade da caixa de diálogo é apresentada. Para um ponto de extremidade seguro (HTTPS), as secções Configuração do serviço de extremidade e certificados da caixa de diálogo são apresentadas, conforme ilustrado no exemplo seguinte.



4. Faça as alterações desejadas no endpoint.

   Para um endpoint não protegido (HTTP), você pode:

   - Altere o tipo de serviço de endpoint entre S3 e Swift.
   - Altere o modo de encadernação de endpoint. Para um endpoint seguro (HTTPS), você pode:
   - Altere o tipo de serviço de endpoint entre S3 e Swift.
   - Altere o modo de encadernação de endpoint.
   - Exibir o certificado de segurança.
   - Carregue ou gere um novo certificado de segurança quando o certificado atual estiver expirado ou prestes a expirar.

     Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor StorageGRID ou um certificado assinado pela CA que foi carregado.

   > Para alterar o protocolo de um endpoint existente, por exemplo, de HTTP para HTTPS, você deve criar um novo endpoint. Siga as instruções para criar pontos de extremidade do balanceador de carga e selecione o protocolo desejado.

5. Clique em **Salvar**.

Informações relacionadas

Criação de pontos de extremidade do balanceador de carga

Remoção dos pontos finais do balanceador de carga

Se você não precisar mais de um ponto de extremidade do balanceador de carga, poderá removê-lo.

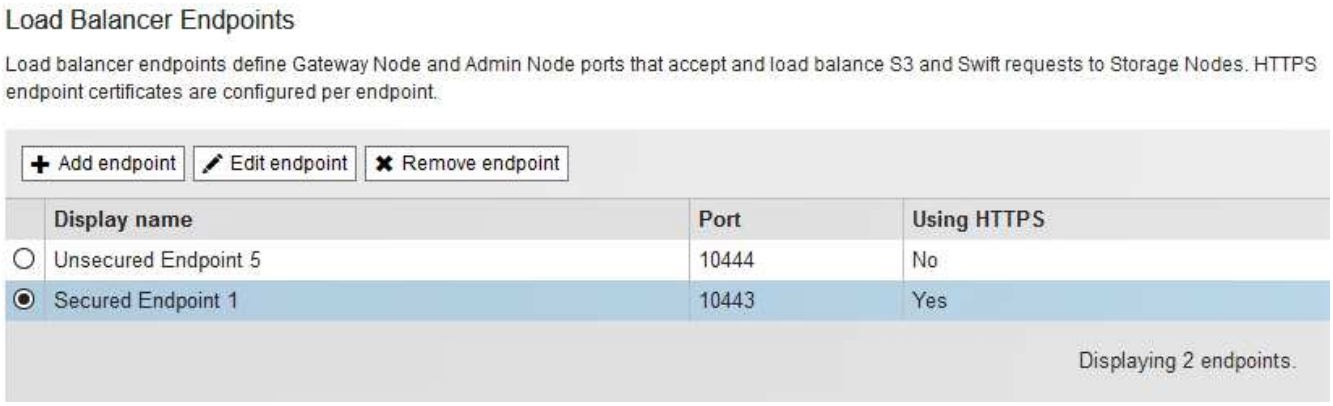
O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida. Os endpoints existentes são listados na tabela.



2. Selecione o botão de opção à esquerda do ponto de extremidade que pretende remover.
3. Clique em **Remover endpoint**.

   É apresentada uma caixa de diálogo de confirmação.

4. Clique em **OK**.

   O ponto final é removido.

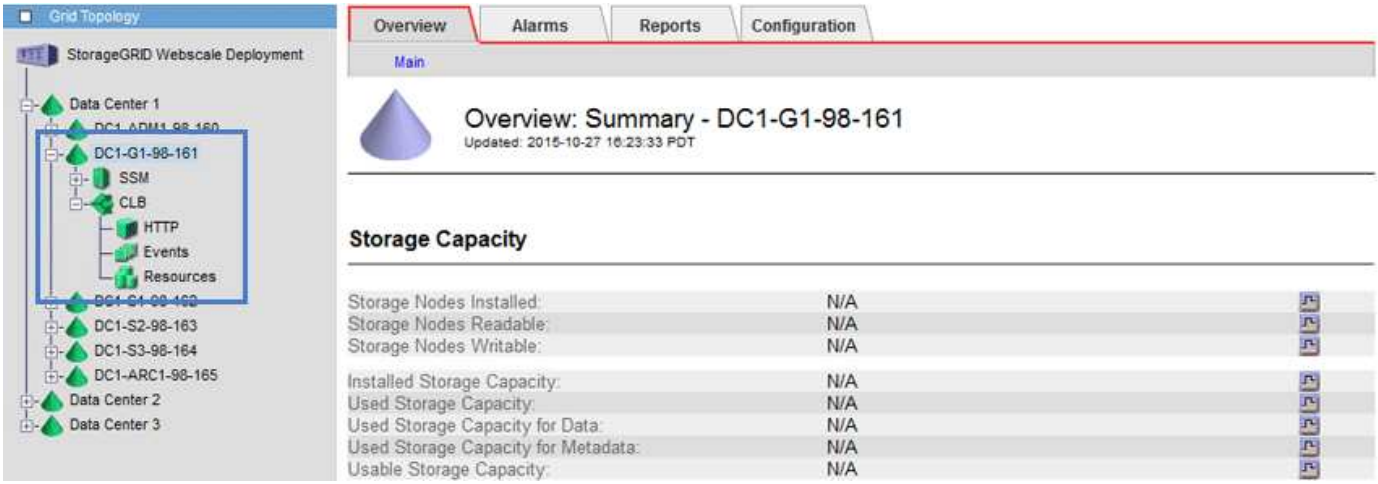
Como funciona o balanceamento de carga - serviço CLB

O serviço CLB (Connection Load Balancer) nos nós de Gateway está obsoleto. O serviço Load Balancer é agora o mecanismo de balanceamento de carga recomendado.

O serviço CLB usa o balanceamento de carga da camada 4 para distribuir conexões de rede TCP de entrada de aplicativos clientes para o nó de armazenamento ideal com base na disponibilidade, carga do sistema e

custo de link configurado pelo administrador. Quando o nó de armazenamento ideal é escolhido, o serviço CLB estabelece uma conexão de rede bidirecional e encaminha o tráfego de e para o nó escolhido. O CLB não considera a configuração da rede de Grade ao direcionar conexões de rede recebidas.

Para visualizar informações sobre o serviço CLB, selecione **Support** > **Tools** > **Grid Topology** e expanda um Gateway Node até selecionar **CLB** e as opções abaixo.



Se você optar por usar o serviço CLB, considere configurar os custos de link para o seu sistema StorageGRID.

Informações relacionadas

"Quais são os custos da ligação"

"Atualizar custos de link"

Gerenciando redes de clientes não confiáveis

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 todas as portas externas disponíveis (consulte as informações sobre comunicações externas nas diretrizes de rede).

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.

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 página Load Balancer Endpoints, configure um ponto de extremidade do balanceador de carga para S3 em HTTPS na porta 443.
2. Na página redes de clientes não confiáveis, especifique que a rede de 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 serviço 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 cliente. Você executaria este passo geral:

- Na página redes de clientes não confiáveis, 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 a Amazon Web Services.

Informações relacionadas

"Diretrizes de rede"

"Configuração dos pontos de extremidade do balanceador de carga"

Especificar a rede cliente de um nó não é confiável

Se você estiver usando uma rede de cliente, poderá especificar se a rede de cliente de cada nó é confiável ou não confiável. Você também pode especificar a configuração padrão para novos nós adicionados em uma expansão.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.
- 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.

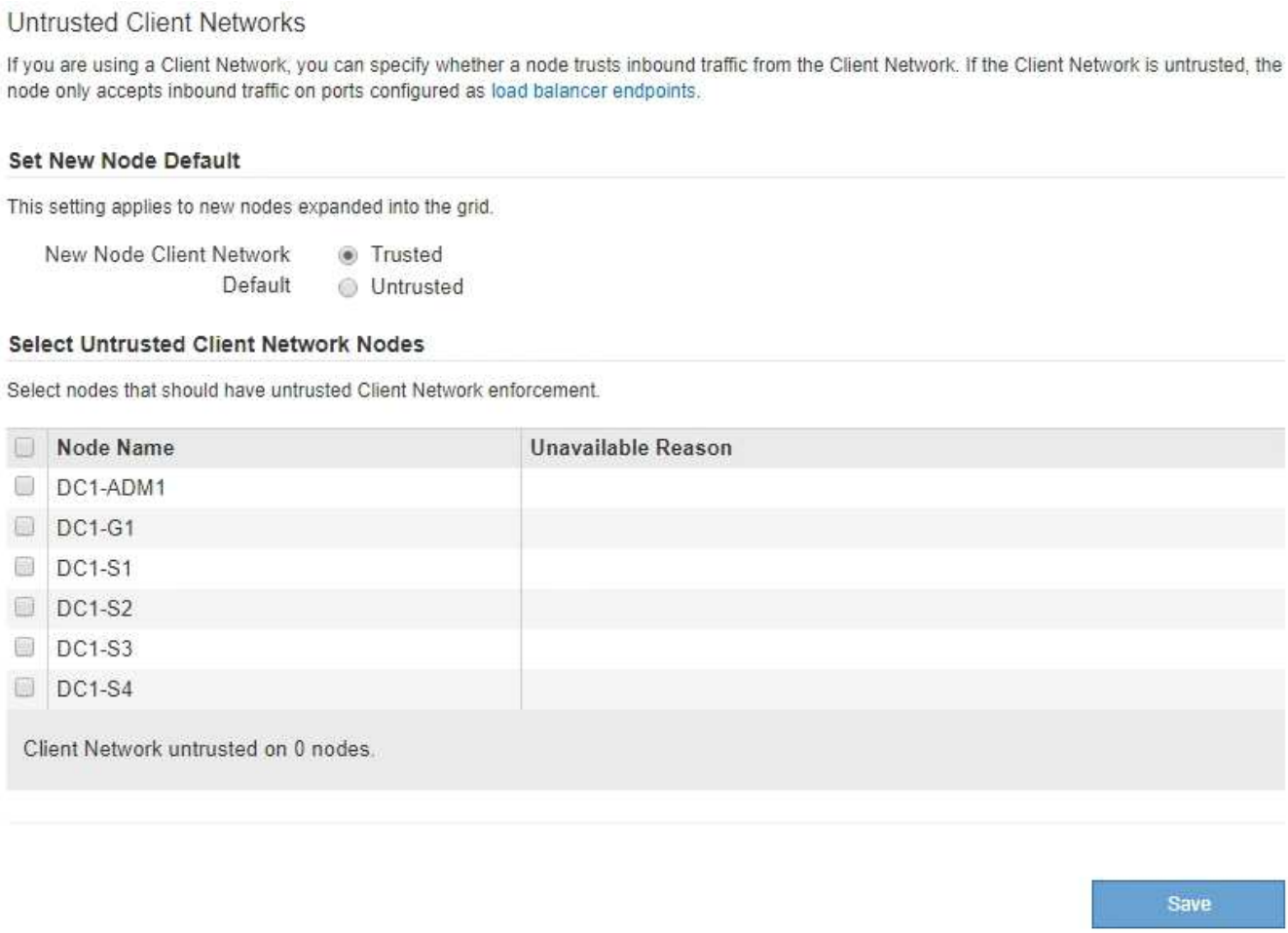
> As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **rede cliente não confiável**.

   A página redes de clientes não confiáveis é exibida.

   Esta página lista todos os nós no seu sistema StorageGRID. A coluna motivo indisponível inclui uma entrada se a rede do cliente no nó tiver de ser fidedigna.



2. Na seção **Definir novo padrão de nó**, especifique qual deve ser a configuração padrão quando novos nós forem adicionados à grade em um procedimento de expansão.
   - **Trusted**: 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 esta página para alterar a configuração de um novo nó específico.

   Esta configuração não afeta os nós existentes no seu sistema StorageGRID.

3. Na seção **Selecione nós de rede de cliente não confiáveis**, selecione os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga configurados explicitamente.

   Você pode selecionar ou desmarcar a caixa de seleção no título para selecionar ou desmarcar todos os nós.

4. Clique em **Salvar**.

   As novas regras de firewall são imediatamente adicionadas e aplicadas. As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Informações relacionadas

"Configuração dos pontos de extremidade do balanceador de carga"

Gerenciamento de grupos de alta disponibilidade

Grupos de alta disponibilidade (HA) podem ser usados para fornecer conexões de dados altamente disponíveis para clientes S3 e Swift. Os GRUPOS HA também podem ser usados para fornecer conexões altamente disponíveis ao Gerenciador de Grade e ao Gerenciador de Locatário.

- "O que é um grupo HA"
- "Como os grupos de HA são usados"
- "Opções de configuração para grupos de HA"
- "Criando um grupo de alta disponibilidade"
- "Edição de um grupo de alta disponibilidade"
- "Removendo um grupo de alta disponibilidade"

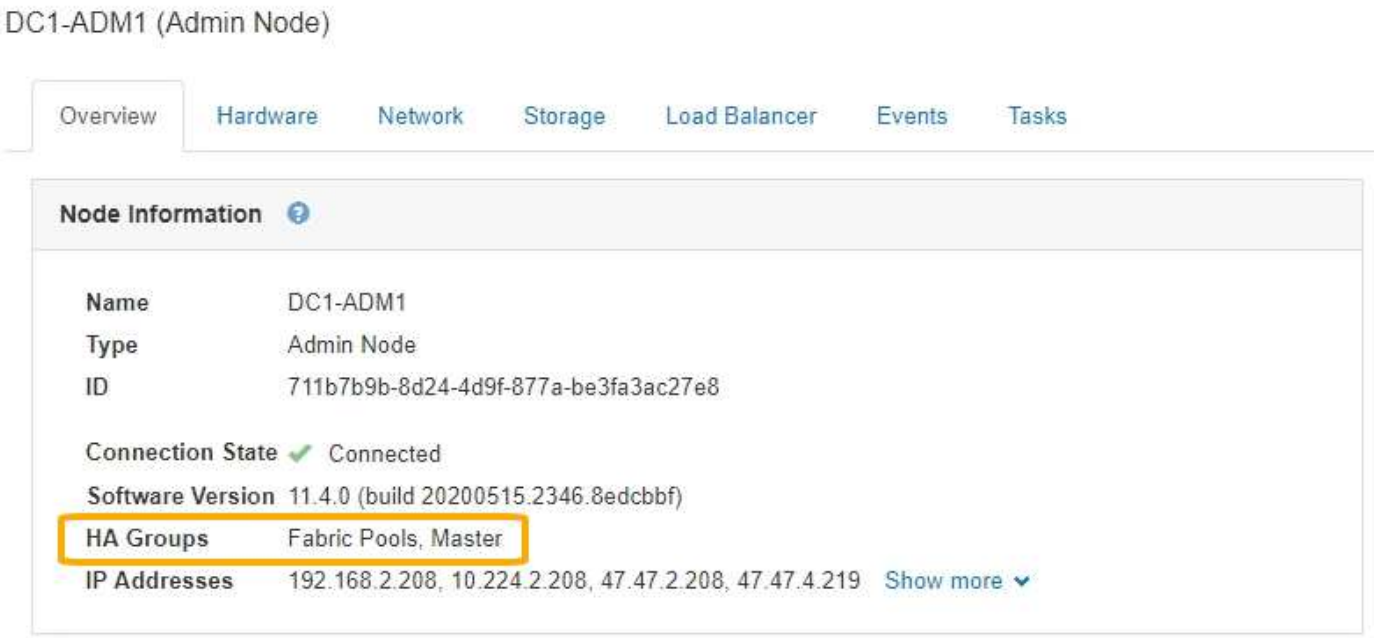
O que é um grupo HA

Os grupos de alta disponibilidade usam endereços IP virtuais (VIPs) para fornecer acesso de backup ativo aos serviços do nó de gateway ou nó de administrador.

Um grupo de HA consiste em uma ou mais interfaces de rede em nós de administração e nós de gateway. Ao criar um grupo HA, você seleciona interfaces de rede pertencentes à rede Grid (eth0) ou à rede Client (eth2). Todas as interfaces de um grupo HA devem estar dentro da mesma sub-rede de rede.

Um grupo de HA mantém um ou mais endereços IP virtuais que são adicionados à interface ativa no grupo. Se a interface ativa ficar indisponível, os endereços IP virtuais serão movidos para outra interface. Esse 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.

A interface ativa em um grupo HA é designada como Master. Todas as outras interfaces são designadas como Backup. Para visualizar estas designações, selecione **nodes** > ***node*** > **Overview**.



Ao criar um grupo HA, você especifica uma interface para ser o mestre preferido. O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup. Quando a falha é resolvida, os endereços VIP são automaticamente movidos de volta para o Master preferido.

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 pela falha do serviço CLB (obsoleto) ou serviços para o Gerenciador de Grade ou o Gerenciador de Tenant.

Se o grupo de HA incluir interfaces de mais de dois nós, a interface ativa poderá ser movida para a interface de qualquer outro nó durante o failover.

Como os grupos de HA são usados

Você pode querer usar grupos de alta disponibilidade (HA) por vários motivos.

- 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 e Swift.
- 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**: Incluem o serviço Load Balancer e o serviço CLB (obsoleto).

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso ao Grid Manager	• Nó de administração principal (**Mestre preferido**) • Nós de administração não primários **Nota:** o nó de administração principal deve ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso apenas ao Gestor do Locatário	• Nós de administração primários ou não primários
Acesso ao cliente S3 ou Swift — Serviço de Load Balancer	• Nós de administração • Nós de gateway
Acesso ao cliente S3 ou Swift — serviço CLB **Nota:** o serviço CLB está obsoleto.	• Nós de gateway

Limitações do uso de grupos de HA com Grid Manager ou Tenant Manager

A falha de serviços para o Gerenciador de Grade ou o Gerenciador de locatário não aciona o failover dentro do grupo de HA.

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 de administração principal não está disponível. Durante o failover, você pode usar o Gerenciador de Grade para monitorar seu sistema StorageGRID.

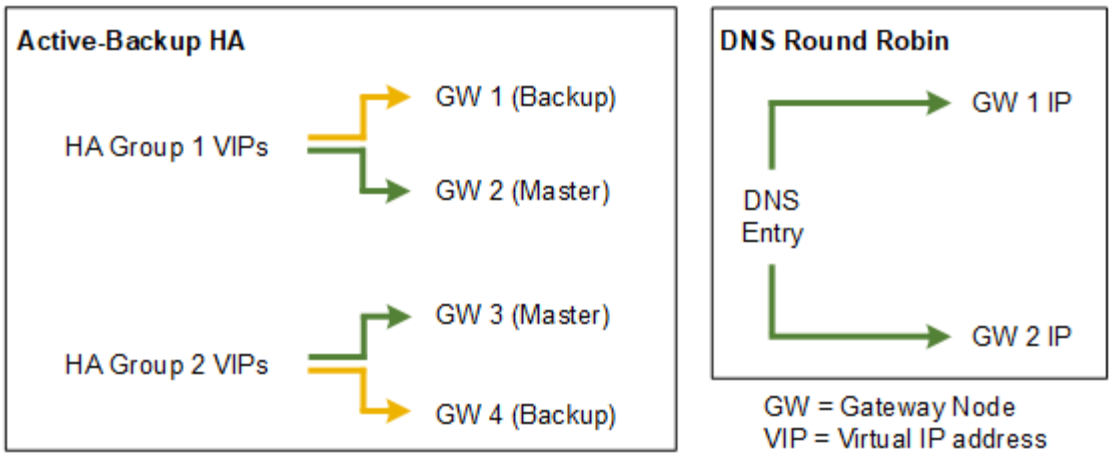
Limitações do uso de grupos HA com o serviço CLB

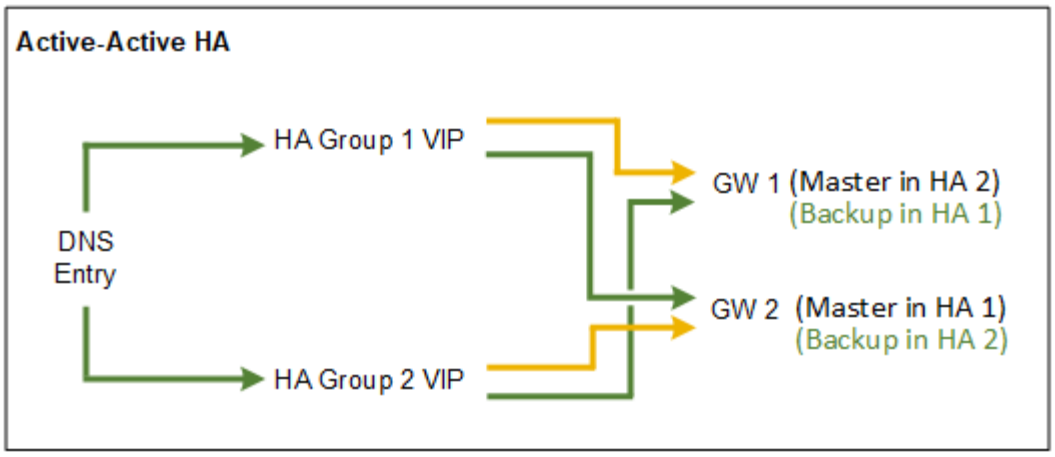
A falha do serviço CLB não aciona o failover no grupo HA.

O serviço CLB está obsoleto.

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.





Ao criar vários grupos de HA sobrepostos, como mostrado no exemplo de HA ativo-ativo, a taxa de transferência total é dimensionada com o número de nós e grupos de HA. Com três ou mais nós e três ou mais grupos de HA, você também pode continuar as operações usando qualquer um dos VIPs, mesmo durante procedimentos de manutenção que exigem que você coloque um nó off-line.

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.
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.

Configuração	Vantagens	Desvantagens
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.

Criando um grupo de alta disponibilidade

Você pode criar um ou mais grupos de alta disponibilidade (HA) para fornecer acesso altamente disponível aos serviços em nós de administração ou nós de gateway.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

Uma interface deve atender às seguintes condições para ser incluída em um grupo HA:

- A interface deve ser para um nó de gateway ou um nó de administrador.
- A interface deve pertencer à rede de Grade (eth0) ou à rede de Cliente (eth2).
- A interface deve ser configurada com endereçamento IP fixo ou estático, não com DHCP.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

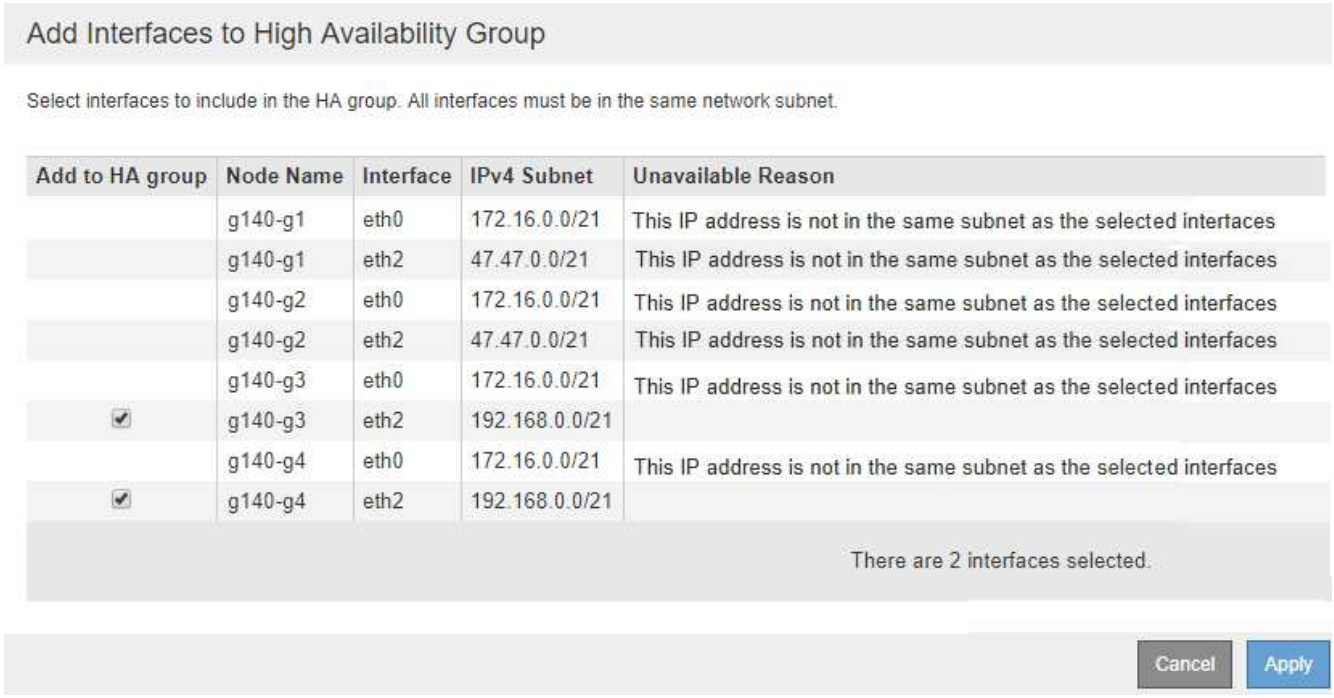
   A página grupos de alta disponibilidade é exibida.

2. Clique em **criar**.

   A caixa de diálogo criar Grupo de alta disponibilidade é exibida.

3. Digite um nome e, se desejado, uma descrição para o grupo HA.
4. Clique em **Select interfaces**.

   A caixa de diálogo Adicionar interfaces ao Grupo de alta disponibilidade é exibida. A tabela lista nós, interfaces e sub-redes IPv4 elegíveis.



Uma interface não aparece na lista se o seu endereço IP for atribuído pelo DHCP.

5. Na coluna **Adicionar ao grupo HA**, marque a caixa de seleção da interface que deseja adicionar ao grupo HA.

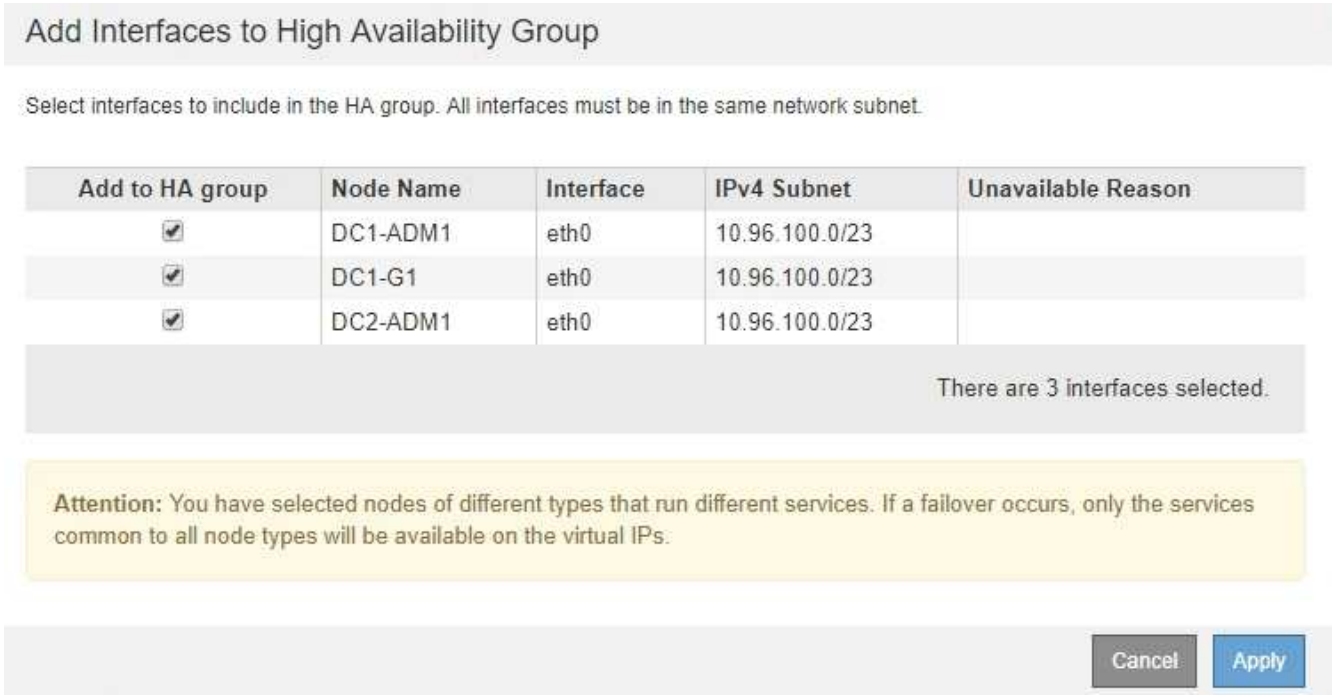
   Observe as seguintes diretrizes para selecionar interfaces:

   - Você deve selecionar pelo menos uma interface.
   - Se você selecionar mais de uma interface, todas as interfaces devem estar na rede de Grade (eth0) ou na rede de Cliente (eth2).
   - Todas as interfaces devem estar na mesma sub-rede ou em sub-redes com um prefixo comum.

     Os endereços IP serão restritos à sub-rede menor (aquela com o maior prefixo).

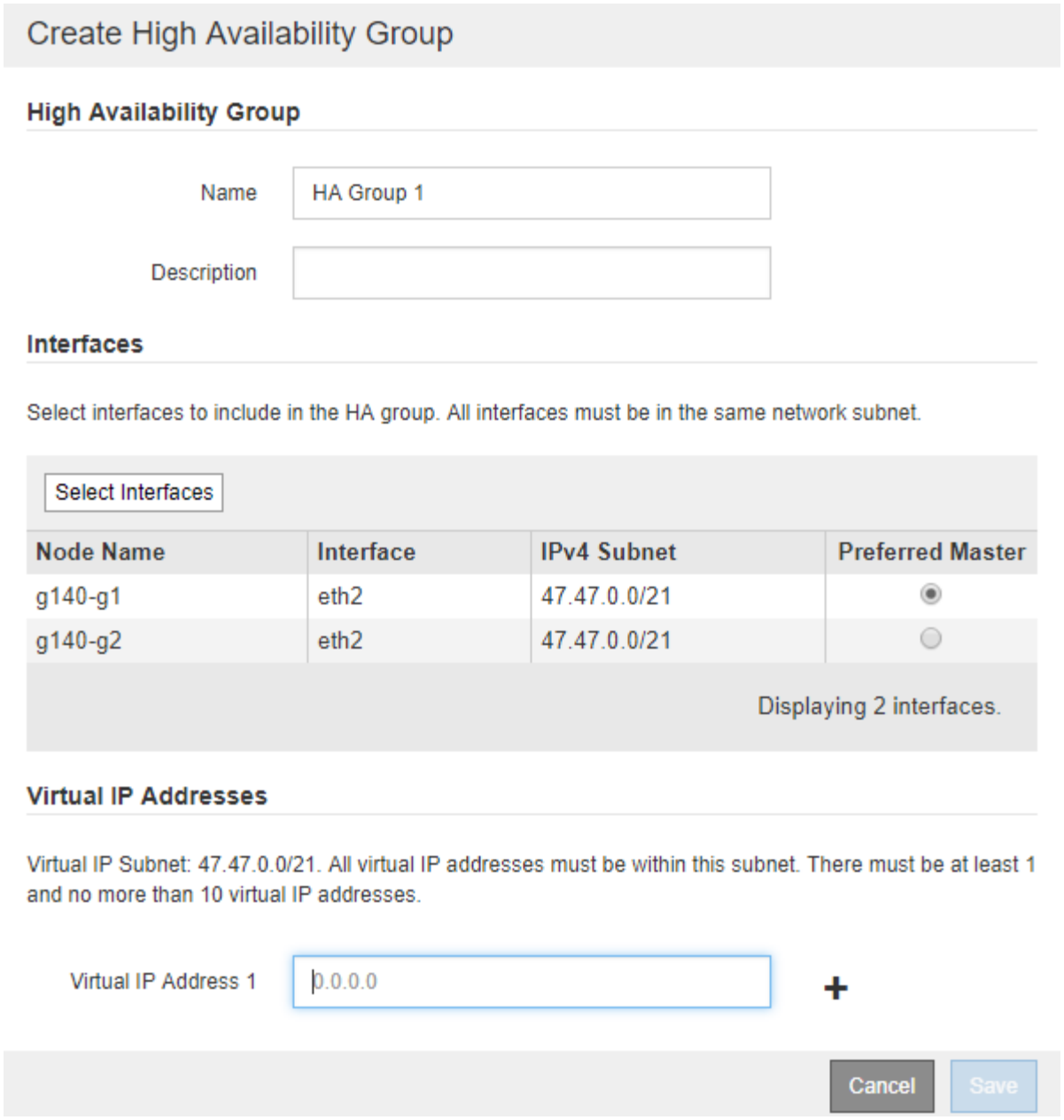
   - Se você selecionar interfaces em diferentes tipos de nós e ocorrer um failover, apenas os serviços comuns aos nós selecionados estarão disponíveis nos IPs virtuais.
     - Selecione dois ou mais nós de administração para proteção de HA do Grid Manager ou do Tenant Manager.
     - Selecione dois ou mais nós de administração, nós de gateway ou ambos para proteção de HA do serviço Load Balancer.
     - Selecione dois ou mais nós de Gateway para proteção de HA do serviço CLB.

       O serviço CLB está obsoleto.



6. Clique em **aplicar**.

   As interfaces selecionadas são listadas na seção interfaces da página criar Grupo de alta disponibilidade. Por padrão, a primeira interface na lista é selecionada como o mestre preferido.



7. Se você quiser que uma interface diferente seja o mestre preferido, selecione essa interface na coluna **Preferred Master**.

   O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup.

   > Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deve selecionar uma interface no nó Admin principal para ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

8. Na seção endereços IP virtuais da página, insira um a 10 endereços IP virtuais para o grupo HA. Clique no sinal de mais (+) para adicionar vários endereços IP.

   Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

   Os endereços IPv4 devem estar dentro da sub-rede IPv4 compartilhada por todas as interfaces membros.

9. Clique em **Salvar**.

   O Grupo HA é criado e agora você pode usar os endereços IP virtuais configurados.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale o VMware"

"Instale Ubuntu ou Debian"

"Gerenciamento do balanceamento de carga"

Edição de um grupo de alta disponibilidade

Você pode editar um grupo de alta disponibilidade (HA) para alterar seu nome e descrição, adicionar ou remover interfaces ou adicionar ou atualizar um endereço IP virtual.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

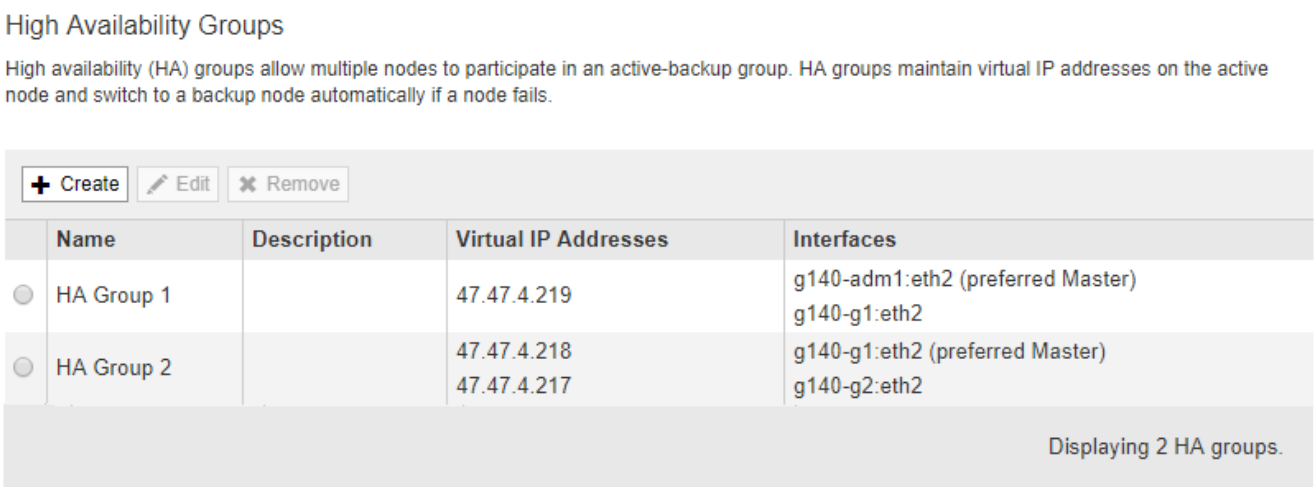
Algumas das razões para editar um grupo HA incluem o seguinte:

- Adicionando uma interface a um grupo existente. O endereço IP da interface deve estar dentro da mesma sub-rede que outras interfaces já atribuídas ao grupo.
- Remover uma interface de um grupo de HA. Por exemplo, você não pode iniciar um procedimento de desativação de site ou nó se a interface de um nó para a rede de Grade ou a rede de cliente for usada em um grupo HA.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

   A página grupos de alta disponibilidade é exibida.

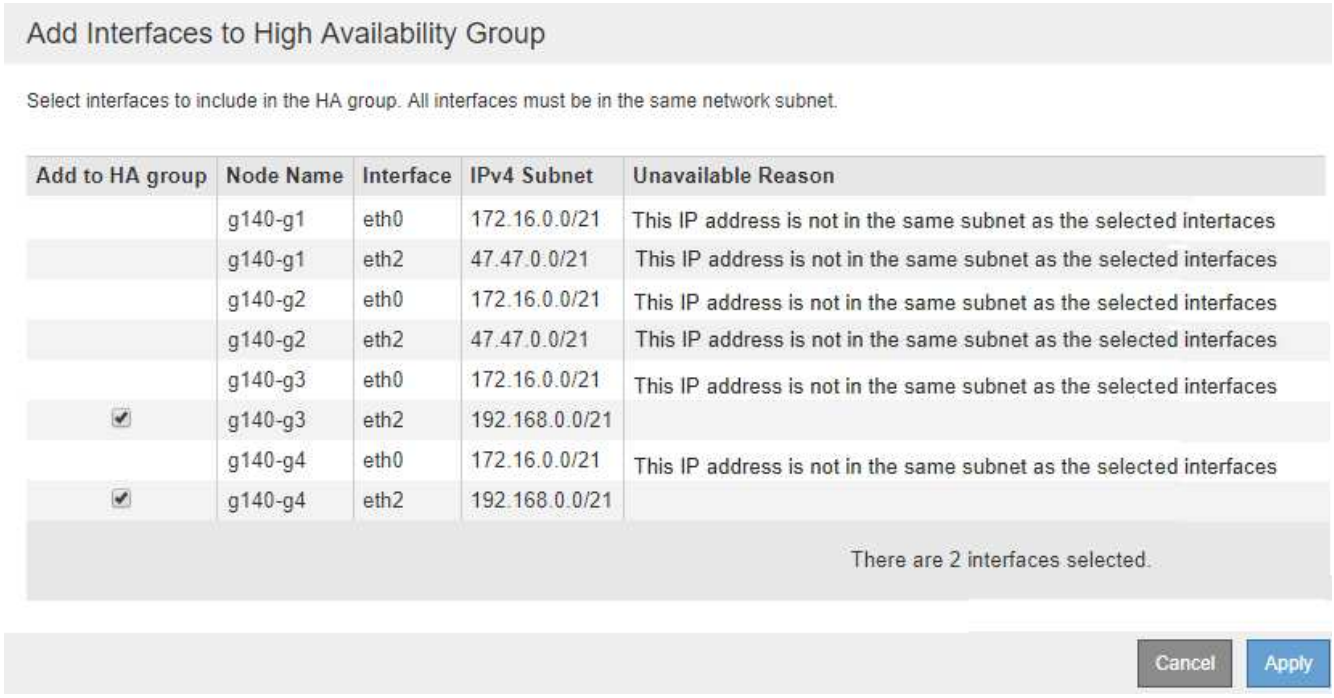


2. Selecione o grupo HA que deseja editar e clique em **Editar**.

   A caixa de diálogo Editar Grupo de alta disponibilidade é exibida.

3. Opcionalmente, atualize o nome ou a descrição do grupo.
4. Opcionalmente, clique em **Select interfaces** para alterar as interfaces do Grupo HA.

   A caixa de diálogo Adicionar interfaces ao Grupo de alta disponibilidade é exibida.



   Uma interface não aparece na lista se o seu endereço IP for atribuído pelo DHCP.

5. Selecione ou desmarque as caixas de seleção para adicionar ou remover interfaces.

   Observe as seguintes diretrizes para selecionar interfaces:

   - Você deve selecionar pelo menos uma interface.
   - Se você selecionar mais de uma interface, todas as interfaces devem estar na rede de Grade (eth0) ou na rede de Cliente (eth2).
   - Todas as interfaces devem estar na mesma sub-rede ou em sub-redes com um prefixo comum.

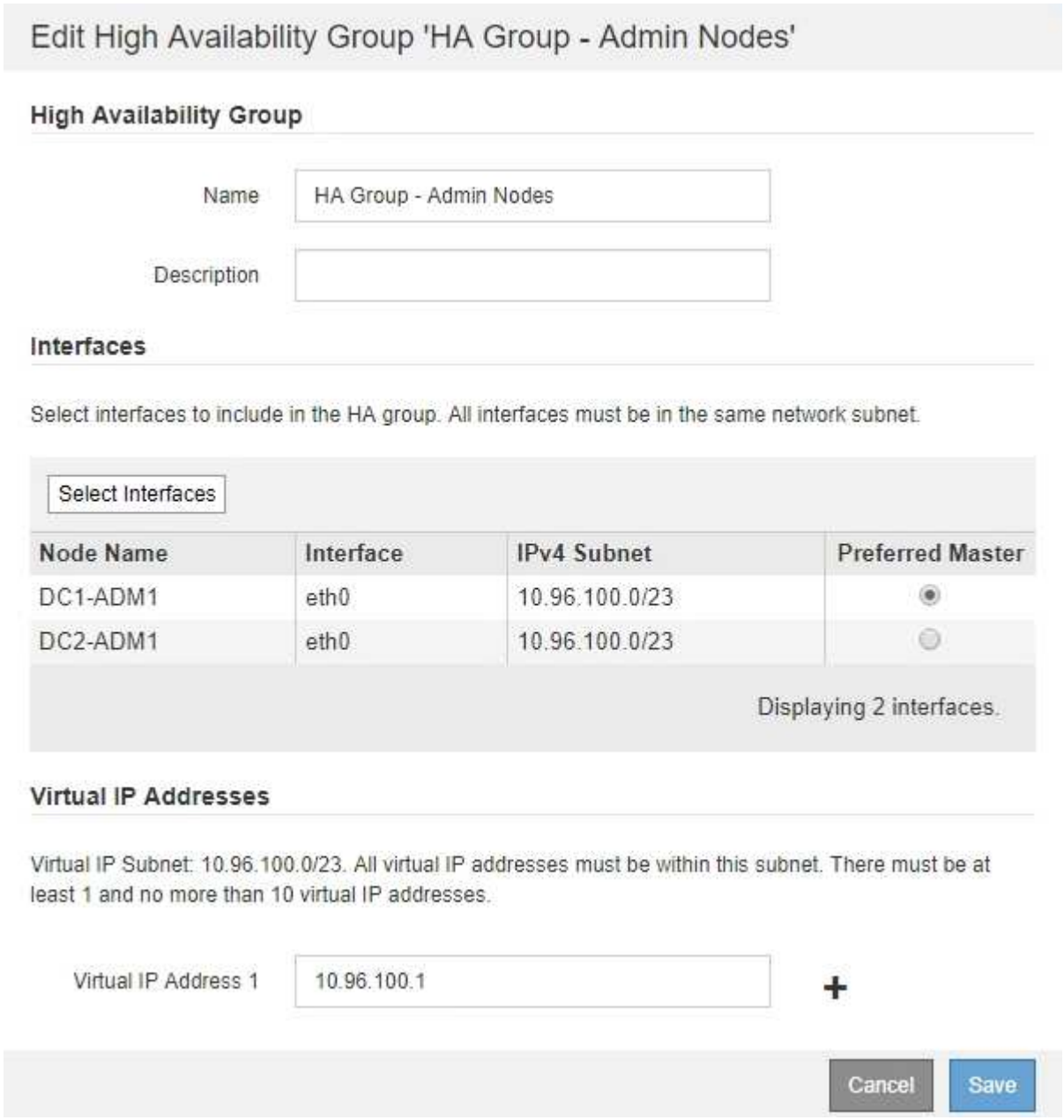
     Os endereços IP serão restritos à sub-rede menor (aquela com o maior prefixo).

   - Se você selecionar interfaces em diferentes tipos de nós e ocorrer um failover, apenas os serviços comuns aos nós selecionados estarão disponíveis nos IPs virtuais.
     - Selecione dois ou mais nós de administração para proteção de HA do Grid Manager ou do Tenant Manager.
     - Selecione dois ou mais nós de administração, nós de gateway ou ambos para proteção de HA do serviço Load Balancer.
     - Selecione dois ou mais nós de Gateway para proteção de HA do serviço CLB.

       O serviço CLB está obsoleto.

6. Clique em **aplicar**.

   As interfaces selecionadas são listadas na seção interfaces da página. Por padrão, a primeira interface na lista é selecionada como o mestre preferido.



7. Se você quiser que uma interface diferente seja o mestre preferido, selecione essa interface na coluna **Preferred Master**.

   O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup.

   Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deve selecionar uma interface no nó Admin principal para ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

8. Opcionalmente, atualize os endereços IP virtuais para o grupo HA.

Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

Os endereços IPv4 devem estar dentro da sub-rede IPv4 compartilhada por todas as interfaces membros.

9. Clique em **Salvar**.

   O Grupo HA é atualizado.

Removendo um grupo de alta disponibilidade

Você pode remover um grupo de alta disponibilidade (HA) que não esteja mais usando.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

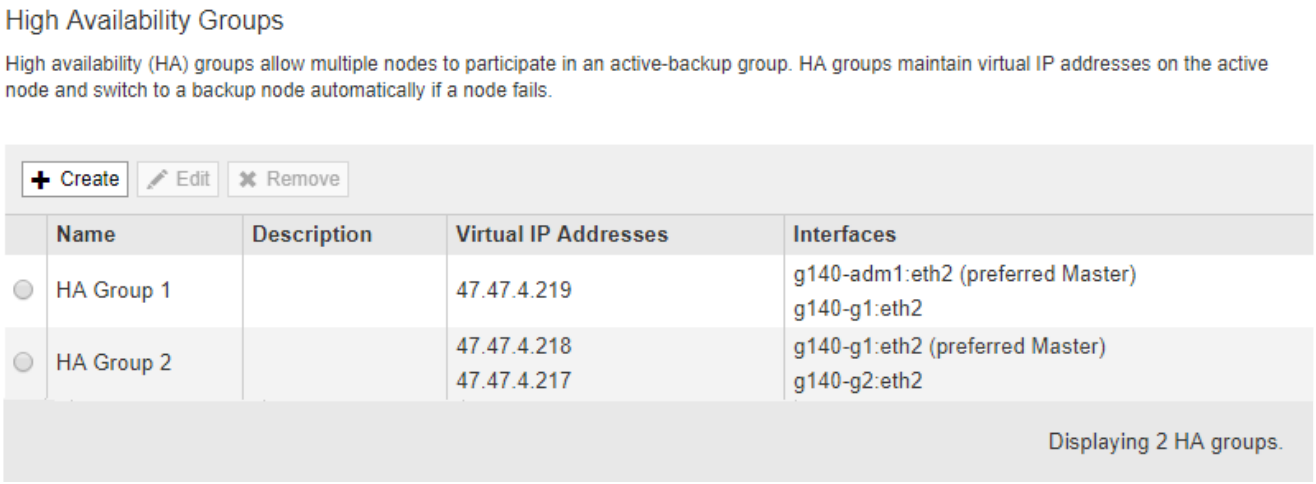
Aborde esta tarefa

Se você remover um grupo HA, qualquer cliente S3 ou Swift configurado para usar um dos endereços IP virtuais do grupo não poderá mais se conetar ao StorageGRID. Para evitar interrupções do cliente, você deve atualizar todos os aplicativos clientes S3 ou Swift afetados antes de remover um grupo 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 ou usando DHCP.

Passos

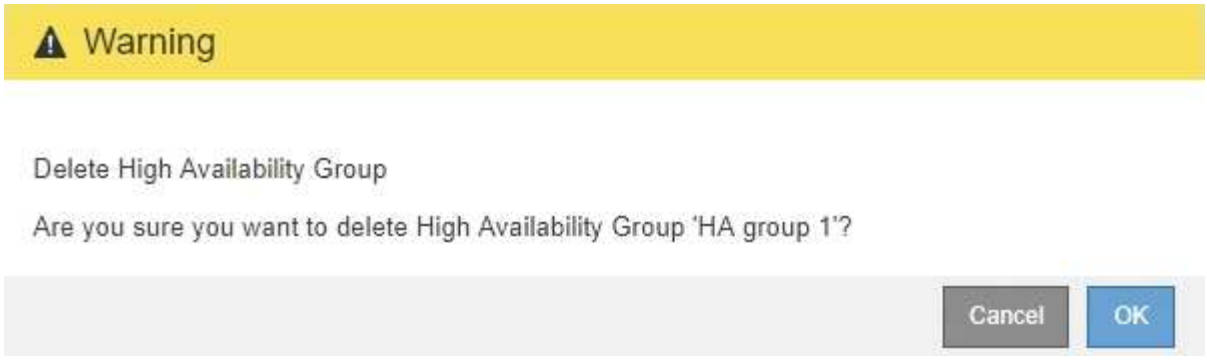
1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

   A página grupos de alta disponibilidade é exibida.



2. Selecione o grupo HA que deseja remover e clique em **Remover**.

   O aviso Excluir Grupo de alta disponibilidade é exibido.



3. Clique em **OK**.

   O grupo HA é removido.

Configurando nomes de domínio de endpoint da API S3

Para oferecer suporte a solicitações de estilo hospedado virtual S3, você deve usar o Gerenciador de Grade para configurar a lista de nomes de domínio de endpoint aos quais os clientes S3 se conetam.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter confirmado 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 executar todas as seguintes tarefas:

- 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 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.

O certificado que um cliente usa para conexões HTTPS depende de como o cliente se coneta à grade:

- Se um cliente se conetar usando o serviço Load Balancer, ele usará o certificado para um ponto de extremidade específico do balanceador de carga.

  Cada ponto de extremidade do balanceador de carga tem seu próprio certificado e cada ponto de extremidade pode ser configurado para reconhecer nomes de domínio de endpoint diferentes.

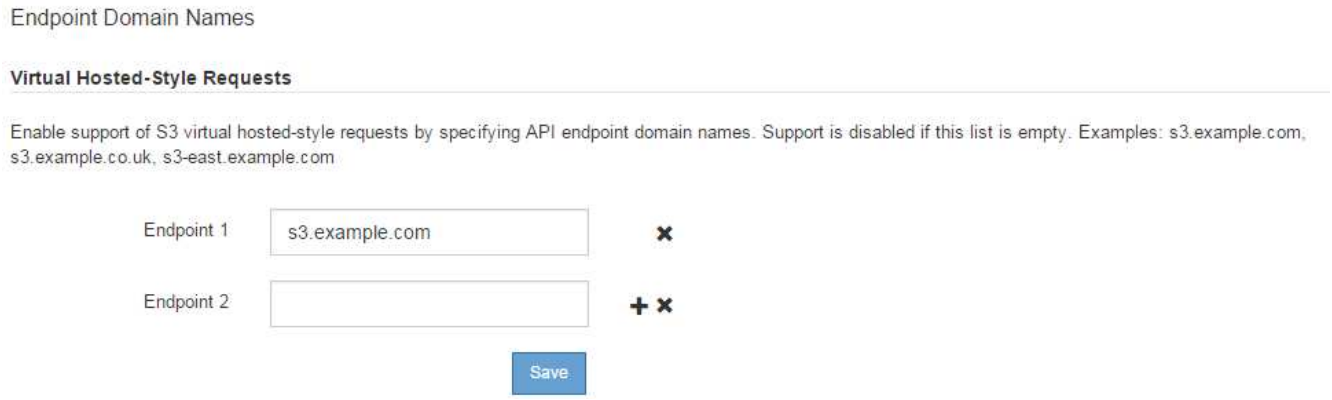
- Se o cliente se conetar a um nó de armazenamento ou ao serviço CLB em um nó de gateway, o cliente usará um certificado de servidor personalizado de grade que foi atualizado para incluir todos os nomes de domínio de endpoint necessários.

  O serviço CLB está obsoleto.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **nomes de domínio**.

   A página nomes de domínio do endpoint é exibida.



2. Para adicionar campos adicionais, insira a lista de nomes de domínio de endpoint da API S3 nos campos **Endpoint**.

   Se esta lista estiver vazia, o suporte para solicitações de estilo hospedado virtual S3 será desativado.

3. Clique em **Salvar**.
4. Certifique-se de que os certificados de servidor que os clientes utilizam correspondem aos nomes de domínio de endpoint necessários.
   - Para clientes que usam o serviço Load Balancer, atualize o certificado associado ao ponto de extremidade do balanceador de carga ao qual o cliente se coneta.
   - Para clientes que se conetam diretamente aos nós de storage ou que usam o serviço CLB nos nós de Gateway, atualize o certificado de servidor personalizado para a grade.

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.

Informações relacionadas

"Use S3"

"Visualização de endereços IP"

"Criando um grupo de alta disponibilidade"

"Configurando um certificado de servidor personalizado para conexões ao nó de armazenamento ou ao serviço CLB"

"Configuração dos pontos de extremidade do balanceador de carga"

Ativar HTTP para comunicações cliente

Por padrão, os aplicativos clientes usam o protocolo de rede HTTPS para todas as conexões com nós de armazenamento ou para o serviço CLB obsoleto em nós de gateway. Opcionalmente, você pode ativar o HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Conclua esta tarefa somente se os clientes S3 e Swift precisarem fazer conexões HTTP diretamente aos nós de armazenamento ou ao serviço CLB obsoleto nos nós de Gateway.

Não é necessário concluir essa tarefa para clientes que usam somente conexões HTTPS ou para clientes que se conetam ao serviço Load Balancer (porque você pode configurar cada ponto de extremidade do Load Balancer para usar HTTP ou HTTPS). Consulte as informações sobre como configurar pontos de extremidade do balanceador de carga para obter mais informações.

"Resumo: Endereços IP e portas para conexões de clientes"Consulte para saber quais portas S3 e clientes Swift usam ao se conetar a nós de armazenamento ou ao serviço CLB obsoleto usando HTTP ou HTTPS

> Tenha cuidado ao ativar o HTTP para uma grade de produção porque as solicitações serão enviadas sem criptografia.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de rede, marque a caixa de seleção **Ativar conexão HTTP** .

3. Clique em **Salvar**.

Informações relacionadas

"Configuração dos pontos de extremidade do balanceador de carga"

"Use S3"

"Use Swift"

Controlar quais operações do cliente são permitidas

Você pode selecionar a opção Prevent Client Modification grid (impedir a modificação do cliente) para negar operações específicas do cliente HTTP.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Impedir Modificação do Cliente é uma configuração de todo o sistema. Quando a opção impedir modificação de cliente é selecionada, as seguintes solicitações são negadas:

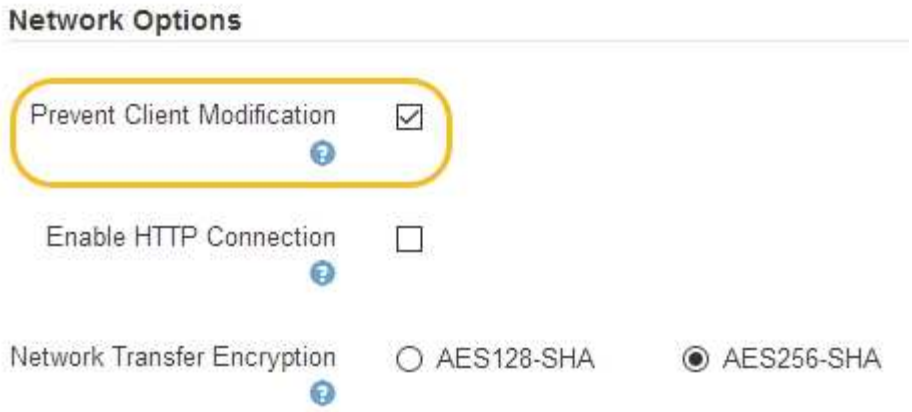
- **S3 API REST**
  - Eliminar pedidos de balde
  - Quaisquer solicitações para modificar os dados de um objeto existente, metadados definidos pelo usuário ou marcação de objeto S3

> Esta configuração não se aplica a buckets com controle de versão ativado. O controle de versão já impede modificações nos dados do objeto, metadados definidos pelo usuário e marcação de objetos.

- * Swift REST API*
  - Eliminar pedidos de contentor
  - Solicitações para modificar qualquer objeto existente. Por exemplo, as seguintes operações são negadas: Put Overwrite, Delete, Metadata Update e assim por diante.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de rede, marque a caixa de seleção **impedir modificação de cliente**.



3. Clique em **Salvar**.

Gerenciamento de redes e conexões StorageGRID

Você pode usar o Gerenciador de Grade para configurar e gerenciar redes e conexões StorageGRID.

"Configurando conexões de cliente S3 e Swift"Consulte para saber como conetar clientes S3 ou Swift.

- "Diretrizes para redes StorageGRID"
- "Visualização de endereços IP"
- "Cifras suportadas para conexões TLS de saída"
- "Alteração da encriptação de transferência de rede"
- "Configurando certificados de servidor"
- "Configurando as configurações de proxy de armazenamento"
- "Configurando as configurações de proxy Admin"
- "Gerir políticas de classificação de tráfego"
- "Quais são os custos da ligação"

Diretrizes para redes StorageGRID

O 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 modificar ou adicionar uma rede para um nó de grade, consulte as instruções de recuperação e manutenção. Para obter mais informações sobre a topologia de rede, consulte as instruções de rede.

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 e Swift, para que a rede de Grade possa ser isolada e protegida. A rede do cliente pode se comunicar com qualquer sub-rede acessível através do gateway local.

Diretrizes

- Cada nó de grade do 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.

Informações relacionadas

"Manter recuperar"

"Diretrizes de rede"

Visualização de 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.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

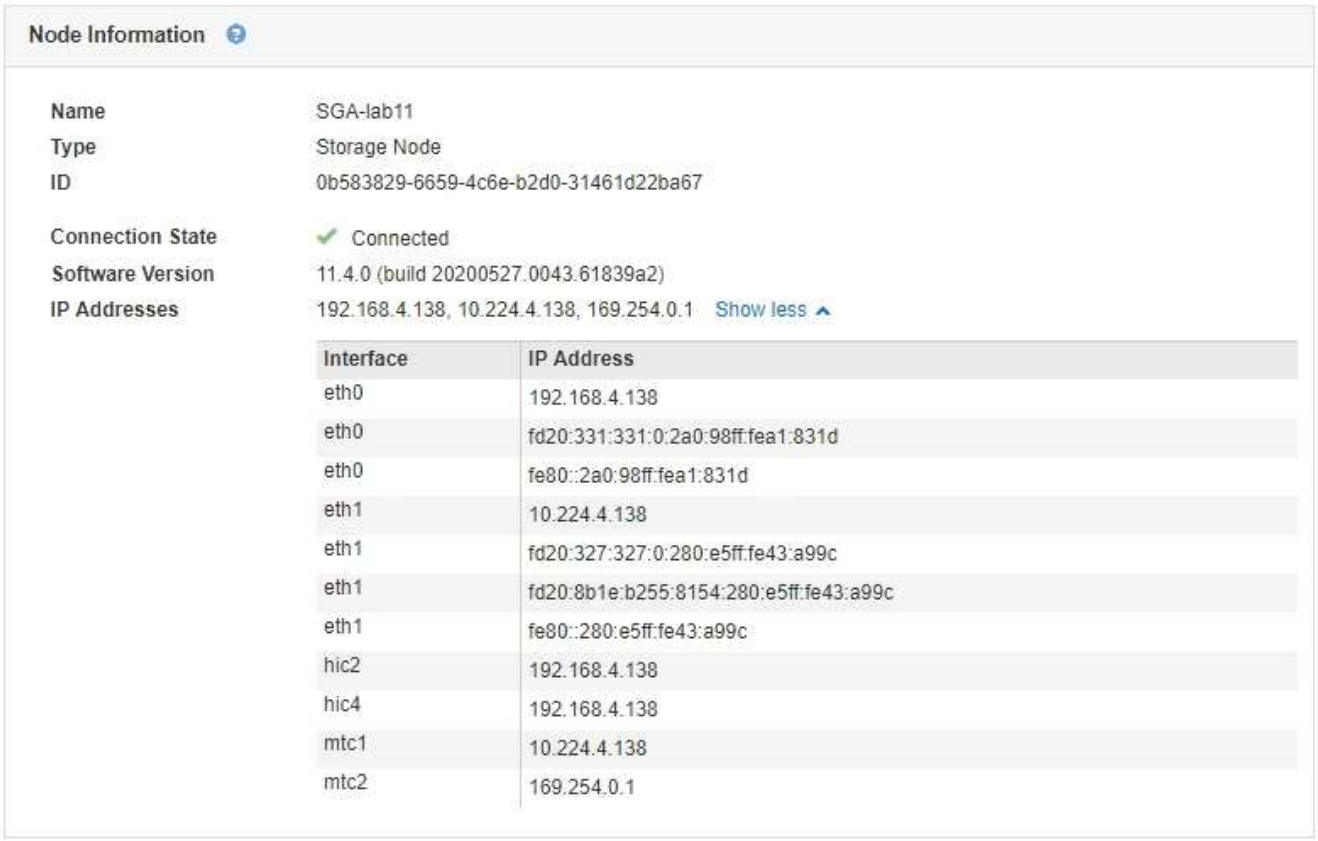
Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, consulte as instruções de recuperação e manutenção.

Passos

1. Selecione **nodes** > ***grid node*** > **Visão geral**.
2. Clique em **Mostrar mais** à direita do título de endereços IP.

   Os endereços IP desse nó de grade são listados em uma tabela.



Informações relacionadas

"Manter recuperar"

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 ou Swift.

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.

Pacotes de codificação TLS 1,2 suportados

Os seguintes conjuntos de codificação TLS 1,2 são suportados:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Pacotes de codificação TLS 1,3 suportados

Os seguintes conjuntos de codificação TLS 1,3 são suportados:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Alteração da encriptação de transferência de rede

O sistema StorageGRID usa a Segurança da camada de Transporte (TLS) para proteger o tráfego de controle interno entre nós de grade. A opção Network Transfer Encryption (encriptação de transferência de rede) define o algoritmo utilizado pelo TLS para encriptar o tráfego de controlo entre nós de grelha. Esta definição não afeta a encriptação de dados.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Por padrão, a criptografia de transferência de rede usa o algoritmo AES256-SHA. O tráfego de controle também pode ser criptografado usando o algoritmo AES128-SHA.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de rede, altere criptografia de transferência de rede para **AES128-SHA** ou **AES256-SHA** (padrão).

3. Clique em **Salvar**.

Configurando certificados de servidor

Você pode personalizar os certificados de servidor usados pelo sistema StorageGRID.

O sistema StorageGRID usa certificados de segurança para vários fins distintos:

- Certificados de servidor 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 de locatário.
- Certificados de servidor de API de storage: Usado para proteger o acesso aos nós de armazenamento e nós de Gateway, que os aplicativos de cliente de API usam para carregar e baixar dados de objeto.

Você pode usar os certificados padrão criados durante a instalação, ou pode substituir qualquer um desses tipos padrão de certificados por seus próprios certificados personalizados.

Tipos suportados de certificado de servidor personalizado

O sistema StorageGRID suporta certificados de servidor personalizados criptografados com RSA ou ECDSA (algoritmo de assinatura digital de curva elítica).

Para obter mais informações sobre como o StorageGRID protege conexões de clientes para a API REST, consulte os guias de implementação S3 ou Swift.

Certificados para pontos de extremidade do balanceador de carga

O StorageGRID gerencia os certificados usados para pontos de extremidade do balanceador de carga separadamente. Para configurar os certificados do balanceador de carga, consulte as instruções para configurar os pontos de extremidade do balanceador de carga.

Informações relacionadas

"Use S3"

"Use Swift"

"Configuração dos pontos de extremidade do balanceador de carga"

Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário

Você pode substituir o certificado de servidor StorageGRID padrão por um único certificado de servidor personalizado que permite aos usuários acessar o Gerenciador de Grade e o Gerenciador de locatário sem encontrar avisos de segurança.

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 servidor personalizado comum e uma chave privada correspondente.

Como um único certificado de servidor personalizado é usado para todos os nós de administração, você deve especificar o certificado como um certificado de curinga ou de vários domínios 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 raiz 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** e o alarme legado de expiração de certificado de Interface de Gerenciamento (MCEP) são acionados quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode visualizar o número de dias até que o certificado de serviço atual expire selecionando **Support** > **Tools** > **Grid Topology**. Em seguida, selecione ***Primary Admin Node*** > **CMN** > **Resources**.

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 do servidor de interface de gerenciamento personalizado expira.
- Você reverte de um certificado de servidor de interface de gerenciamento personalizado para o certificado de servidor padrão.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção certificado do servidor de interface de gerenciamento, clique em **Instalar certificado personalizado**.
3. Carregue os ficheiros de certificado do servidor necessários:
   - **Certificado do servidor**: O arquivo de certificado do servidor personalizado (`.crt`).
   - **Chave privada do certificado do servidor**: O arquivo de chave privada do certificado do servidor personalizado (`.key`).

     As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

   - **CA Bundle**: Um único arquivo 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.
4. Clique em **Salvar**.

   Os certificados de servidor personalizados são usados para todas as novas conexões de cliente subsequentes.

   Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor

StorageGRID ou um certificado assinado pela CA que foi carregado.

> Depois de carregar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados (ou alarmes legados) sejam apagados.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

Restaurando os certificados de servidor padrão para o Gerenciador de Grade e o Gerenciador de locatário

Você pode reverter para o uso dos certificados de servidor padrão para o Gerenciador de Grade e o Gerenciador de locatário.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Gerenciar certificado do servidor de interface, clique em **usar certificados padrão**.
3. Clique em **OK** na caixa de diálogo de confirmação.

   Quando você restaura os certificados de servidor padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. Os certificados de servidor padrão são usados para todas as novas conexões de cliente subsequentes.

4. Atualize a página para garantir que o navegador da Web seja atualizado.

Configurando um certificado de servidor personalizado para conexões ao nó de armazenamento ou ao serviço CLB

Você pode substituir o certificado do servidor usado para conexões de cliente S3 ou Swift ao nó de armazenamento ou ao serviço CLB (obsoleto) no nó de gateway. O certificado de servidor personalizado de substituição é específico para a sua organização.

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, os usuários também podem precisar instalar o certificado CA raiz no cliente API S3 ou Swift que eles usarão 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 Server certificate for Storage API Endpoints** e o alarme legacy Storage API Service Endpoints Certificate Expiration (SCEP) são acionados quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode visualizar o número de dias até que o certificado de serviço atual expire selecionando **Support** > **Tools** > **Grid Topology**. Em seguida, selecione ***Primary Admin Node*** > **CMN** > **Resources**.

Os certificados personalizados só são usados se os clientes se conetarem ao StorageGRID usando o serviço CLB obsoleto nos nós do gateway ou se eles se conetarem diretamente aos nós de armazenamento. Os

clientes S3 ou Swift que se conetam ao StorageGRID usando o serviço de balanceador de carga em nós de administração ou nós de gateway usam o certificado configurado para o ponto de extremidade do balanceador de carga.

> O alerta **Expiration of load balancer endpoint certificate** é acionado para os pontos de extremidade do balanceador de carga que expirarão em breve.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Object Storage API Service Endpoints Server Certificate, clique em **Install Custom Certificate** (Instalar certificado personalizado).
3. Carregue os ficheiros de certificado do servidor necessários:
   - **Certificado do servidor**: O arquivo de certificado do servidor personalizado (`.crt`).
   - **Chave privada do certificado do servidor**: O arquivo de chave privada do certificado do servidor personalizado (`.key`).

     > As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

   - **CA Bundle**: Um único arquivo 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.
4. Clique em **Salvar**.

   O certificado de servidor personalizado é usado para todas as novas conexões de cliente API subsequentes.

   Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor StorageGRID ou um certificado assinado pela CA que foi carregado.

   > Depois de carregar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados (ou alarmes legados) sejam apagados.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

Informações relacionadas

"Use S3"

"Use Swift"

"Configurando nomes de domínio de endpoint da API S3"

Restaurando os certificados de servidor padrão para os endpoints S3 e Swift REST API

Você pode reverter para o uso dos certificados de servidor padrão para os endpoints da API REST S3 e Swift.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.

2. Na seção Object Storage API Service Endpoints Server Certificate (certificado do servidor de Endpoints), clique em **Use Default Certificates** (usar certificados padrão).
3. Clique em **OK** na caixa de diálogo de confirmação.

   Quando você restaura os certificados de servidor padrão para os endpoints da API de armazenamento de objetos, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. Os certificados de servidor padrão são usados para todas as novas conexões de cliente API subsequentes.

4. Atualize a página para garantir que o navegador da Web seja atualizado.

Copiar o certificado CA do sistema StorageGRID

O StorageGRID usa uma autoridade de certificação (CA) interna para proteger o tráfego interno. Este certificado não muda se você carregar seus próprios certificados.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

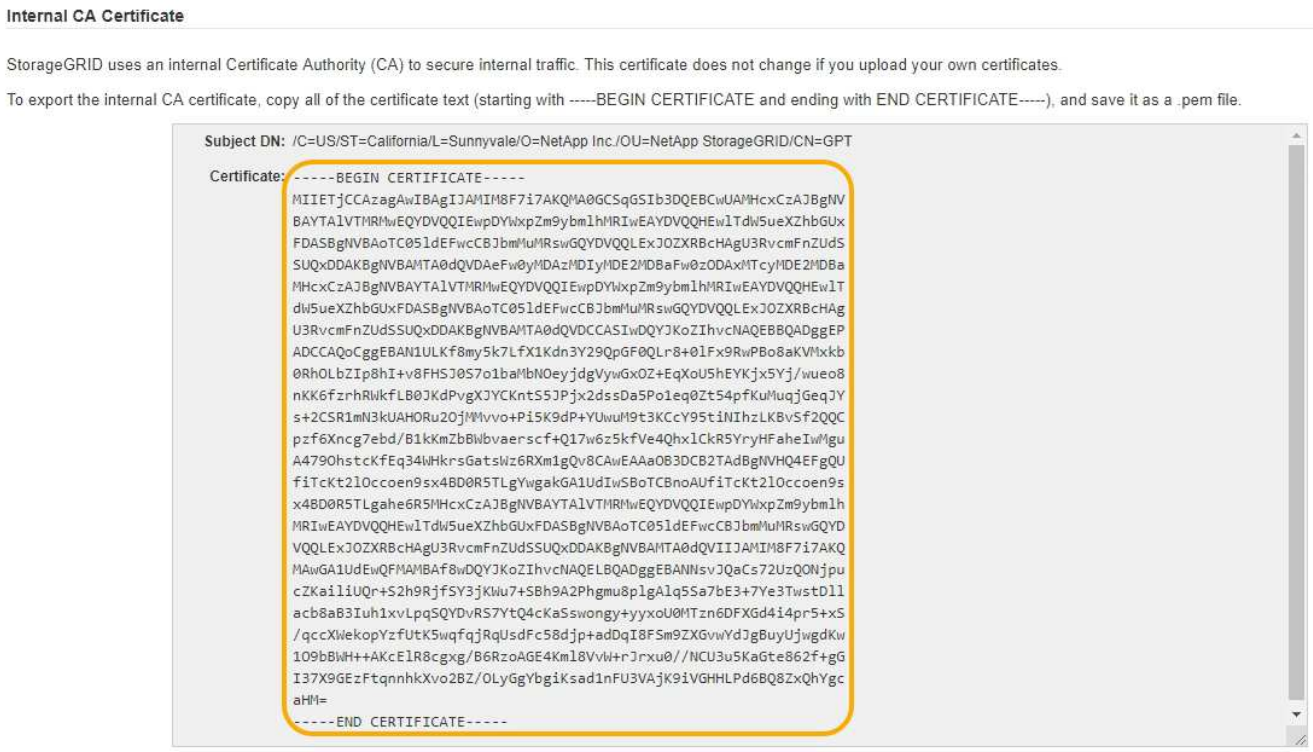
Sobre esta tarefa

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 **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção **certificado de CA interno**, selecione todo o texto do certificado.

   Você deve incluir `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` em sua seleção.



3. Clique com o botão direito do rato no texto selecionado e selecione **Copiar**.
4. Cole o certificado copiado em um editor de texto.
5. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Configurando 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.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Quando você cria um ponto de extremidade do 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, consulte as instruções de configuração do StorageGRID for FabricPool.

O serviço CLB (Connection Load Balancer) separado nos nós de gateway está obsoleto e não é mais recomendado para uso com o FabricPool.

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 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.

Informações relacionadas

"Configurar o StorageGRID para FabricPool"

Gerando um certificado de servidor autoassinado para a interface de gerenciamento

Você pode usar um script para gerar um certificado de servidor auto-assinado para clientes de API de gerenciamento que exigem validação estrita do nome de host.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Em ambientes de produção, você deve usar um certificado assinado por uma autoridade de certificação (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.

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 usado pelo Gerenciador de Grade e pelo Gerenciador de Tenant.
- 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 da API 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 365
```

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 **Configuração** > **certificados de servidor** > **certificado de servidor de interface de gerenciamento**.
7. Configure seu cliente de API de gerenciamento para usar o certificado público que você copiou. Inclua as tags DE INÍCIO e FIM.

Configurando as configurações de 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.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

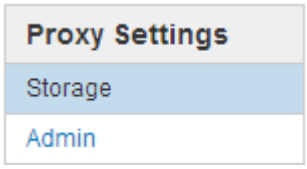
Sobre esta tarefa

Você pode configurar as configurações para um único proxy de armazenamento.

Passos

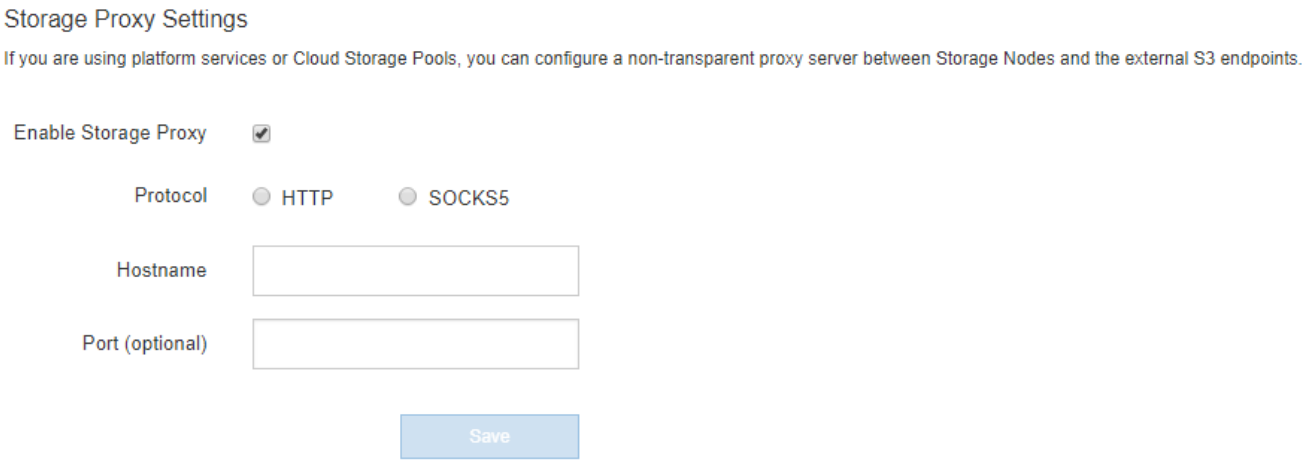
1. Selecione **Configuração** > **Configurações de rede** > **Configurações de proxy**.

   A página Configurações do proxy de armazenamento é exibida. Por padrão, **Storage** está selecionado no menu da barra lateral.

2. Marque a caixa de seleção **Enable Storage Proxy** (Ativar proxy de armazenamento*).

   Os campos para configurar um proxy de armazenamento são exibidos.

3. Selecione o protocolo para o proxy de armazenamento não transparente.
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.

   Você pode deixar este campo em branco se usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Clique em **Salvar**.

   Depois que o proxy Storage for 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.

Depois de terminar

Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção **Ativar proxy de armazenamento** e clique em **Salvar**.

Informações relacionadas

"Rede e portas para serviços de plataforma"

"Gerenciar objetos com ILM"

Configurando as configurações de proxy Admin

Se você enviar mensagens AutoSupport usando HTTP ou HTTPS, poderá configurar um servidor proxy não transparente entre nós de administração e suporte técnico (AutoSupport).

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

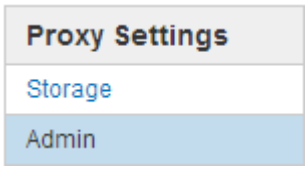
Você pode configurar as configurações para um único proxy Admin.

Passos

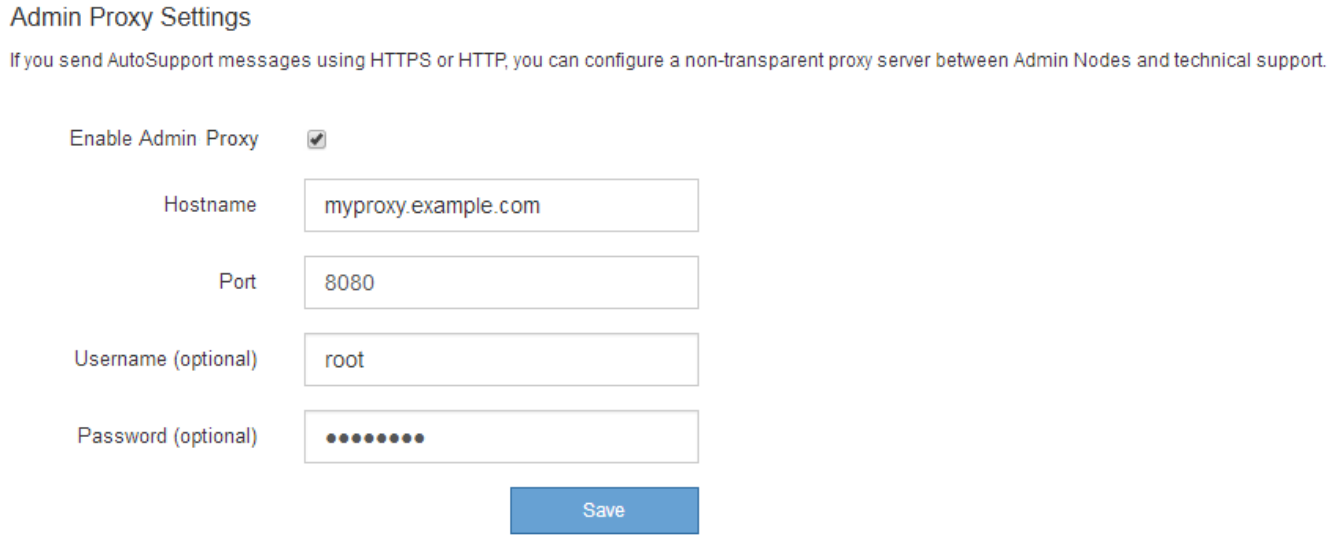
1. Selecione **Configuração** > **Configurações de rede** > **Configurações de proxy**.

   É apresentada a página Admin Proxy Settings (Definições de proxy de administração). Por padrão, **Storage** está selecionado no menu da barra lateral.

2. No menu da barra lateral, selecione **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 o nome de usuário do proxy.

   Deixe este campo em branco se o servidor proxy não exigir um nome de usuário.

7. Opcionalmente, insira a senha do proxy.

   Deixe este campo em branco se o servidor proxy não exigir uma senha.

8. Clique em **Salvar**.

   Depois que o proxy Admin é salvo, o servidor proxy entre nós Admin 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, desmarque a caixa de seleção **Ativar proxy Admin** e clique em **Salvar**.

Informações relacionadas

"Especificando o protocolo para mensagens AutoSupport"

Gerir políticas de classificação de tráfego

Para aprimorar suas ofertas de qualidade de serviço (QoS), você pode criar políticas de classificação de tráfego para identificar e monitorar diferentes tipos de tráfego de rede. Essas políticas podem ajudar na limitação e monitoramento de tráfego.

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 de correspondência e limites opcionais

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
- Inquilinos
- Sub-redes (IPv4 sub-redes contendo o cliente)
- Pontos finais (pontos finais 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.

Opcionalmente, você pode definir limites para uma política com base nos seguintes parâmetros:

- Agregar largura de banda em
- Agregar largura de banda para fora
- Solicitações de leitura simultânea
- Solicitações de gravação simultânea

- Largura de banda por solicitação in
- Saída de largura de banda por solicitação
- Leia a taxa de solicitação
- Taxa de solicitações de gravação

> 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.

Limitação de tráfego

Quando você criou políticas de classificação de tráfego, o tráfego é limitado de acordo com o tipo de regras e limites definidos. 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. 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.

Usando 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.

Os limites de classificação de tráfego são implementados 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.

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	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

Nível de serviço	Capacidade	Proteção de dados	Desempenho	Custo
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

Criando políticas de classificação de tráfego

Você cria políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por intervalo, locatário, sub-rede IP ou ponto de extremidade do balanceador de carga. Opcionalmente, você pode definir limites para uma política com base na largura de banda, no número de solicitações simultâneas ou na taxa de solicitações.

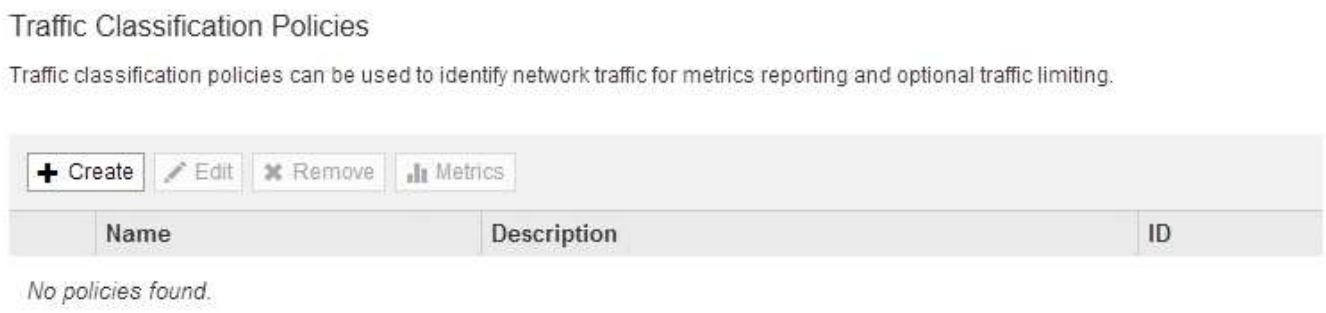
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.
- Você precisa ter criado os pontos de extremidade do balanceador de carga que você deseja corresponder.
- Você deve ter criado os inquilinos que você deseja corresponder.

Passos

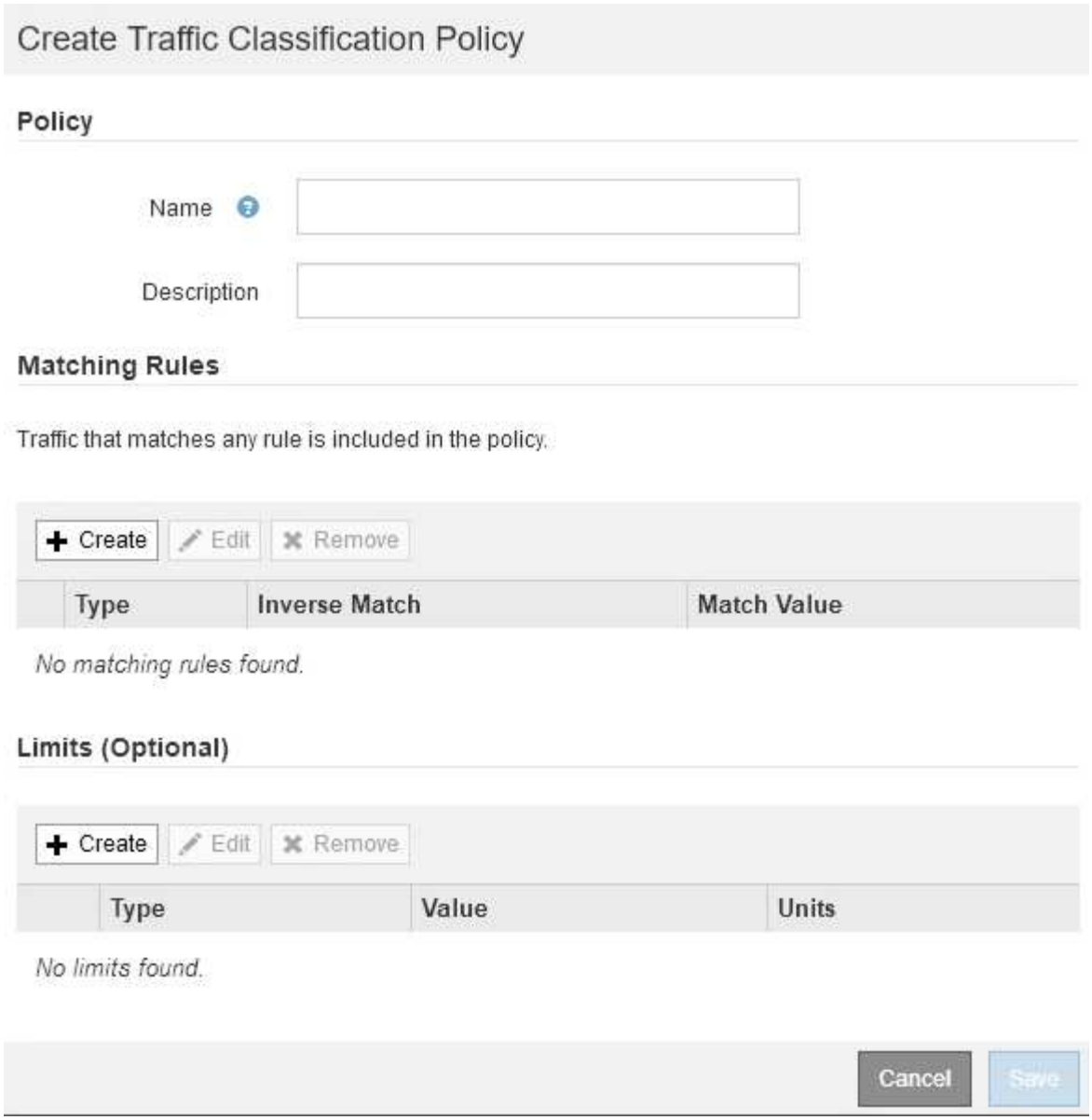
1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   É apresentada a página políticas de classificação de tráfego.



2. Clique em **criar**.

   É apresentada a caixa de diálogo criar política de classificação de tráfego.



3. No campo **Nome**, insira um nome para a política.

   Introduza um nome descritivo para que possa reconhecer a política.

4. Opcionalmente, adicione uma descrição para a política no campo **Description**.

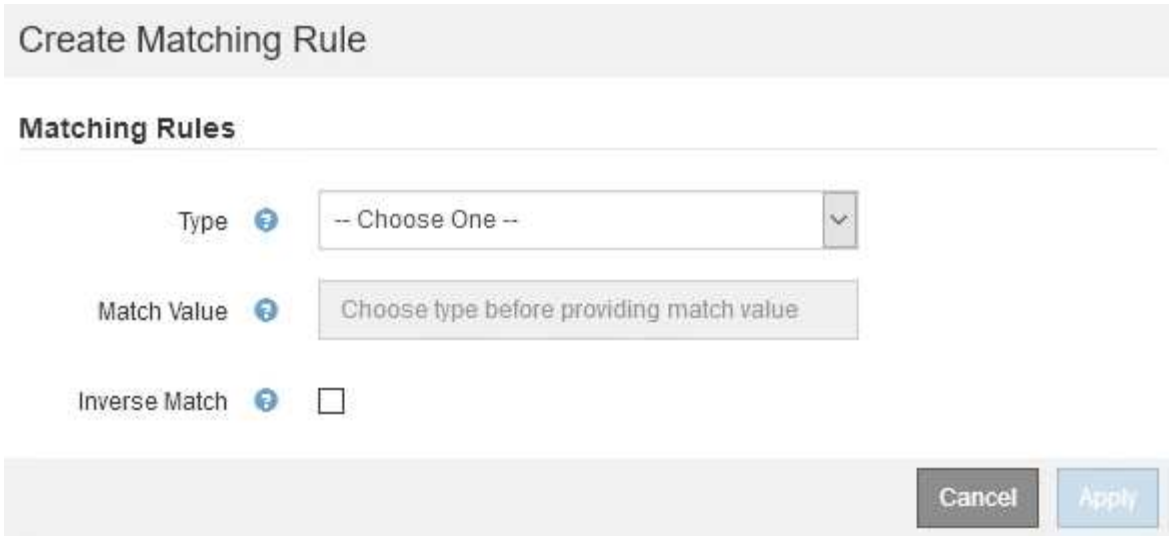
   Por exemplo, descreva ao que esta política de classificação de tráfego se aplica e ao que ela limitará.

5. Crie uma ou mais regras correspondentes para a política.

   Regras de correspondência controlam quais entidades serão afetadas por esta política de classificação de tráfego. Por exemplo, selecione Locatário se desejar que essa diretiva se aplique ao tráfego de rede de um locatário específico. Ou selecione ponto final se pretender que esta política se aplique ao tráfego de rede num ponto de extremidade do balanceador de carga específico.

   a. Clique em **criar** na seção **regras correspondentes**.

      A caixa de diálogo criar regra de correspondência é exibida.



b. Na lista suspensa **Type**, selecione o tipo de entidade a ser incluída na regra correspondente.

c. No campo **valor de correspondência**, insira um valor de correspondência com base no tipo de entidade que você escolheu.

   - Balde: Introduza um nome de intervalo.
   - Bucket Regex: Insira uma expressão regular que será usada para corresponder a um conjunto de nomes de bucket.

     A expressão regular não está ancorada. Use a âncora "caret" para corresponder ao início do nome do intervalo e use a âncora "doll" para corresponder ao final do nome.

   - CIDR: Insira uma sub-rede IPv4, na notação CIDR, que corresponda à sub-rede desejada.
   - Endpoint: Selecione um endpoint na lista de endpoints existentes. Esses são os pontos finais do balanceador de carga definidos na página pontos finais do balanceador de carga.
   - Locatário: Selecione um locatário na lista de inquilinos existentes. A correspondência de inquilinos baseia-se na propriedade do bucket que está sendo acessado. O acesso anônimo a um bucket corresponde ao locatário que possui o bucket.

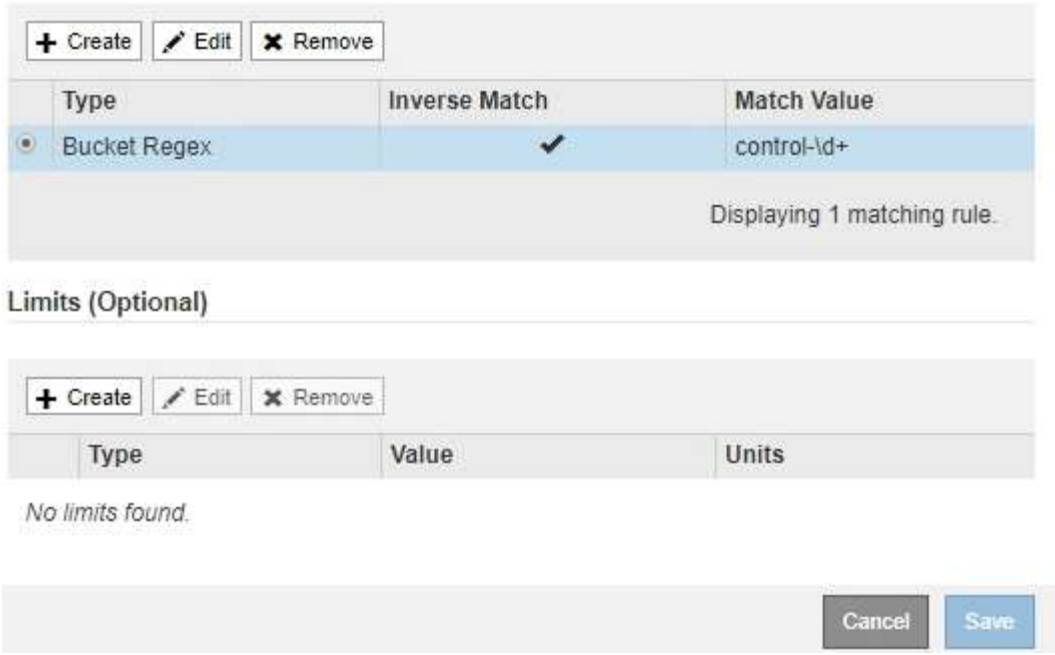
d. Se você quiser corresponder todo tráfego de rede *exceto* tráfego consistente com o valor tipo e correspondência definido, marque a caixa de seleção **Inverse**. Caso contrário, deixe a caixa de seleção desmarcada.

   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 **inverso**.

   > 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.

e. Clique em **aplicar**.

   A regra é criada e está listada na tabela regras correspondentes.



a. Repita estas etapas para cada regra que você deseja criar para a política.

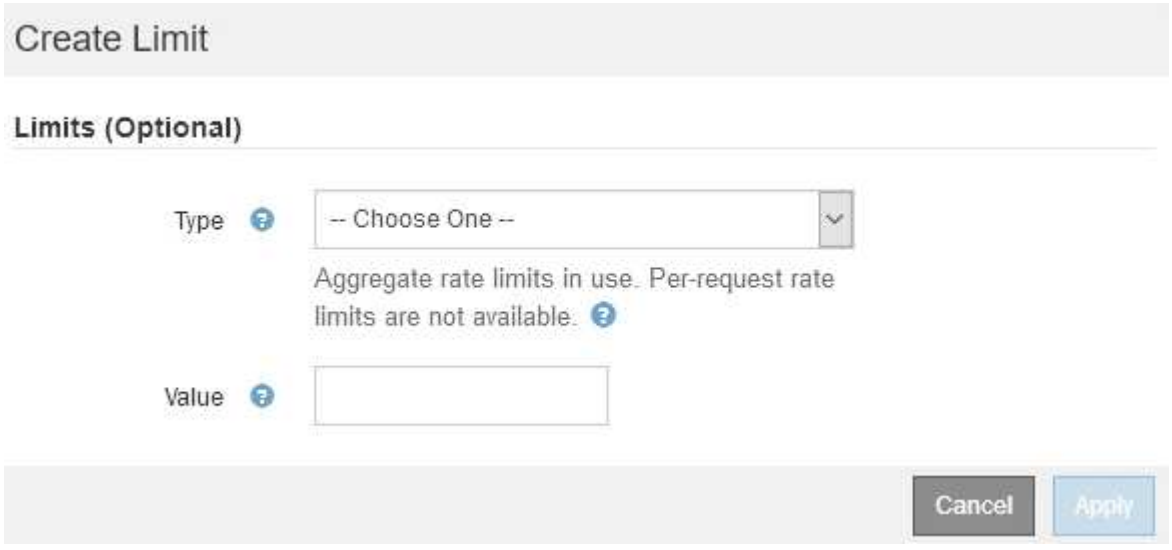
> O tráfego que corresponde a qualquer regra é Tratado pela política.

6. Opcionalmente, crie limites para a política.

> Mesmo que você não crie limites, o StorageGRID coleta métricas para que você possa monitorar o tráfego de rede que corresponde à política.

a. Clique em **criar** na seção **limites**.

A caixa de diálogo criar limite é exibida.



b. Na lista suspensa **Type**, selecione o tipo de limite que deseja aplicar à política.

Na lista a seguir, **in** refere-se ao tráfego de clientes S3 ou Swift para o balanceador de carga StorageGRID, e **OUT** refere-se ao tráfego do balanceador de carga para clientes S3 ou Swift.

- Agregar largura de banda em
- Agregar largura de banda para fora
- Solicitações de leitura simultânea
- Solicitações de gravação simultânea
- Largura de banda por solicitação in
- Saída de largura de banda por solicitação
- Leia a taxa de solicitação
- Taxa de solicitações de gravação

> 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, 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. A StorageGRID implementa as correspondências "melhores" para limites de largura de banda na seguinte ordem:

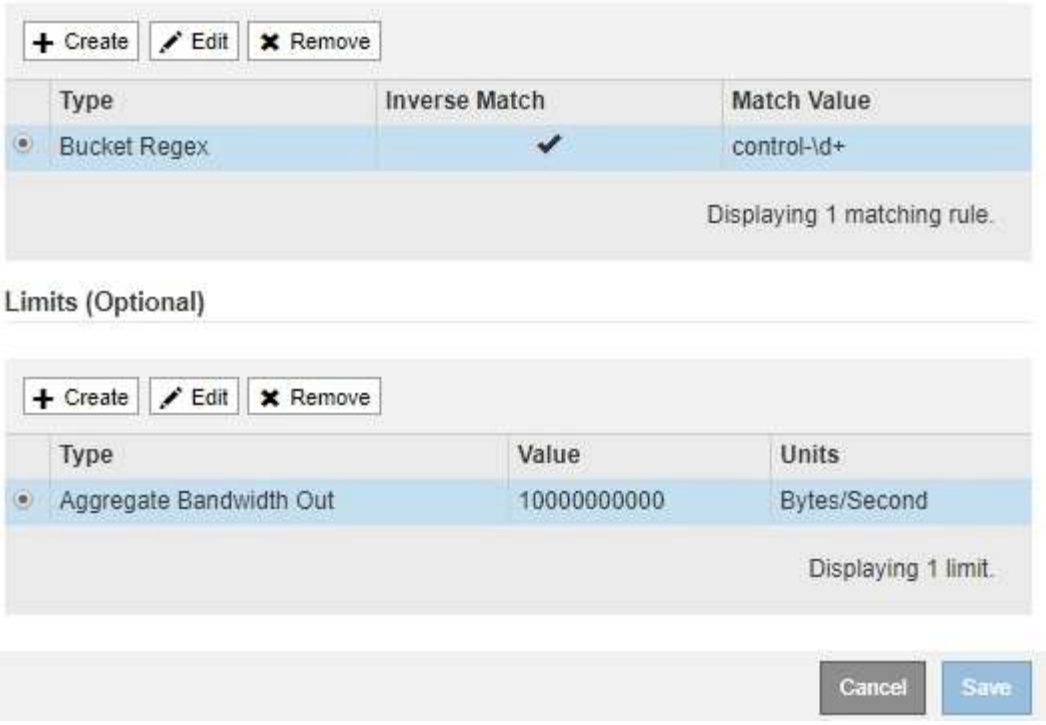
- Endereço IP exato (/máscara 32)
- Nome exato do balde
- Regex do balde
- Locatário
- Endpoint
- Correspondências CIDR não exatas (não /32)
- Correspondências inversas

c. No campo **value**, insira um valor numérico para o tipo de limite escolhido.

   As unidades esperadas são mostradas quando você seleciona um limite.

d. Clique em **aplicar**.

   O limite é criado e é listado na tabela limites.



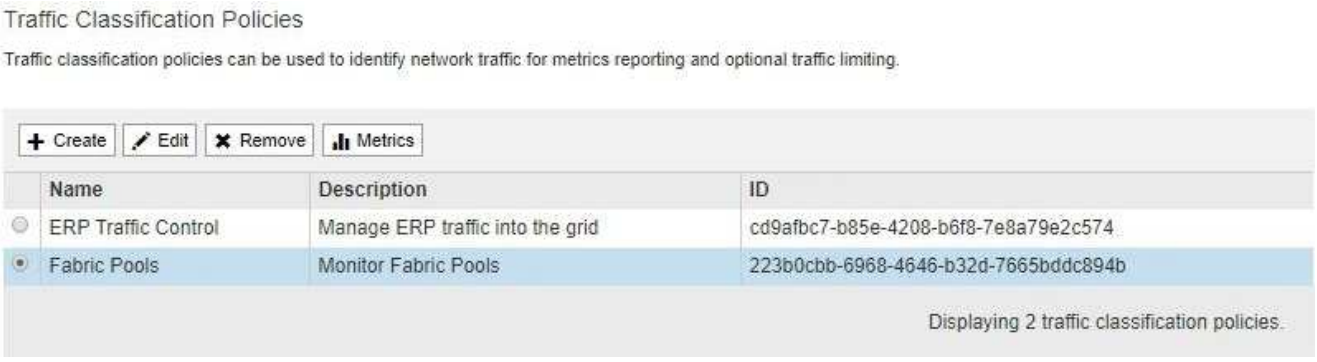
e. Repita estas etapas para cada limite que você deseja adicionar à política.

   Por exemplo, se você quiser criar um limite de largura de banda de 40 Gbps para um nível SLA, crie uma largura de banda agregada no limite e um limite de largura de banda agregada para fora e defina cada um para 40 Gbps.

   Para converter megabytes por segundo em gigabits por segundo, multiplique por oito. Por exemplo, 125 MB/s é equivalente a 1.000 Mbps ou 1 Gbps.

7. Quando terminar de criar regras e limites, clique em **Salvar**.

   A política é guardada e está listada na tabela políticas de classificação de tráfego.



   O tráfego de clientes S3 e Swift agora é 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.

Informações relacionadas

"Gerenciamento do balanceamento de carga"

"Visualização de métricas de tráfego de rede"

Editar uma 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.

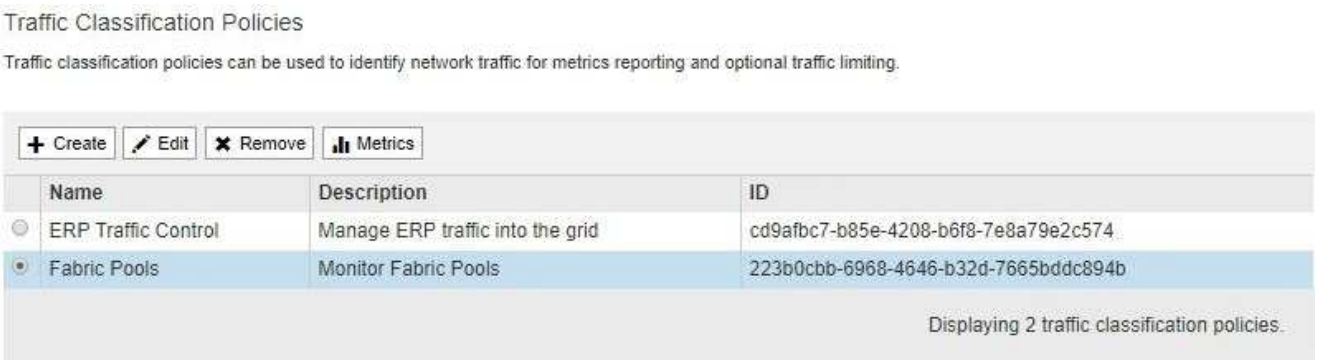
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Passos

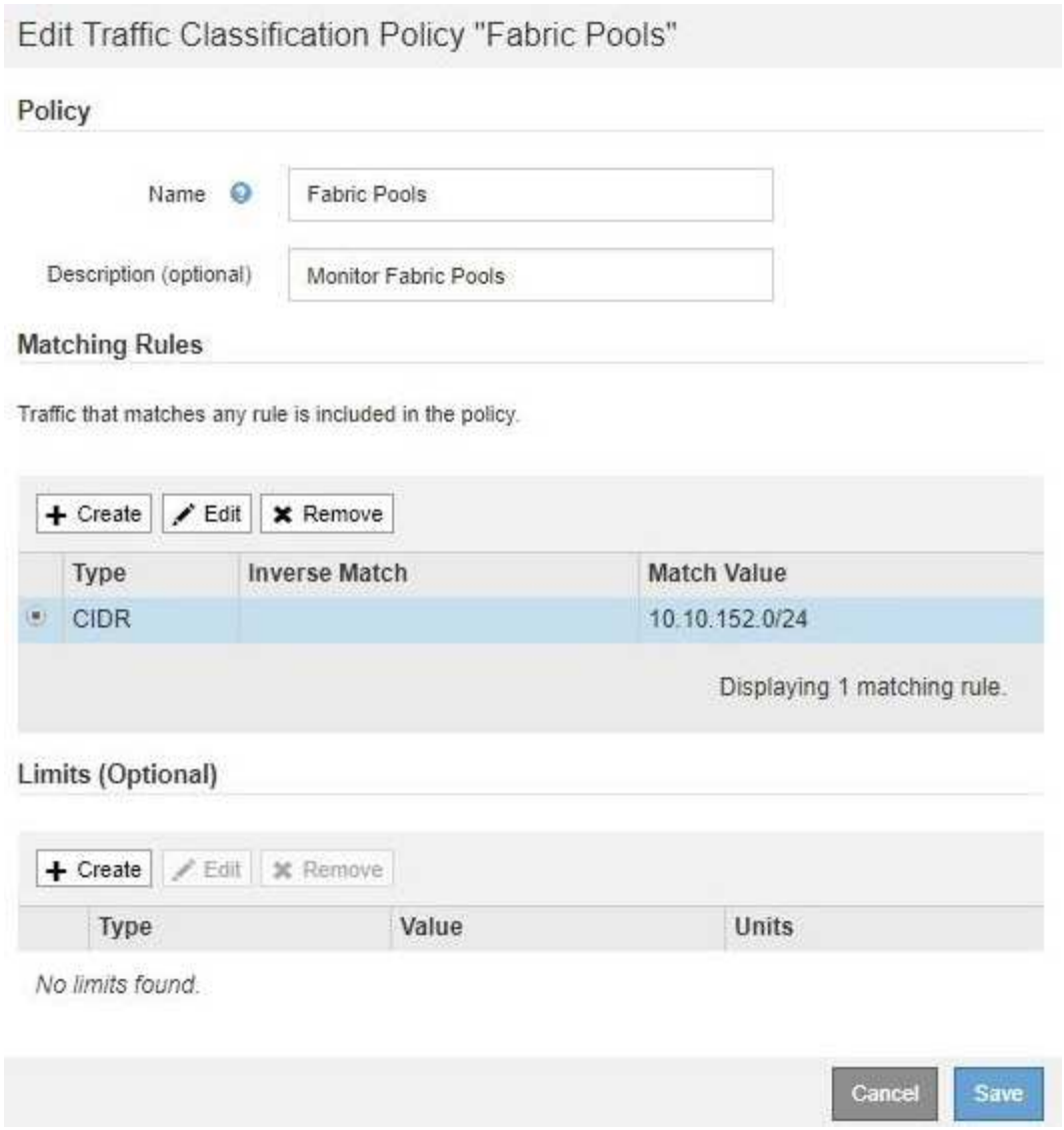
1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

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



2. Selecione o botão de opção à esquerda da política que pretende editar.
3. Clique em **Editar**.

   A caixa de diálogo Editar diretiva de classificação de tráfego é exibida.



4. Crie, edite ou remova regras e limites correspondentes conforme necessário.
   a. Para criar uma regra ou limite correspondente, clique em **criar** e siga as instruções para criar uma regra ou criar um limite.
   b. Para editar uma regra ou limite correspondente, selecione o botão de opção para a regra ou limite, clique em **Editar** na seção **regras correspondentes** ou na seção **limites** e siga as instruções para criar uma regra ou criar um limite.
   c. Para remover uma regra ou limite correspondente, selecione o botão de opção para a regra ou limite e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover a regra ou limite.
5. Quando terminar de criar ou editar uma regra ou um limite, clique em **aplicar**.
6. Quando terminar de editar a política, clique em **Salvar**.

   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

Se você não precisar mais de uma política de classificação de tráfego, você pode excluí-

la.

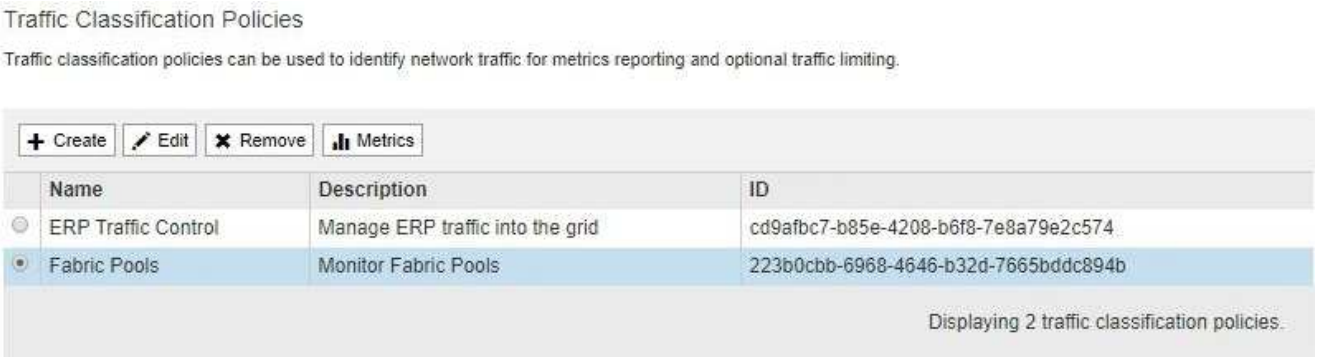
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

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



2. Selecione o botão de opção à esquerda da política que pretende eliminar.
3. Clique em **Remover**.

   É apresentada uma caixa de diálogo Aviso.

4. Clique em **OK** para confirmar que deseja excluir a política.

   A política é eliminada.

Visualização de métricas de tráfego de rede

Pode monitorizar o tráfego de rede visualizando os gráficos disponíveis na página políticas de classificação de tráfego.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

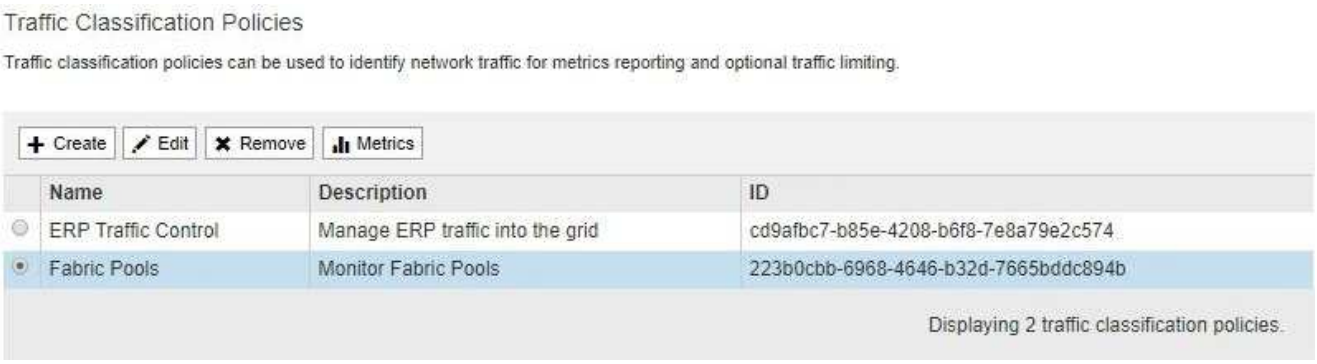
Para qualquer política de classificação de tráfego existente, você pode exibir métricas para o serviço Load Balancer para determinar se a diretiva está limitando com êxito o tráfego na rede. Os dados nos gráficos podem ajudá-lo a determinar se você precisa ajustar a política.

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 **Configuração** > **Configurações de rede** > **classificação de tráfego**.

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



2. Selecione o botão de opção à esquerda da política para a qual deseja exibir as métricas.
3. Clique em **Metrics**.

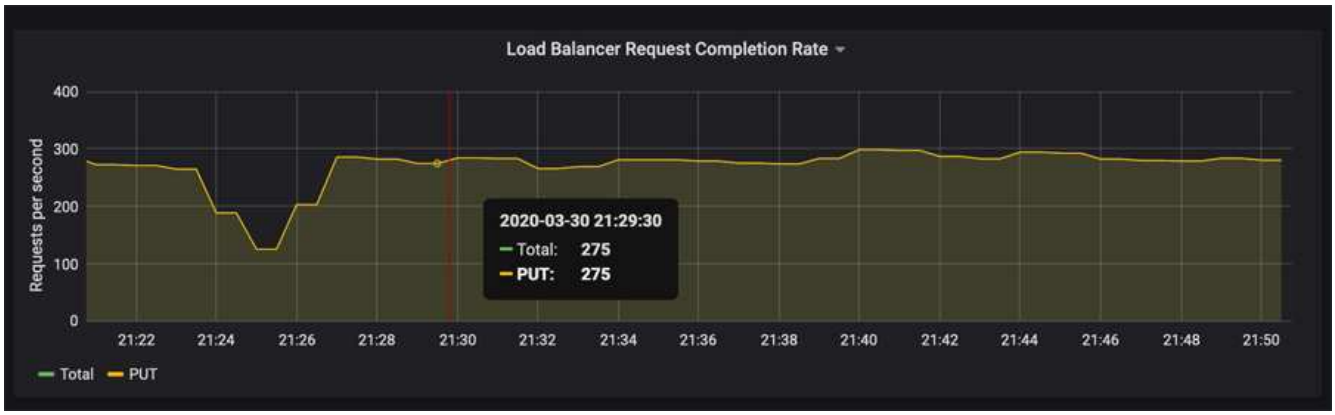
   Uma nova janela do navegador é aberta e os gráficos da Política de classificação de tráfego são exibidos. Os gráficos exibem métricas apenas para o tráfego que corresponde à política selecionada.

   Você pode selecionar outras políticas para exibir usando a lista suspensa **policy**.

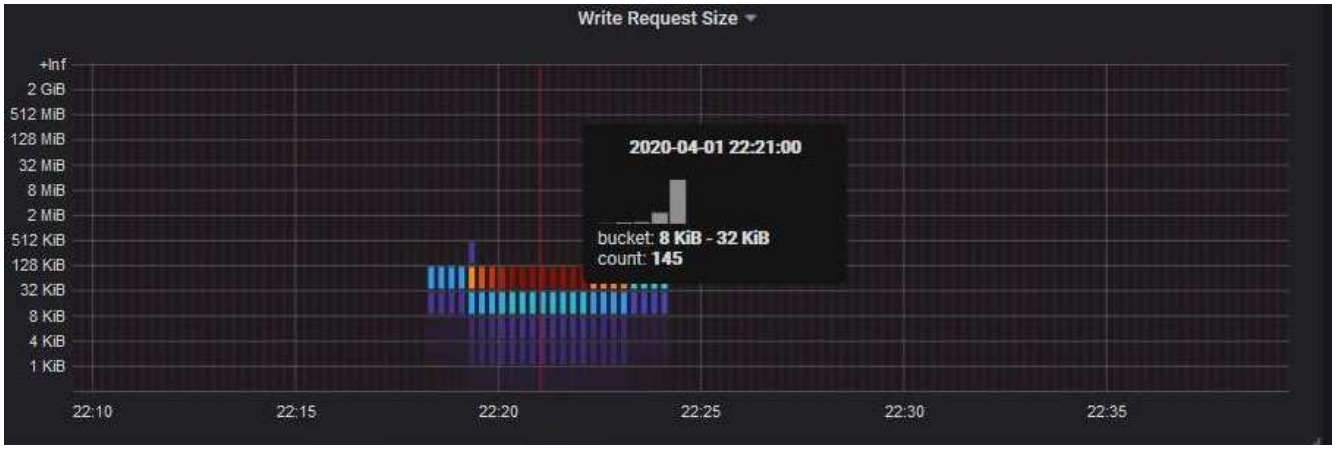
   Os gráficos a seguir estão incluídos na página da Web.

- Tráfego de solicitação do Load Balancer: 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.
- Taxa de conclusão da solicitação do Load Balancer: Este gráfico fornece uma média móvel de 3 minutos do número de solicitações concluídas 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.
- 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.
- Duração média da solicitação (não-erro): Este gráfico fornece uma média móvel de 3 minutos de duração da solicitação, 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 solicitação de gravação por tamanho do objeto: Este mapa de calor fornece uma média móvel de 3 minutos da taxa na qual as solicitações de gravação são concluídas com base no tamanho do objeto. Neste contexto, as solicitações de escrita referem-se apenas a SOLICITAÇÕES PUT.
- Taxa de solicitação de leitura por tamanho do objeto: Este mapa de calor fornece uma média móvel de 3 minutos da taxa na qual as solicitações de leitura são concluídas com base no tamanho do objeto. Neste contexto, as solicitações de leitura referem-se apenas a SOLICITAÇÕES GET. As cores no mapa de calor indicam a frequência relativa de um tamanho de objeto dentro de um gráfico individual. As cores mais frias (por exemplo, roxo e azul) indicam taxas relativas mais baixas, e as cores mais quentes (por exemplo, laranja e vermelho) indicam taxas relativas mais altas.

4. Passe o cursor sobre um gráfico de linhas para ver um pop-up de valores em uma parte específica do gráfico.



5. Passe o cursor sobre um mapa de calor 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.



6. Use a lista suspensa **Policy** (Política*) no canto superior esquerdo para selecionar uma política diferente.

   São apresentados os gráficos da política selecionada.

7. Em alternativa, aceda aos gráficos a partir do menu **Support**.
   a. Selecione **Support** > **Tools** > **Metrics**.
   b. Na seção **Grafana** da página, selecione **Política de classificação de tráfego**.
   c. Selecione a política na lista suspensa no canto superior esquerdo da página.

      As políticas de classificação de tráfego são identificadas pelo seu ID. Os IDs de política são listados na página políticas de classificação de tráfego.

8. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustar a política.

Informações relacionadas

"Monitorizar Resolução de problemas"

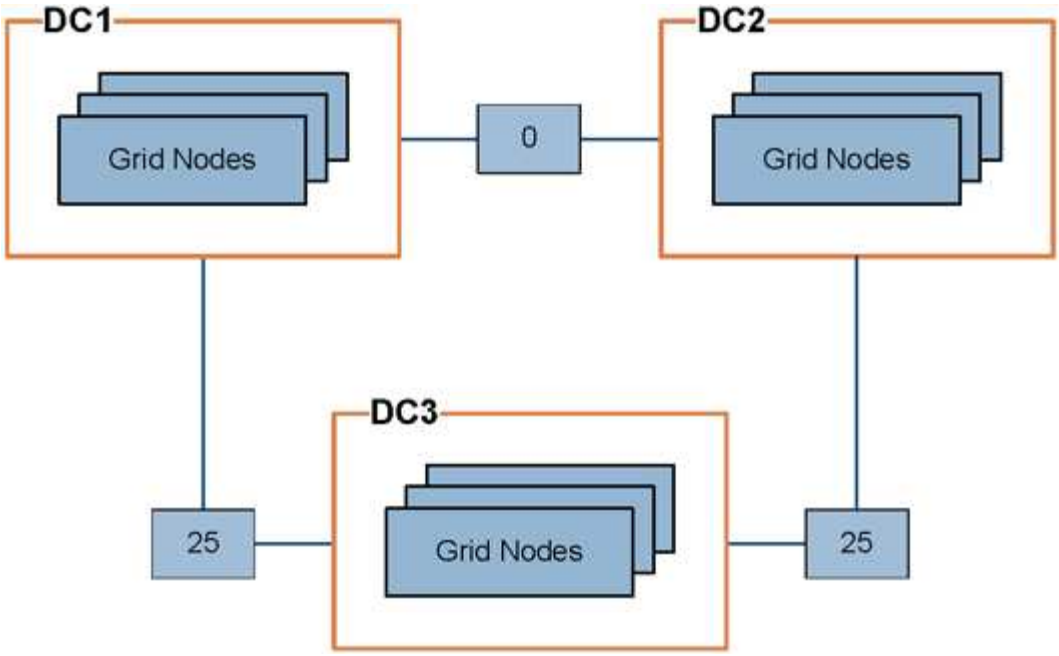
Quais são os custos da ligação

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.

- 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 CLB nos nós do Gateway para direcionar as conexões do cliente.

  O serviço CLB está obsoleto.

O diagrama mostra uma grade de três sites que tem custos de link configurados entre sites:



- O serviço CLB nos nós de Gateway distribui igualmente as conexões de cliente para todos os nós de armazenamento 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 D2 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.

Informações relacionadas

"Como funciona o balanceamento de carga - serviço CLB"

Atualizar custos de link

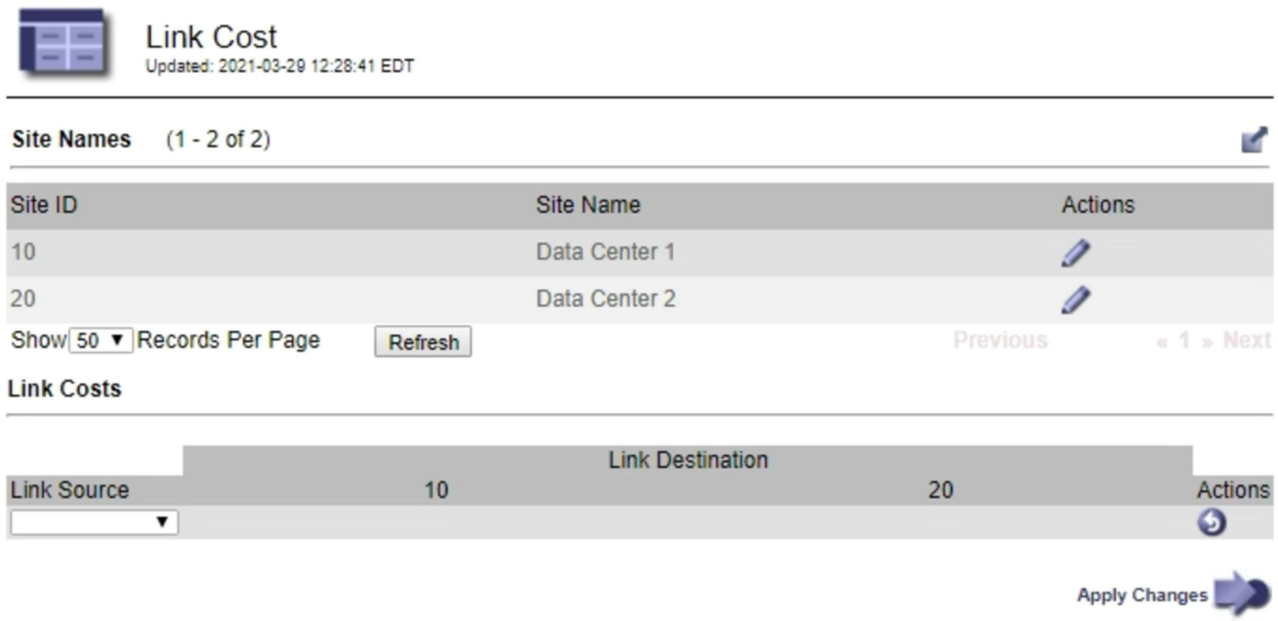
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Configuração da Página de topologia de Grade.

Passos

1. Selecione **Configuração** > **Definições de rede** > **custo de ligação**.



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 igual ao destino.

   Para cancelar as alterações, clique em **Revert**.

3. Clique em **aplicar alterações**.

Configurando o AutoSupport

O recurso AutoSupport permite que o sistema StorageGRID envie mensagens de status e integridade para o suporte técnico. 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 as mensagens do AutoSupport para serem enviadas para um destino adicional.

Informações incluídas nas mensagens do AutoSupport

As mensagens do AutoSupport incluem informações como as seguintes:

- Versão do software StorageGRID
- Versão do sistema operativo
- Informações sobre atributos no nível do sistema e no nível da localização
- Alertas e alarmes recentes (sistema legado)
- Status atual de todas as tarefas de grade, incluindo dados históricos
- Informações de eventos conforme listado na página **nós** > ***Grid Node*** > **Eventos**
- Utilização da base de dados do Admin Node
- Número de objetos perdidos ou perdidos
- Definições de configuração da grelha
- Entidades NMS
- Política ILM ativa
- Arquivo de especificação de grade provisionada
- Métricas de diagnóstico

Você pode ativar o recurso AutoSupport e as opções individuais do AutoSupport quando instalar o StorageGRID pela primeira vez, ou ativá-los posteriormente. Se o AutoSupport não estiver habilitado, uma mensagem será exibida no Painel de Gerenciamento de Grade. A mensagem inclui um link para a página de configuração do AutoSupport.

Você pode selecionar o símbolo "x" para fechar a mensagem. A mensagem não aparecerá novamente até que o cache do navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

Usando o Active IQ

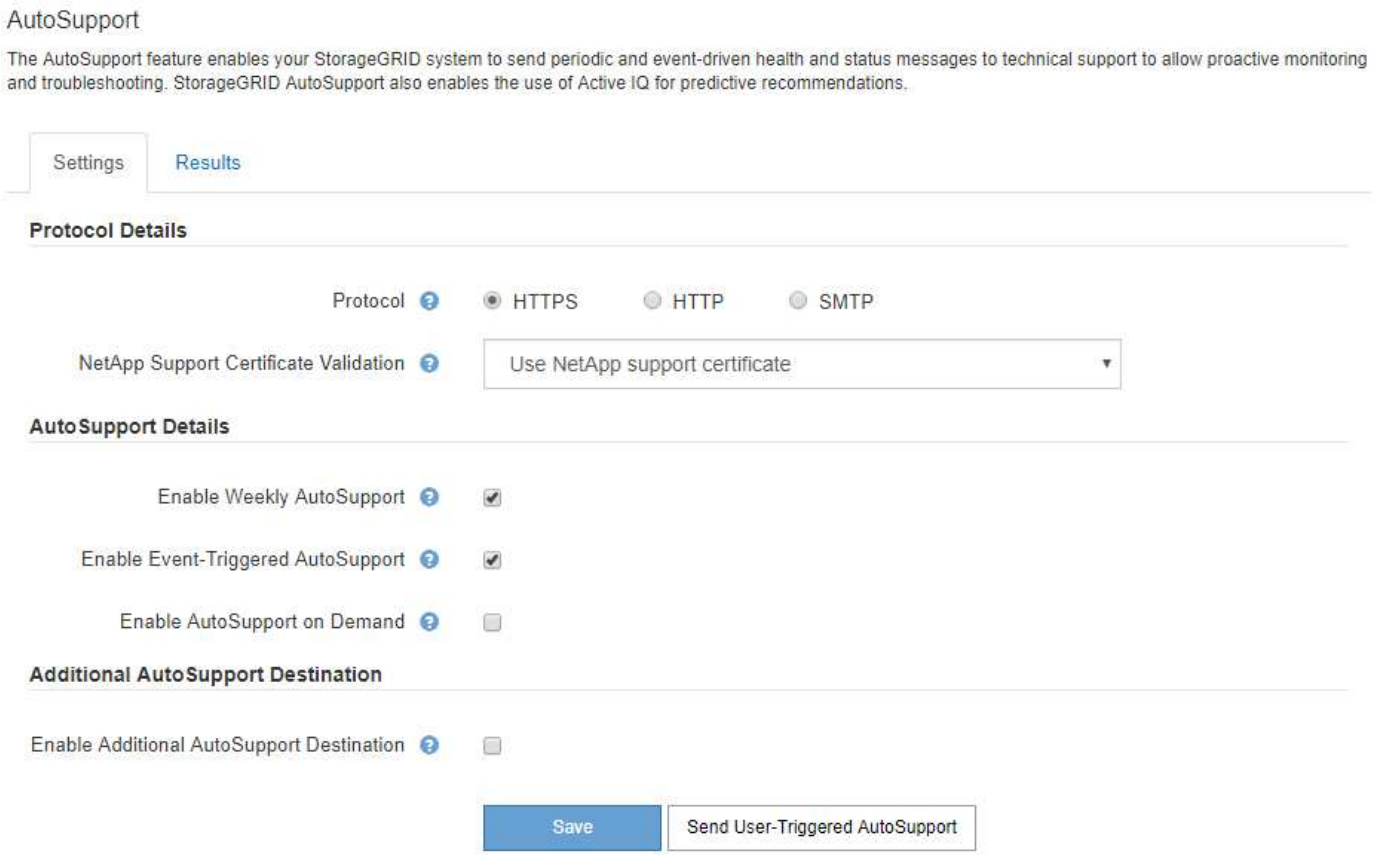
O Active IQ é um consultor digital baseado na nuvem que utiliza as análises preditivas e o conhecimento da comunidade da base instalada da NetApp. Suas avaliações de risco contínuas, alertas preditivos, orientações prescritivas e ações automatizadas ajudam a evitar problemas antes que eles ocorram, levando a uma melhor integridade do sistema e maior disponibilidade do sistema.

Você deve habilitar o AutoSupport se quiser usar os painéis e a funcionalidade do Active IQ no site de suporte da NetApp.

"Documentação do consultor digital da Active IQ"

Aceder às definições do AutoSupport

Você configura o AutoSupport usando o Gerenciador de Grade (**suporte** > **Ferramentas** > **AutoSupport**). A página **AutoSupport** tem duas guias: **Configurações** e **resultados**.



Protocolos para envio de mensagens AutoSupport

Você pode escolher um dos três protocolos para enviar mensagens AutoSupport:

- HTTPS
- HTTP
- SMTP

Se você enviar mensagens AutoSupport usando HTTPS ou HTTP, poderá configurar um servidor proxy não transparente entre nós de administração e suporte técnico.

Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de configurar um servidor de correio SMTP.

Opções de AutoSupport

Você pode usar qualquer combinação das seguintes opções para enviar mensagens do AutoSupport para o suporte técnico:

- **Semanal**: Enviar automaticamente mensagens AutoSupport uma vez por semana. Predefinição: Activado.
- **Event-dispolled**: Envie automaticamente mensagens AutoSupport 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 mensagens AutoSupport automaticamente, o que é útil quando eles estão trabalhando ativamente em um problema (requer protocolo de transmissão HTTPS AutoSupport). Predefinição: Desativada.
- **Ativado pelo usuário**: Envie mensagens AutoSupport manualmente a qualquer momento.

Informações relacionadas

"Suporte à NetApp"

Especificando o protocolo para mensagens AutoSupport

Você pode usar um dos três protocolos para enviar mensagens AutoSupport.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.
- Se você usar o protocolo HTTPS ou HTTP para enviar mensagens AutoSupport, você deve ter fornecido acesso de saída à Internet para o nó de administração principal, diretamente ou usando um servidor proxy (conexões de entrada não necessárias).
- Se utilizar o protocolo HTTPS ou HTTP e pretender utilizar um servidor proxy, tem de ter configurado um servidor proxy Admin.
- Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de ter configurado um servidor de correio SMTP. A mesma configuração do servidor de e-mail é usada para notificações de e-mail de alarme (sistema legado).

Sobre esta tarefa

As mensagens AutoSupport podem ser enviadas usando qualquer um dos seguintes protocolos:

- **HTTPS**: Esta é a configuração padrão e recomendada para novas instalações. O protocolo HTTPS utiliza a porta 443. Se pretender ativar a funcionalidade AutoSupport On Demand, tem de utilizar o protocolo HTTPS.
- **HTTP**: Este protocolo não é seguro, a menos que seja usado em um ambiente confiável onde o servidor proxy converte para HTTPS ao enviar dados pela Internet. O protocolo HTTP usa a porta 80.
- **SMTP**: Use esta opção se quiser que as mensagens do AutoSupport sejam enviadas por e-mail. Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de configurar um servidor de correio SMTP na página Configuração de e-mail legado (**suporte** > **Alarmes (legado)** > **Configuração de e-mail legado**).

> O SMTP era o único protocolo disponível para mensagens AutoSupport antes do lançamento do StorageGRID 11,2. Se você instalou uma versão anterior do StorageGRID inicialmente, o SMTP pode ser o protocolo selecionado.

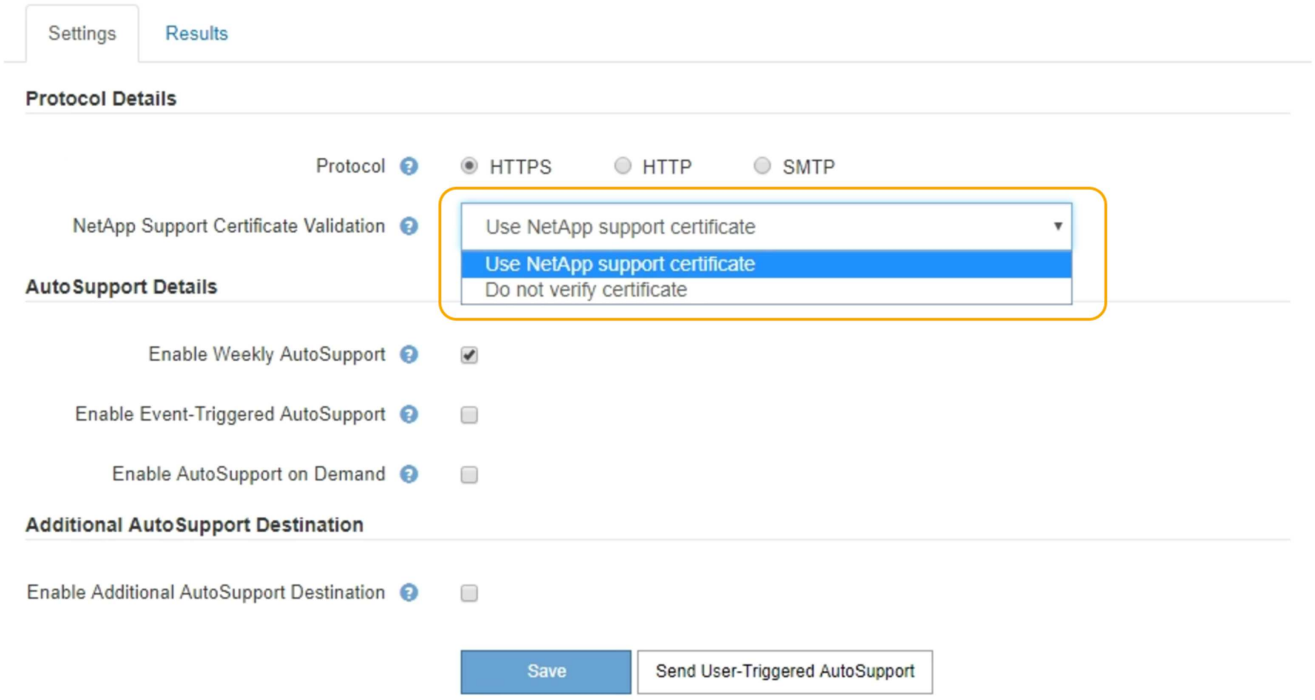
O protocolo definido é utilizado para enviar todos os tipos de mensagens AutoSupport.

Passos

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

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

2. Selecione o protocolo que pretende utilizar para enviar mensagens AutoSupport.



3. Selecione sua escolha para **Validação de certificado de suporte NetApp**.
   - Use o certificado de suporte NetApp (padrão): A validação do certificado garante que a transmissão de mensagens AutoSupport seja segura. O certificado de suporte do NetApp já está instalado com o software StorageGRID.
   - Não verificar 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. Selecione **Guardar**.

   Todas as mensagens semanais, acionadas pelo utilizador e acionadas por eventos são enviadas utilizando o protocolo selecionado.

Informações relacionadas

"Configurando as configurações de proxy Admin"

Habilitando o AutoSupport sob demanda

O AutoSupport On Demand pode ajudar a resolver problemas nos quais o suporte técnico está trabalhando ativamente. Quando você ativa o AutoSupport sob demanda, o suporte técnico pode solicitar que as mensagens do AutoSupport sejam enviadas sem a necessidade de sua intervenção.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.
- Você deve ter ativado mensagens AutoSupport semanais.
- Tem de ter definido o protocolo de transporte como HTTPS.

Sobre esta tarefa

Quando você ativa esse recurso, o suporte técnico pode solicitar que seu sistema StorageGRID envie mensagens do AutoSupport automaticamente. O suporte técnico também pode definir o intervalo de tempo de polling para consultas AutoSupport On Demand.

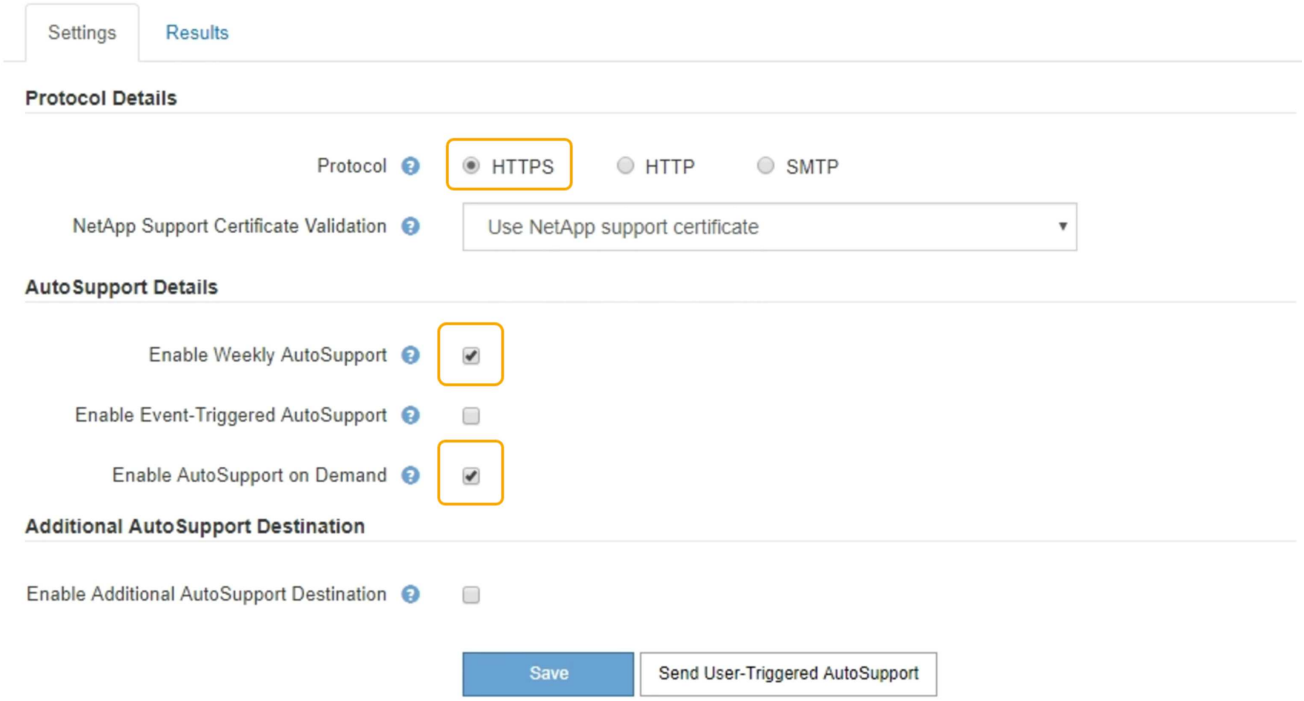
O suporte técnico não pode ativar ou desativar o AutoSupport a pedido.

Passos

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

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

2. Selecione o botão de opção HTTPS na secção **Protocol Details** (Detalhes do protocolo) da página.



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 mensagens AutoSupport semanais

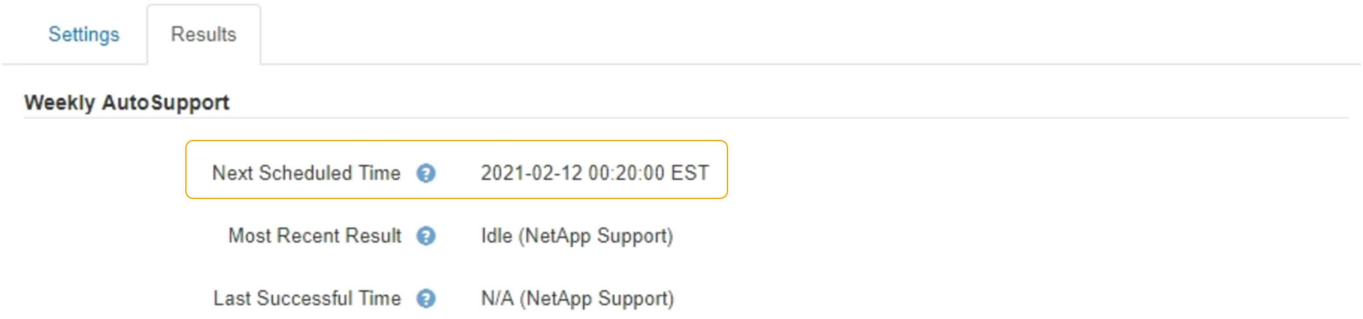
Por padrão, o sistema StorageGRID está configurado para enviar uma mensagem AutoSupport para o suporte da NetApp uma vez por semana.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

Sobre esta tarefa

Para determinar quando a mensagem AutoSupport semanal é enviada, consulte **hora programada seguinte** em **AutoSupport semanal** na página **AutoSupport** > **resultados**.



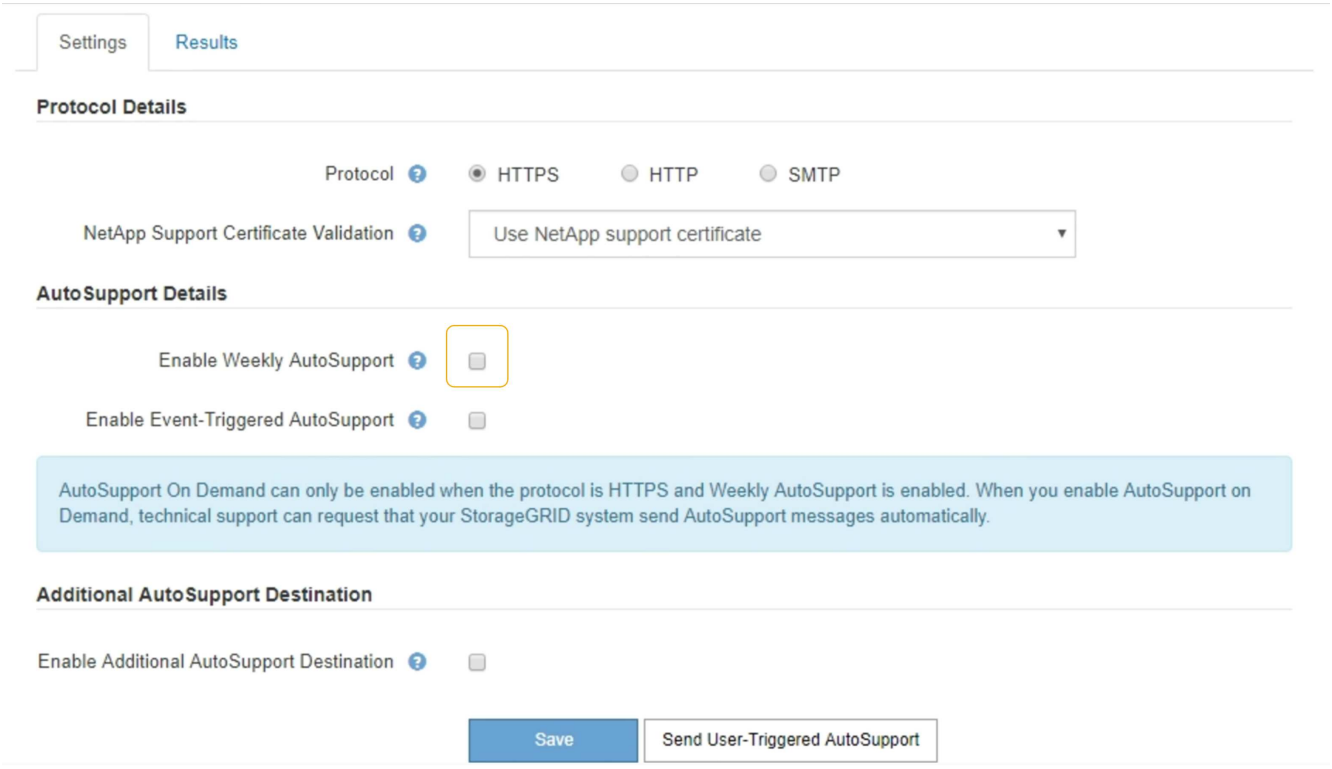
Pode desativar o envio automático de uma mensagem AutoSupport a qualquer momento.

Passos

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

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

2. Desmarque a caixa de seleção **Ativar AutoSupport semanal**.



3. Selecione **Guardar**.

Desativando mensagens AutoSupport acionadas por eventos

Por padrão, o sistema StorageGRID é configurado para enviar uma mensagem AutoSupport para o suporte da NetApp quando ocorre um alerta importante ou outro evento significativo do sistema.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

Sobre esta tarefa

Você pode desativar as mensagens AutoSupport acionadas por eventos a qualquer momento.

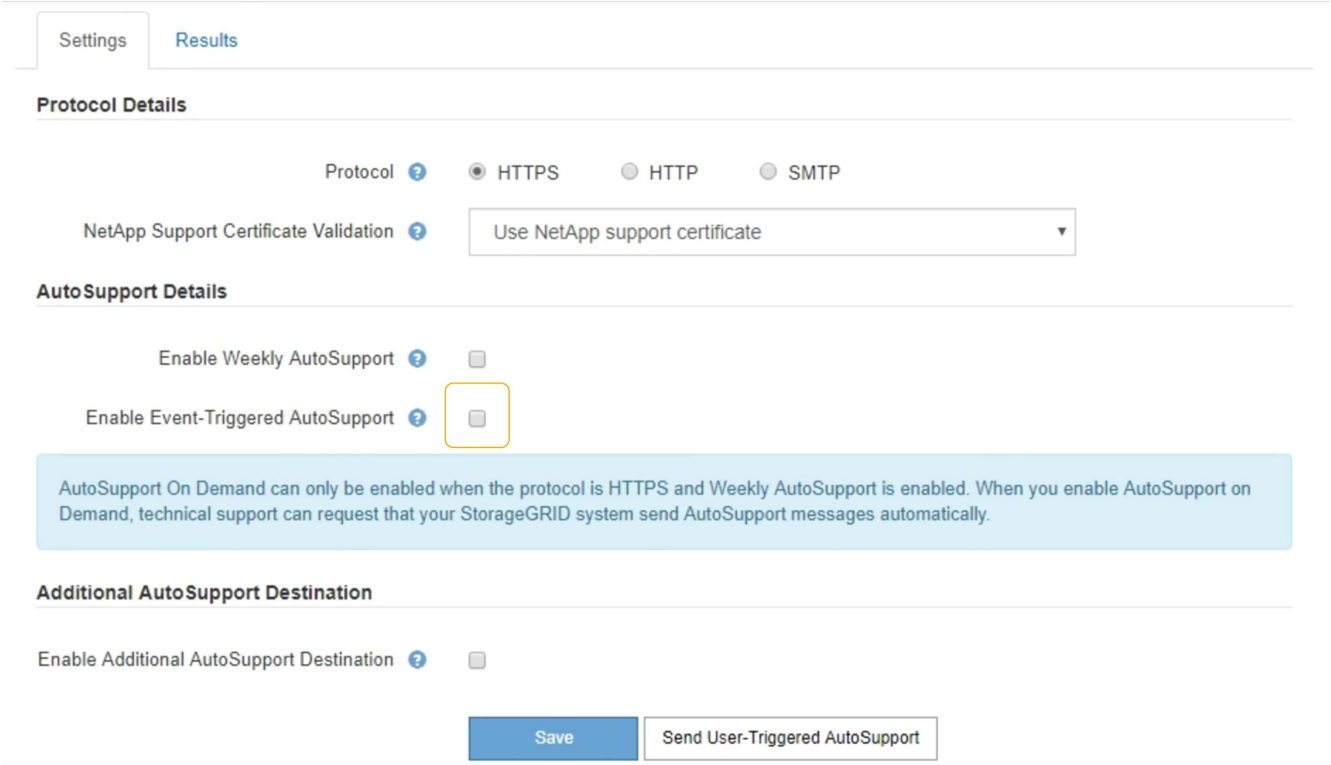
> As mensagens AutoSupport acionadas por eventos também são suprimidas quando você suprime as notificações por e-mail em todo o sistema. (Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**. Em seguida, selecione **notificação suprimir tudo**.)

Passos

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

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

2. Desmarque a caixa de seleção **Enable Event-Triggered** (Ativar AutoSupport acionado por evento*).



3. Selecione **Guardar**.

Acionando manualmente uma mensagem AutoSupport

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

Passos

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

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

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

   O StorageGRID tenta enviar uma mensagem do AutoSupport para o suporte técnico. Se a tentativa for bem-sucedida, os valores **resultado mais recente** e **último tempo bem-sucedido** na guia **resultados** serão atualizados. Se houver um problema, o valor **resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar a mensagem AutoSupport novamente.

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

Adicionar um destino AutoSupport adicional

Quando você ativa o AutoSupport, as mensagens de estado e de saúde são enviadas para o suporte do NetApp. Você pode especificar um destino adicional para todas as mensagens do AutoSupport.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

Sobre esta tarefa

Para verificar ou alterar o protocolo usado para enviar mensagens AutoSupport, consulte as instruções para especificar um protocolo AutoSupport.

> Não é possível usar o protocolo SMTP para enviar mensagens AutoSupport para um destino adicional.

"Especificando o protocolo para mensagens AutoSupport"

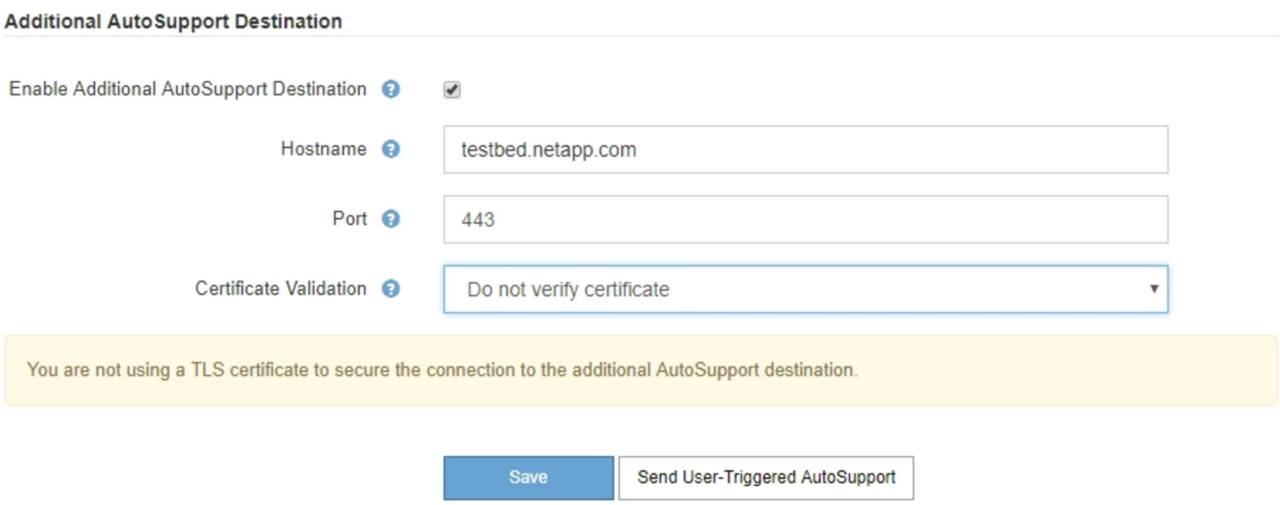
Passos

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

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

2. Selecione **Ativar destino AutoSupport adicional**.

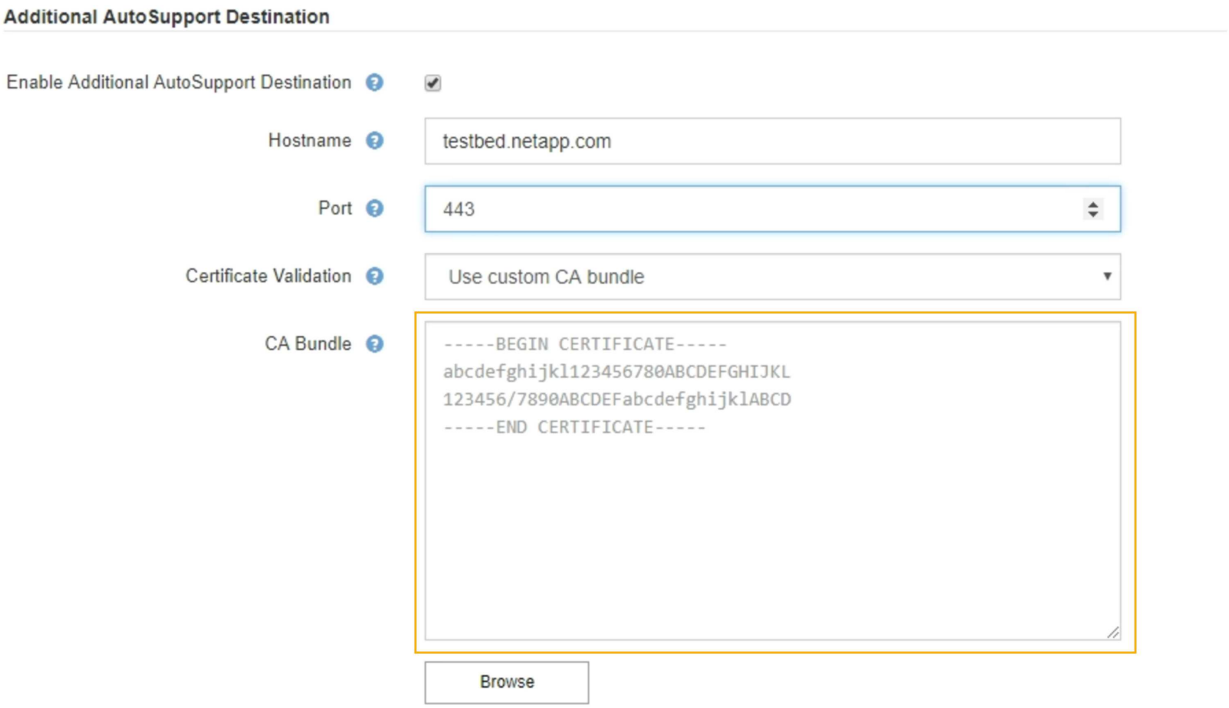
   São apresentados os campos de destino AutoSupport adicional.



3. Introduza o nome de anfitrião do servidor ou o endereço IP de um servidor de destino AutoSupport adicional.

   Pode introduzir apenas um destino adicional.

4. Introduza a porta utilizada para ligar a um servidor de destino AutoSupport adicional (a predefinição é a porta 80 para HTTP ou a porta 443 para HTTPS).
5. Para enviar suas mensagens do AutoSupport com validação de certificado, selecione **Use custom CA bundle** no menu suspenso **Validação de certificado**. Em seguida, execute um dos seguintes procedimentos:
   - Use uma ferramenta de edição para copiar e colar todo o conteúdo de cada um dos arquivos de certificado CA codificados em PEM no campo **CA bundle**, concatenado em ordem de cadeia de certificados. Você deve incluir `----BEGIN CERTIFICATE----` e `----END CERTIFICATE----` em sua seleção.



◦ Selecione **Procurar**, navegue até o arquivo que contém os certificados e selecione **abrir** para carregar o arquivo. A validação do certificado garante que a transmissão de mensagens AutoSupport é segura.

6. Para enviar suas mensagens do AutoSupport sem validação de certificado, selecione **não verificar certificado** na lista suspensa **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.

   Uma mensagem de aviso é exibida: "Você não está usando um certificado TLS para proteger a conexão com o destino AutoSupport adicional."

7. Selecione **Guardar**.

   Todas as futuras mensagens AutoSupport semanais, acionadas por eventos e acionadas pelo usuário serão enviadas para o destino adicional.

Envio de mensagens do e-Series AutoSupport através do StorageGRID

Você pode enviar mensagens do e-Series SANtricity System Manager AutoSupport para o suporte técnico por meio de um nó de administração do StorageGRID, em vez da porta de gerenciamento do dispositivo de storage.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um navegador da Web compatível.
- Você tem a permissão Administrador do dispositivo de armazenamento ou a permissão de acesso root.

> 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

As mensagens AutoSupport do e-Series contêm detalhes do hardware de armazenamento e são mais específicas do que outras mensagens AutoSupport enviadas pelo sistema StorageGRID.

Configure um endereço de servidor proxy especial no Gerenciador de sistema do SANtricity para fazer com que as mensagens do AutoSupport sejam transmitidas através de um nó de administração do StorageGRID sem o uso da porta de gerenciamento do dispositivo. As mensagens AutoSupport transmitidas desta forma respeitam as definições de proxy do Remetente e administrador preferenciais que podem ter sido configuradas no Gestor de grelha.

Se você quiser configurar o servidor proxy Admin no Gerenciador de Grade, consulte as instruções para configurar as configurações do proxy Admin.

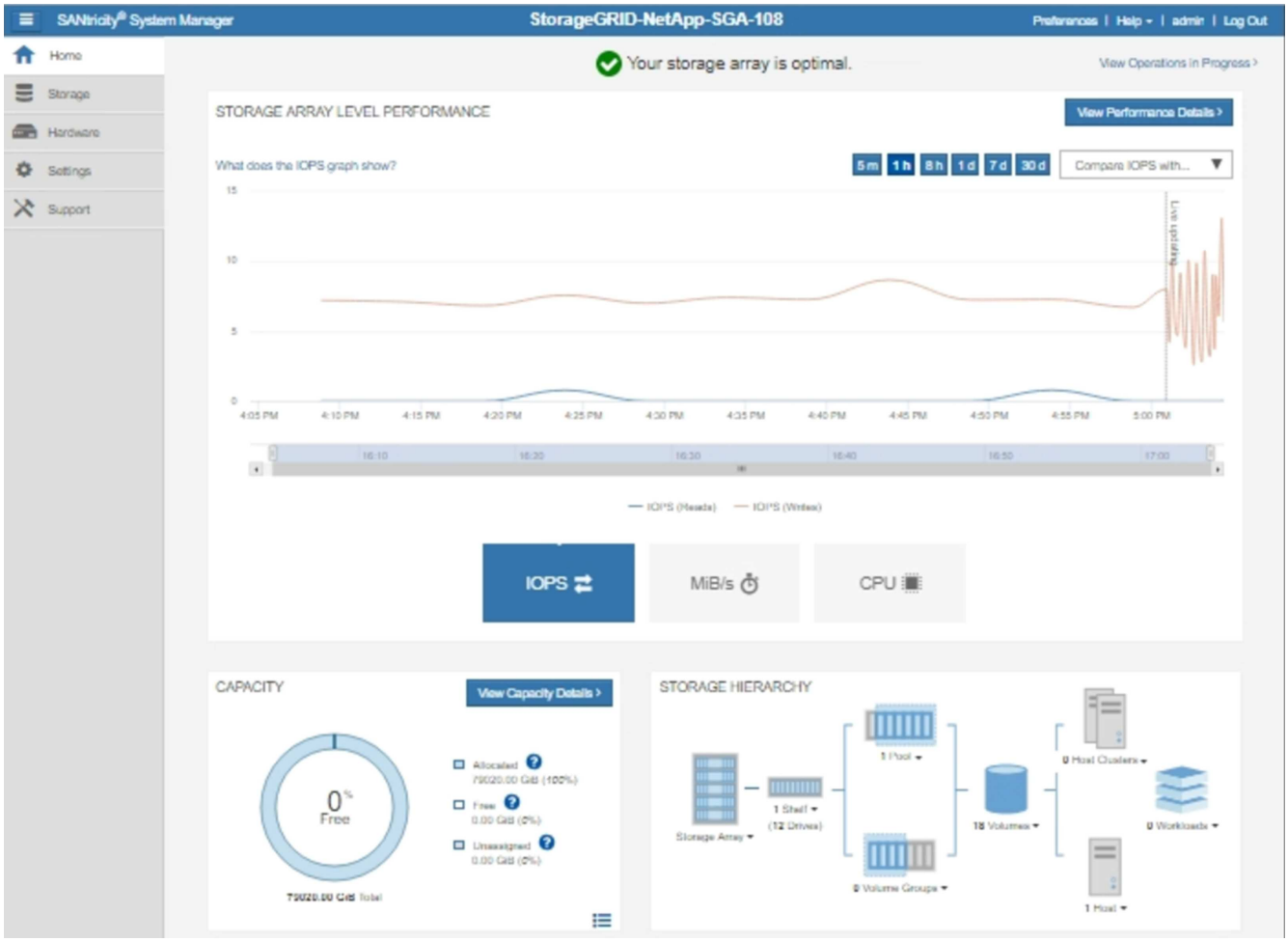
"Configurando as configurações de proxy Admin"

> Este procedimento destina-se apenas à configuração de um servidor proxy StorageGRID para mensagens AutoSupport e-Series. Para obter detalhes adicionais sobre as informações de configuração do e-Series AutoSupport, consulte o centro de documentação do e-Series.
>
> "Centro de Documentação de sistemas NetApp e-Series"

Passos

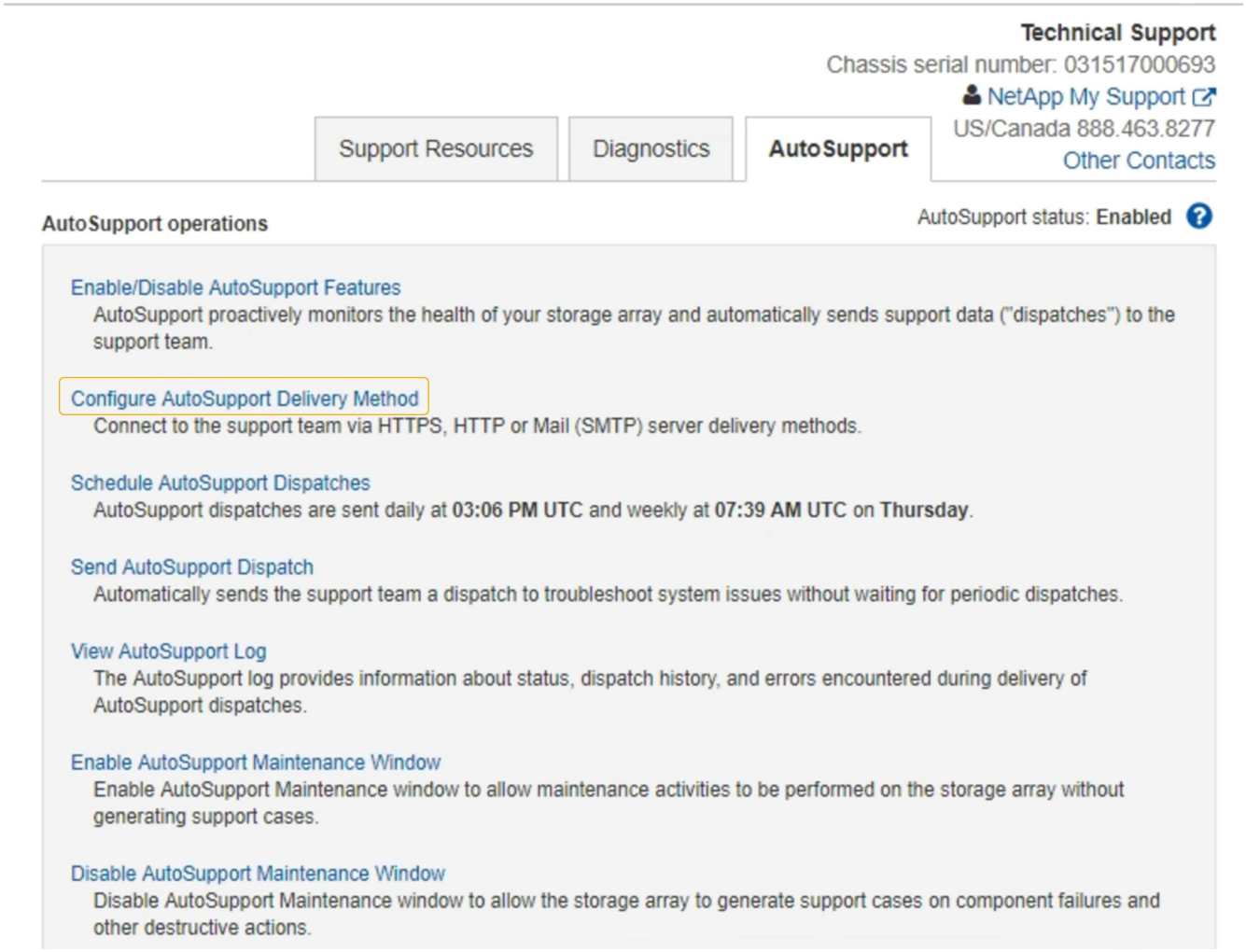
1. No Gerenciador de Grade, selecione **nós**.
2. Na lista de nós à esquerda, selecione o nó do dispositivo de storage que deseja configurar.
3. Selecione **Gerenciador do sistema SANtricity**.

   É apresentada a página inicial do Gestor do sistema SANtricity.



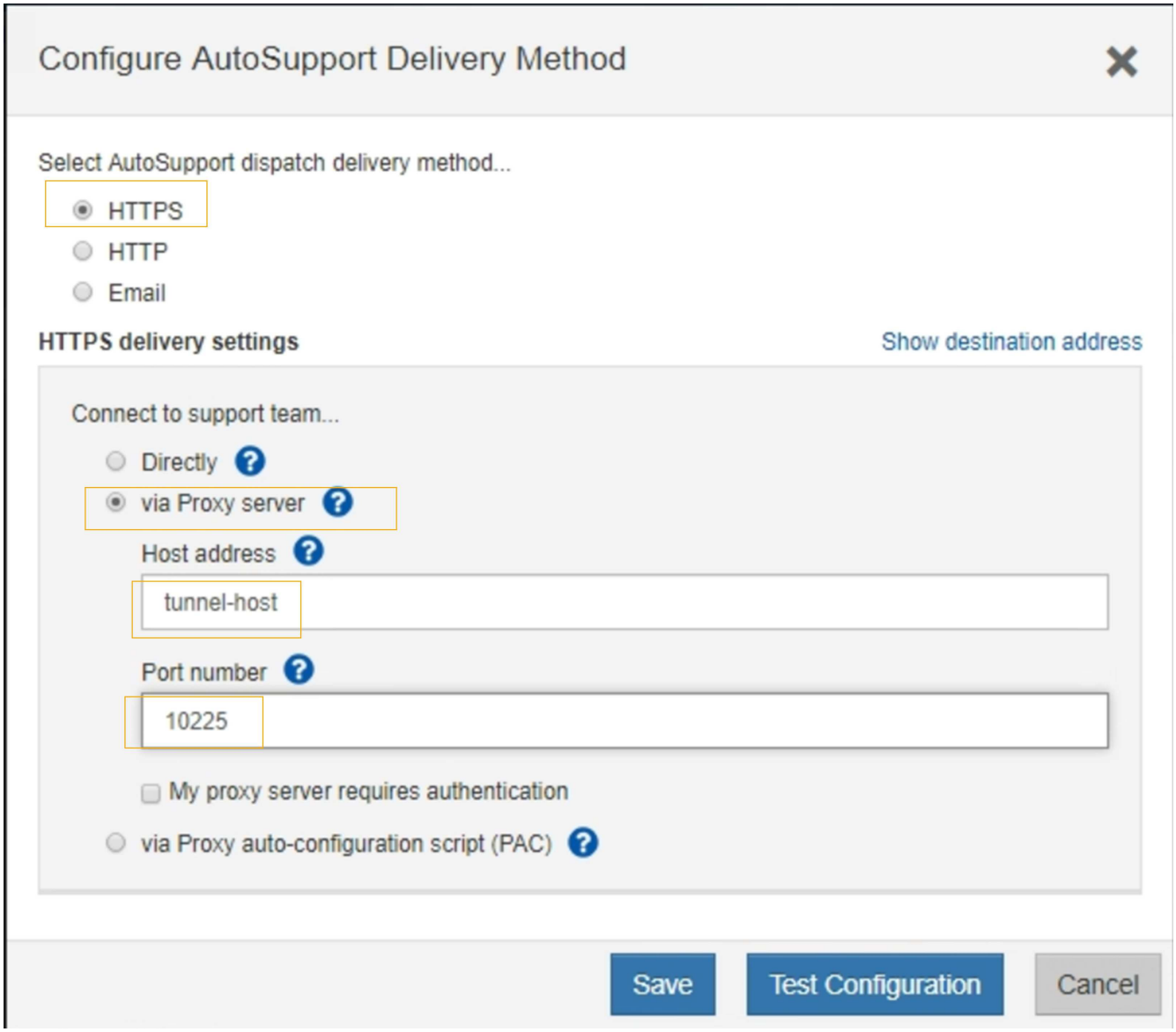
4. Selecione **suporte** > **Centro de suporte** > **AutoSupport**.

   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 protocolo 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 mensagens AutoSupport da série e.

9. Introduza `10225` o **número da porta**.

   `10225` É o número da porta no servidor proxy StorageGRID que recebe mensagens 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 de administrador do remetente preferido pode se conetar ao site de suporte do NetApp e tente o teste novamente.

11. Selecione **Guardar**.

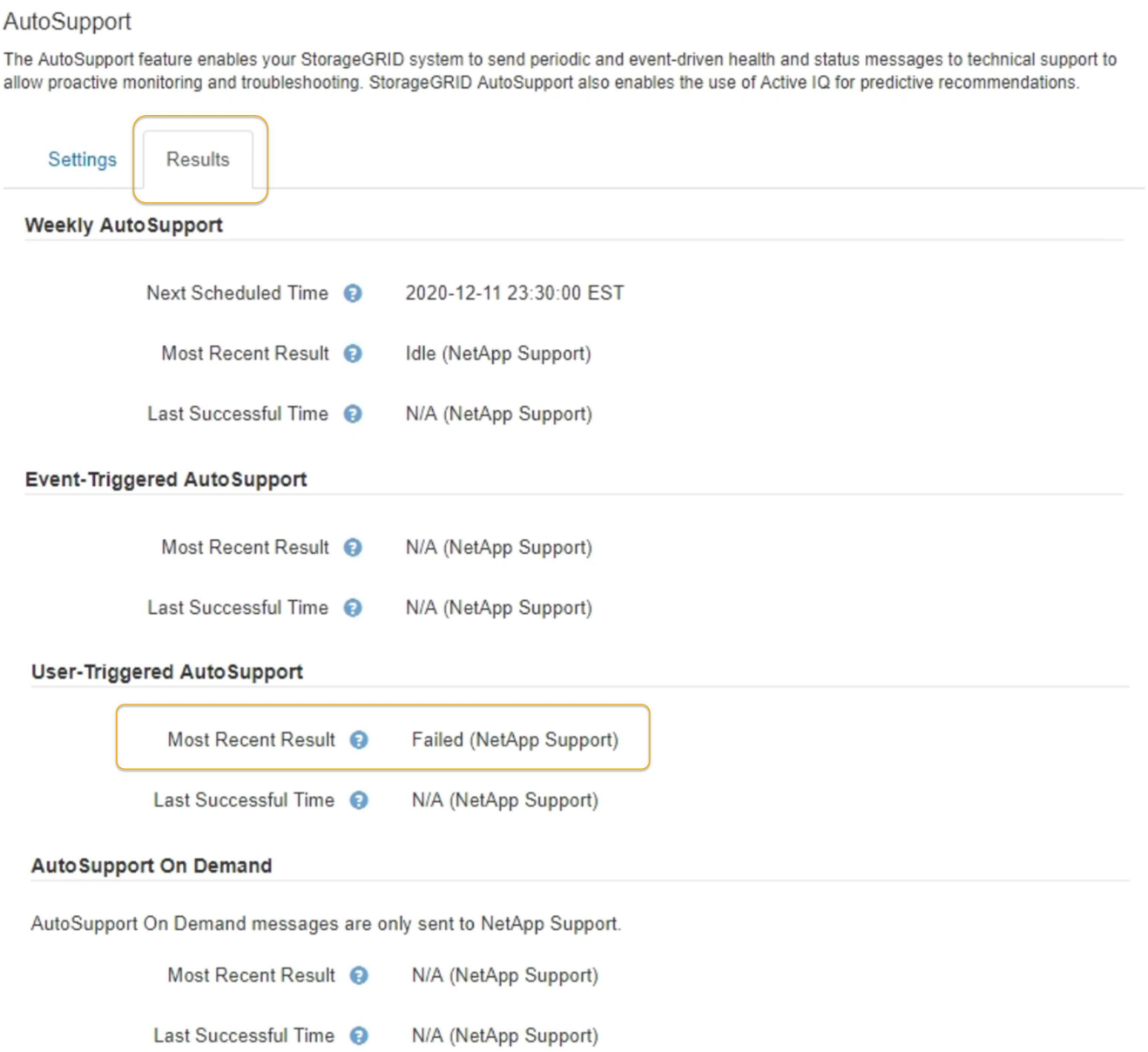
    A configuração é salva e uma mensagem de confirmação aparece: ""o método de entrega AutoSupport foi configurado."

Solução de problemas de mensagens do AutoSupport

Se uma tentativa de enviar uma mensagem AutoSupport falhar, o sistema StorageGRID executa ações diferentes dependendo do tipo de mensagem AutoSupport. Você pode verificar o status das mensagens do AutoSupport selecionando **suporte** > **Ferramentas** > **AutoSupport** > **resultados**.

> As mensagens AutoSupport acionadas por evento são suprimidas quando você suprime as notificações de e-mail em todo o sistema. (Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**. Em seguida, selecione **notificação suprimir tudo**.)

Quando a mensagem AutoSupport não é enviada, "'Falha'" aparece na guia **resultados** da página **AutoSupport**.



Falha semanal da mensagem AutoSupport

Se uma mensagem AutoSupport semanal não for enviada, o sistema StorageGRID executa as seguintes ações:

1. Atualiza o atributo de resultado mais recente para tentar novamente.
2. Tenta reenviar a mensagem 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 uma mensagem AutoSupport novamente na próxima hora programada.
5. Mantém a programação regular do AutoSupport se a mensagem falhar porque o serviço NMS não está disponível e se uma mensagem for enviada antes de sete dias passar.
6. Quando o serviço NMS estiver disponível novamente, envia uma mensagem AutoSupport imediatamente se uma mensagem não tiver sido enviada por sete dias ou mais.

Falha de mensagem AutoSupport acionada pelo usuário ou por evento

Se uma mensagem AutoSupport acionada pelo usuário ou por um evento não for enviada, 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 messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Não tenta enviar a mensagem 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 (**suporte** > **Alarmes (legado)** > **> Configuração de e-mail legado**). A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Saiba como configurar as definições do servidor de correio eletrónico no "monitorar solucionar problemas de instruções".

Correção de uma falha de mensagem 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 messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Informações relacionadas

"Monitorizar Resolução de problemas"

Gerenciando nós de storage

Os nós de storage fornecem capacidade e serviços de storage em disco. O gerenciamento de nós de storage envolve o monitoramento da quantidade de espaço utilizável em cada nó, usando configurações de marca d'água e aplicando configurações de nó de storage.

- "O que é um nó de storage"
- "Gerenciando Opções de armazenamento"
- "Gerenciamento do storage de metadados de objetos"
- "Configuração de configurações globais para objetos armazenados"
- "Configurações do nó de storage"
- "Gerenciamento de nós de storage completos"

O que é um nó de storage

Os nós de storage gerenciam e armazenam dados e metadados de objetos. Cada sistema StorageGRID precisa ter pelo menos três nós de storage. Se você tiver vários

locais, cada local no sistema StorageGRID também precisará ter três nós de storage.

Um nó de armazenamento inclui os serviços e processos necessários para armazenar, mover, verificar e recuperar dados de objetos e metadados no disco. Você pode exibir informações detalhadas sobre os nós de storage na página **nós**.

O que é o serviço ADC

O serviço controlador de domínio administrativo (ADC) autentica os nós de grade e suas conexões entre si. O serviço ADC é hospedado em cada um dos três primeiros 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.você pode visualizar informações ADC para um nó de armazenamento na página de topologia de grade (**suporte** > **topologia de grade**).

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.

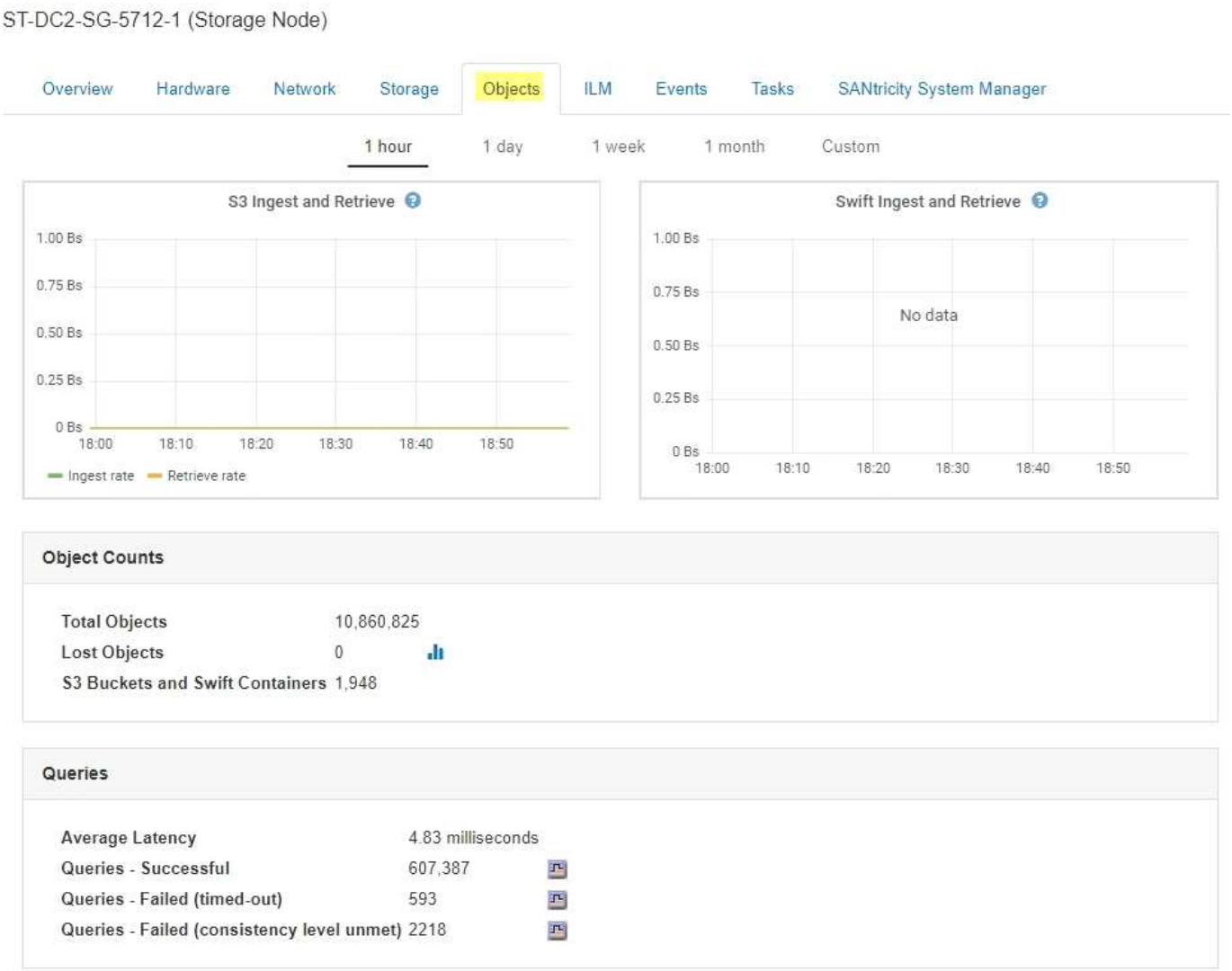
O que é o serviço DDS

Hospedado por um nó de armazenamento, o serviço armazenamento de dados distribuído (DDS) faz interface com o banco de dados Cassandra para executar tarefas em segundo plano nos metadados de objetos armazenados no sistema StorageGRID.

Contagens de objetos

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 ou Swift).

Você pode ver a contagem total de objetos na página nós > guia objetos para qualquer nó de storage.



Consultas

Você pode identificar o tempo médio que leva para executar uma consulta contra o armazenamento de metadados através do serviço DDS específico, o número total de consultas bem-sucedidas e o número total de consultas que falharam devido a um problema de tempo limite.

Você pode querer revisar as informações de consulta para monitorar a integridade do armazenamento de metadados, Cassandra, que afeta o desempenho de ingestão e recuperação do sistema. Por exemplo, se a latência de uma consulta média for lenta e o número de consultas com falha devido a tempos limite for alto, o armazenamento de metadados pode estar encontrando uma carga maior ou executando outra operação.

Você também pode exibir o número total de consultas que falharam devido a falhas de consistência. Falhas no nível de consistência resultam de um número insuficiente de armazenamentos de metadados disponíveis no momento em que uma consulta é realizada através do serviço DDS específico.

Você pode usar a página Diagnósticos para obter informações adicionais sobre o estado atual da grade. "A executar o diagnóstico"Consulte .

Garantias de consistência e controles

O StorageGRID garante consistência de leitura após gravação para objetos recém-criados. Qualquer operação GET após uma operação PUT concluída com êxito poderá ler os dados recém-gravados. As

substituições de objetos existentes, atualizações de metadados e exclusões permanecem, eventualmente, consistentes.

O que é o serviço LDR

Hospedado por cada nó de armazenamento, o serviço de roteador de distribuição local (LDR) lida com o transporte de conteúdo para o sistema StorageGRID. O transporte de conteúdo abrange muitas tarefas, incluindo armazenamento de dados, roteamento e manuseio de solicitações. O serviço LDR faz a maior parte do trabalho árduo 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 dados de objetos
- Transferências de dados de objeto de outro serviço LDR (Storage Node)
- Gerenciamento de storage de dados
- Interfaces de protocolo (S3 e Swift)

O serviço LDR também gerencia o mapeamento de objetos S3 e Swift para os "manipuladores de conteúdo" exclusivos que o sistema StorageGRID atribui a cada objeto ingerido.

Consultas

As consultas LDR incluem consultas para localização de objetos durante operações de recuperação e arquivamento. Você pode identificar o tempo médio que leva para executar uma consulta, o número total de consultas bem-sucedidas e o número total de consultas que falharam devido a um problema de tempo limite.

Você pode revisar as informações de consulta para monitorar a integridade do armazenamento de metadados, o que afeta o desempenho de ingestão e recuperação do sistema. Por exemplo, se a latência de uma consulta média for lenta e o número de consultas com falha devido a tempos limite for alto, o armazenamento de metadados pode estar encontrando uma carga maior ou executando outra operação.

Você também pode exibir o número total de consultas que falharam devido a falhas de consistência. Falhas no nível de consistência resultam de um número insuficiente de armazenamentos de metadados disponíveis no momento em que uma consulta é executada através do serviço LDR específico.

Você pode usar a página Diagnósticos para obter informações adicionais sobre o estado atual da grade. "A executar o diagnóstico"Consulte .

Atividade ILM

As métricas de gerenciamento do ciclo de vida das informações (ILM) permitem monitorar a taxa na qual os objetos são avaliados para a implementação do ILM. Você pode exibir essas métricas no Dashboard ou na página nós > guia ILM para cada nó de storage.

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.

Você pode ver os armazenamentos de objetos para um nó de storage na página nós > guia armazenamento.

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	4.40 TB	1.35 TB	43.99 GB	0 bytes	1.00%	No Errors
0001	1.97 TB	1.57 TB	44.76 GB	351.14 GB	20.09%	No Errors
0002	1.97 TB	1.46 TB	43.29 GB	465.20 GB	25.81%	No Errors
0003	1.97 TB	1.70 TB	43.51 GB	223.98 GB	13.58%	No Errors
0004	1.97 TB	1.92 TB	44.03 GB	0 bytes	2.23%	No Errors
0005	1.97 TB	1.46 TB	43.67 GB	463.36 GB	25.73%	No Errors
0006	1.97 TB	1.92 TB	43.10 GB	1.61 GB	2.27%	No Errors
0007	1.97 TB	1.35 TB	46.05 GB	575.24 GB	31.53%	No Errors
0008	1.97 TB	1.81 TB	46.00 GB	112.84 GB	8.06%	No Errors
0009	1.97 TB	1.57 TB	43.91 GB	352.72 GB	20.13%	No Errors
000A	1.97 TB	1.70 TB	44.31 GB	226.81 GB	13.76%	No Errors
000B	1.97 TB	1.92 TB	43.17 GB	780.07 MB	2.23%	No Errors
000C	1.97 TB	1.58 TB	44.32 GB	339.56 GB	19.48%	No Errors
000D	1.97 TB	1.82 TB	44.47 GB	107.34 GB	7.70%	No Errors
000E	1.97 TB	1.68 TB	43.07 GB	241.70 GB	14.45%	No Errors
000F	2.03 TB	1.50 TB	44.57 GB	475.47 GB	25.67%	No Errors

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 cópias replicadas e fragmentos codificados por apagamento.

Para garantir até mesmo o uso de espaço para cópias replicadas, os dados de objeto de um determinado objeto são armazenados em um armazenamento de objetos com base no espaço de storage disponível. Quando um ou mais objetos armazenam preenchimento até a capacidade, os armazenamentos de objetos restantes continuam armazenando objetos até que não haja mais espaço no nó de armazenamento.

Proteção de metadados

Metadados de objeto são informações relacionadas ou uma descrição de um objeto; por exemplo, tempo de modificação de objeto ou local de armazenamento. O StorageGRID armazena metadados de objetos em um banco de dados Cassandra, que faz interface com o serviço LDR.

Para garantir redundância e, portanto, proteção contra perda, três cópias dos metadados de objetos são mantidas em cada local. As cópias são distribuídas uniformemente por todos os nós de storage em cada local. Esta replicação não é configurável e executada automaticamente.

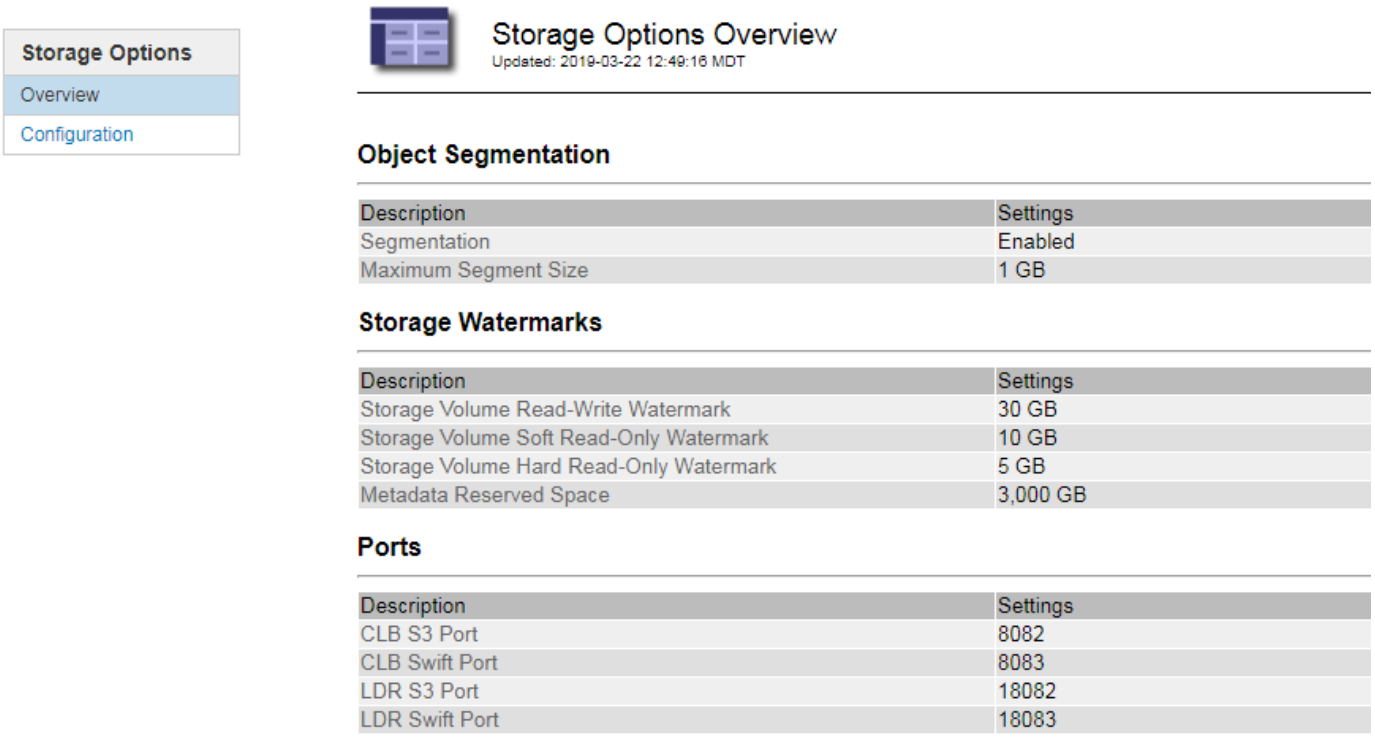
"Gerenciamento do storage de metadados de objetos"

Gerenciando Opções de armazenamento

Você pode exibir e configurar Opções de armazenamento usando o menu Configuração

no Gerenciador de Grade. As opções de armazenamento incluem as definições de segmentação de objetos e os valores atuais para marcas d'água de armazenamento. Você também pode exibir as portas S3 e Swift usadas pelo serviço CLB obsoleto em nós de Gateway e pelo serviço LDR em nós de armazenamento.

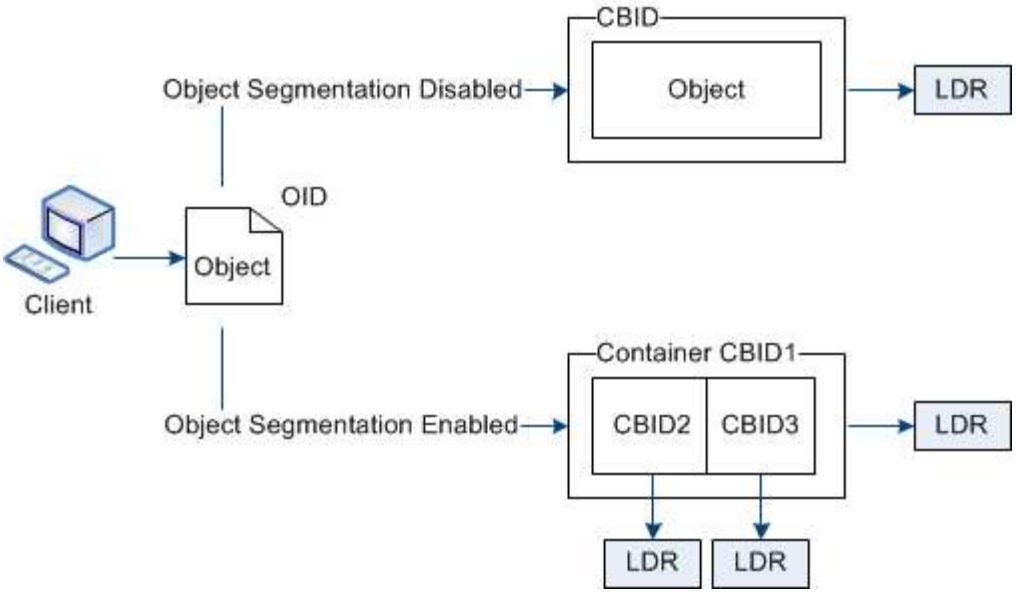
Para obter informações sobre atribuições de portas, "Resumo: Endereços IP e portas para conexões de clientes"consulte .



Qual é a segmentação de objetos

A segmentação de objetos é o processo de dividir um objeto em uma coleção de objetos menores de tamanho fixo, a fim de 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.



Se o seu sistema StorageGRID incluir um nó de arquivamento cujo tipo de destino é disposição em camadas na nuvem — Serviço de armazenamento simples e o sistema de armazenamento de arquivamento segmentado for o Amazon Web Services (AWS), o tamanho máximo do segmento deve ser menor ou igual a 4,5 GiB (4.831.838.208 bytes). Esse limite superior garante que a limitação de cinco GBs da AWS não seja excedida. As solicitações à AWS que excedem esse valor falham.

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.

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:

segmento de container e segmento 1 e segmento 2 são três objetos armazenados

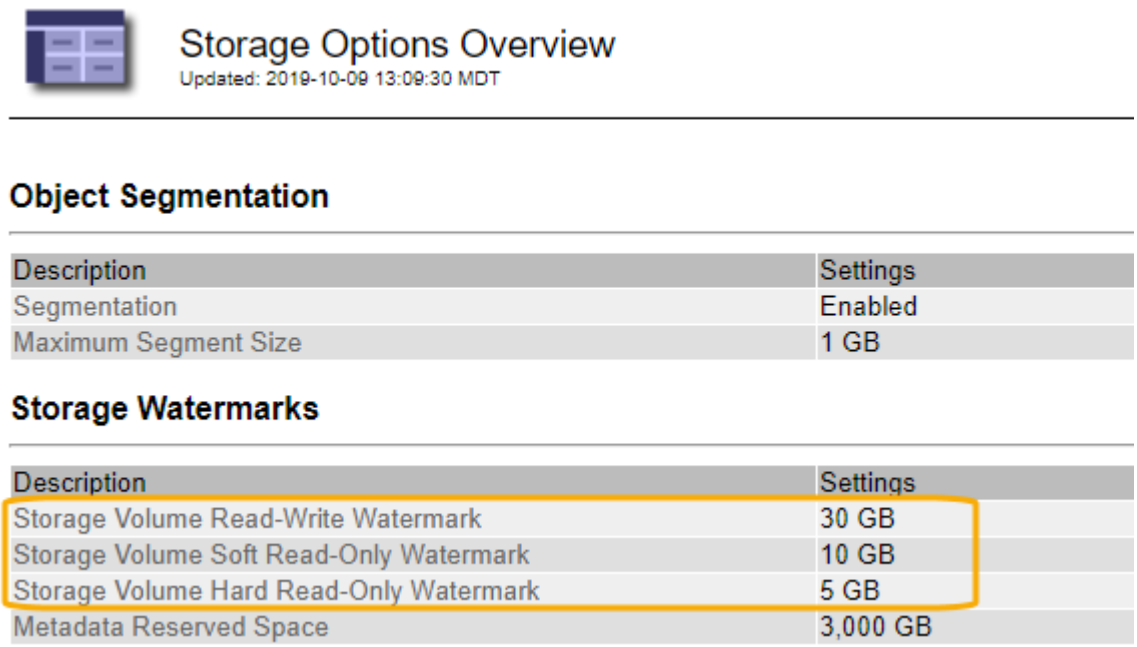
Você pode melhorar o desempenho ao lidar com objetos grandes, garantindo que:

- Cada Gateway e nó de armazenamento tem largura de banda de rede suficiente para a taxa de transferência necessária. Por exemplo, configure redes Grid e Client separadas em interfaces Ethernet de 10 Gbps.
- Nós de Gateway e storage suficientes são implantados para a taxa de transferência necessária.
- Cada nó de storage tem desempenho de e/S de disco suficiente para a taxa de transferência necessária.

Quais são as marcas d'água do volume de armazenamento

O StorageGRID usa marcas d'água de volume de storage para permitir que você monitore a quantidade de espaço utilizável disponível nos nós de storage. Se a quantidade de espaço disponível em um nó for menor do que uma configuração de marca d'água configurada, o alarme de Status do armazenamento (SSTS) será acionado para que você possa determinar se precisa adicionar nós de armazenamento.

Para ver as definições atuais das marcas de água do volume de armazenamento, selecione **Configuração** > **Opções de armazenamento** > **Visão geral**.



Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

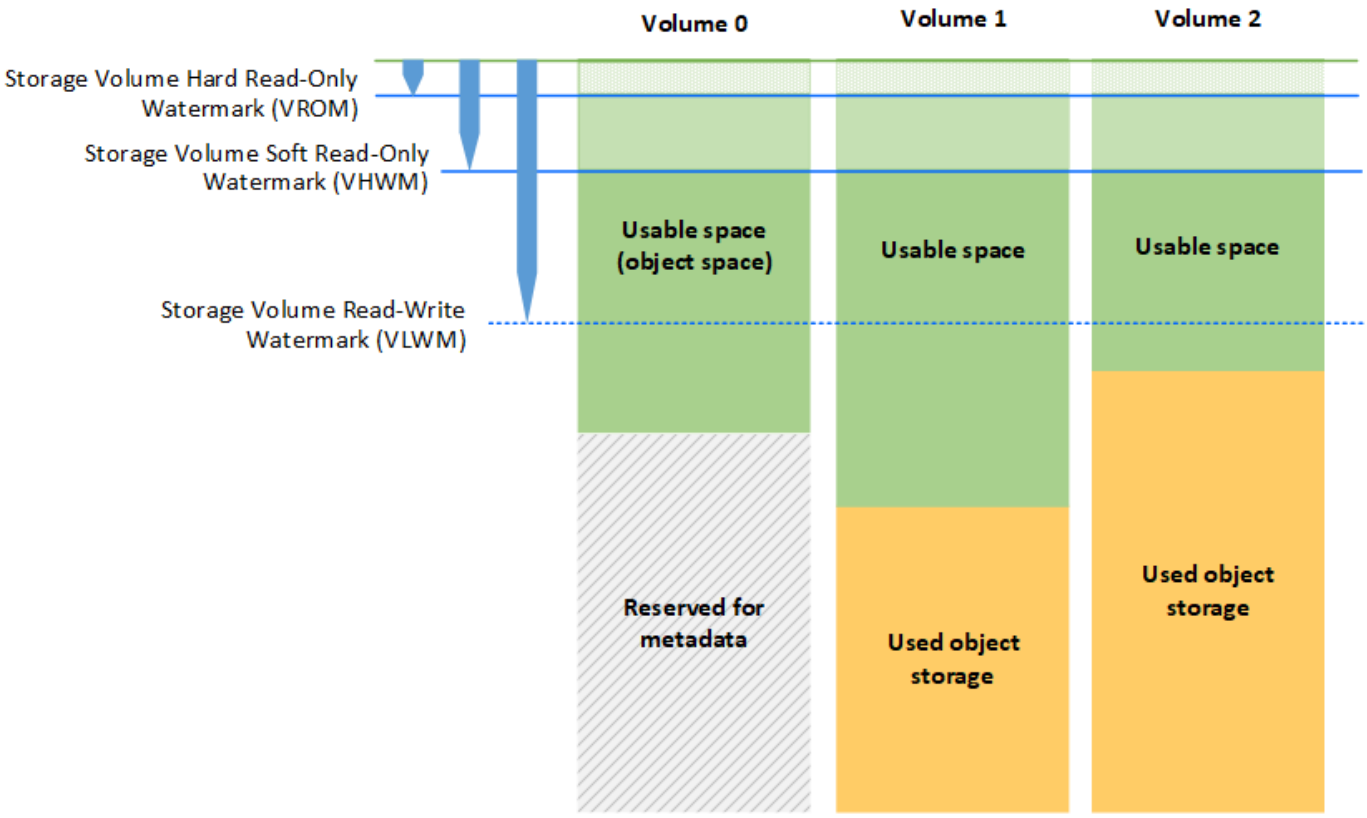
Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

A figura a seguir representa um nó de armazenamento que tem três volumes e mostra a posição relativa das três marcas d'água do volume de armazenamento. Em cada nó de storage, o StorageGRID reserva espaço no volume 0 para metadados de objetos. Qualquer espaço restante nesse volume é usado para dados de objetos. Todos os outros volumes são usados exclusivamente para dados de objetos, o que inclui cópias replicadas e fragmentos codificados por apagamento.



As marcas de água do volume de armazenamento são padrões de todo o sistema que indicam a quantidade mínima de espaço livre necessária em cada volume no nó de armazenamento para evitar que o StorageGRID altere o comportamento de leitura e gravação do nó ou acione um alarme. Observe que todos os volumes devem alcançar a marca d'água antes que o StorageGRID tome medidas. Se alguns volumes tiverem mais do que a quantidade mínima necessária de espaço livre, o alarme não será acionado e o comportamento de leitura e gravação do nó não será alterado.

Marca d'água suave apenas de leitura (VHWM)

A marca d'água somente leitura suave do volume de armazenamento é a primeira marca d'água a indicar que o espaço utilizável de um nó para dados de objeto está se tornando cheio. Essa marca d'água representa quanto espaço livre deve existir em cada volume em um nó de armazenamento para impedir que o nó entre no "modo somente leitura fácil". O modo somente leitura suave significa que o nó de armazenamento anuncia serviços somente leitura para o resto do sistema StorageGRID, mas atende a todas as solicitações de gravação pendentes.

Se a quantidade de espaço livre em cada volume for inferior à definição desta marca d'água, o alarme de Estado de armazenamento (SSTS) é acionado no nível de aviso e o nó de armazenamento passa para o modo apenas leitura suave.

Por exemplo, suponha que o volume de armazenamento Soft Read-Only Watermark esteja definido como 10 GB, que é o valor padrão. Se menos de 10 GB de espaço livre permanecer em cada volume no nó de armazenamento, o alarme SSTS é acionado no nível de aviso e o nó de armazenamento passa para o modo apenas leitura suave.

Marca d’água apenas de leitura (VROM)

A marca d’água 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. Essa marca d’água representa quanto espaço livre deve existir em cada volume em um nó de armazenamento para impedir que o nó entre no modo somente leitura." o modo somente leitura dura significa que o nó de armazenamento é somente leitura e não aceita mais solicitações de gravação.

Se a quantidade de espaço livre em cada volume em um nó de armazenamento for menor do que a configuração desta marca d’água, o alarme de Status de armazenamento (SSTS) será acionado no nível principal e o nó de armazenamento será transferido para o modo somente leitura.

Por exemplo, suponha que o volume de armazenamento Hard Read-Only Watermark esteja definido como 5 GB, que é o seu valor padrão. Se menos de 5 GB de espaço livre permanecer em cada volume de armazenamento no nó de armazenamento, o alarme SSTS é acionado no nível principal e o nó de armazenamento passa para o modo apenas de leitura difícil.

O valor da marca de água de apenas leitura de volume de armazenamento tem de ser inferior ao valor da marca de água de apenas leitura suave do volume de armazenamento.

Marca d’água de leitura-escrita do volume de armazenamento (VLWM)

A marca d’água de leitura e gravação do volume de armazenamento aplica-se apenas a nós de armazenamento que tenham sido transferidos para o modo somente leitura. Essa marca d’água determina quando o nó de armazenamento pode ser lido e gravado novamente.

Por exemplo, suponha que um nó de armazenamento tenha sido transferido para o modo somente leitura difícil. Se a marca de água de leitura e gravação do volume de armazenamento estiver definida como 30 GB (padrão), o espaço livre em cada volume de armazenamento no nó de armazenamento deve aumentar de 5 GB para 30 GB antes que o nó possa ser lido e gravado novamente.

O valor da marca de água de leitura-escrita do volume de armazenamento deve ser superior ao valor da marca de água de leitura suave do volume de armazenamento.

Informações relacionadas

"Gerenciamento de nós de storage completos"

Gerenciamento do 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 ou do contentor Swift, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a

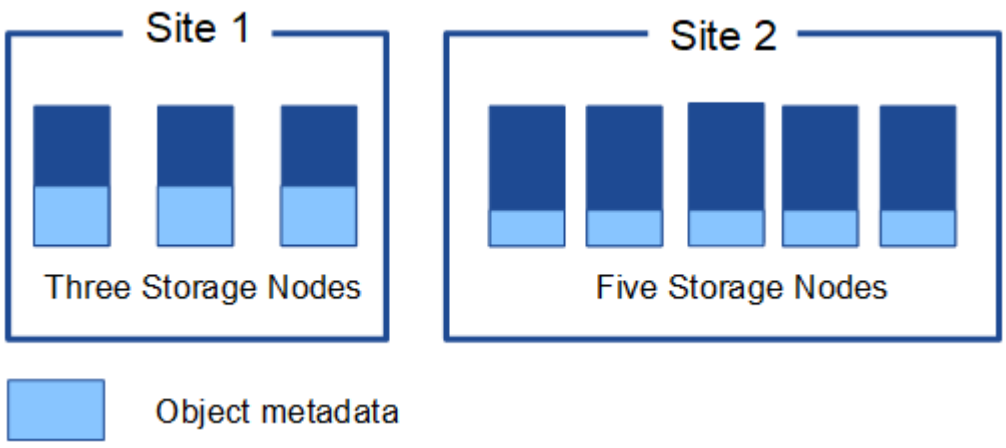
data e hora em que o objeto foi criado pela primeira vez e a data e hora em que o objeto foi modificado pela última vez.

- 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?

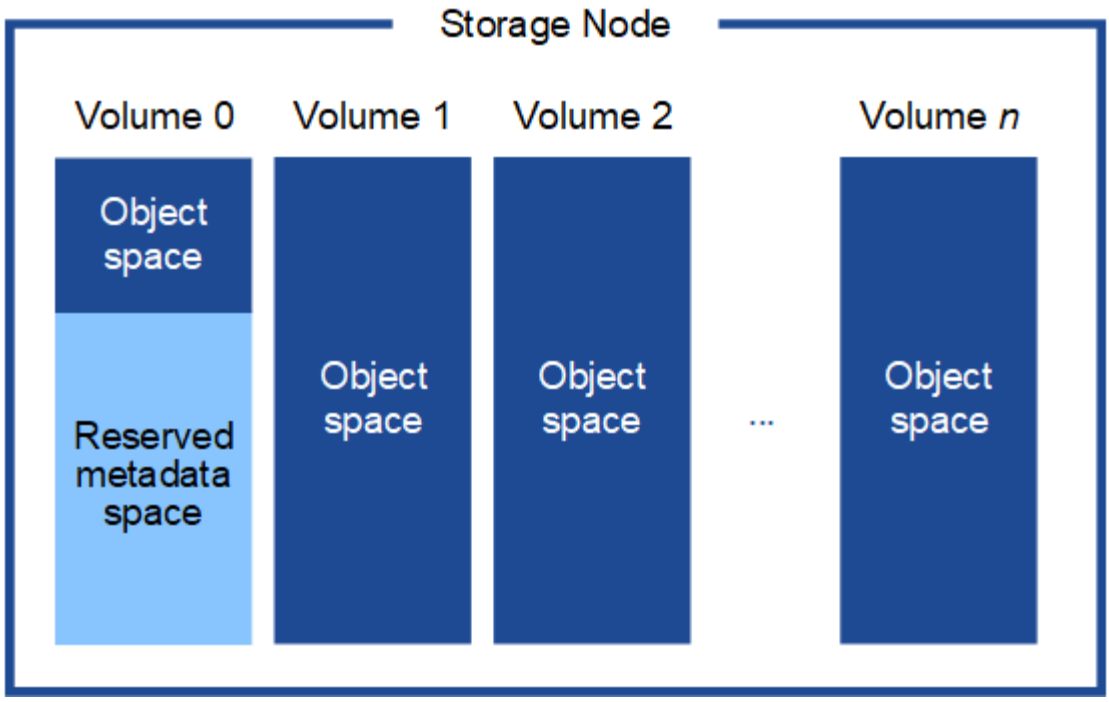
O StorageGRID mantém metadados de objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados do objeto. Para fornecer redundância e proteger os metadados de objetos contra perda, o StorageGRID armazena três cópias dos metadados de todos os objetos no sistema em cada local. As três cópias dos metadados de objetos são distribuídas uniformemente por todos os nós de storage em cada local.

Essa figura representa os nós de storage em dois locais. Cada local tem a mesma quantidade de metadados de objetos, que é igualmente distribuída pelos 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, descritos abaixo.

Definição de espaço reservado 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 para o StorageGRID 11,5 é baseado no seguinte:

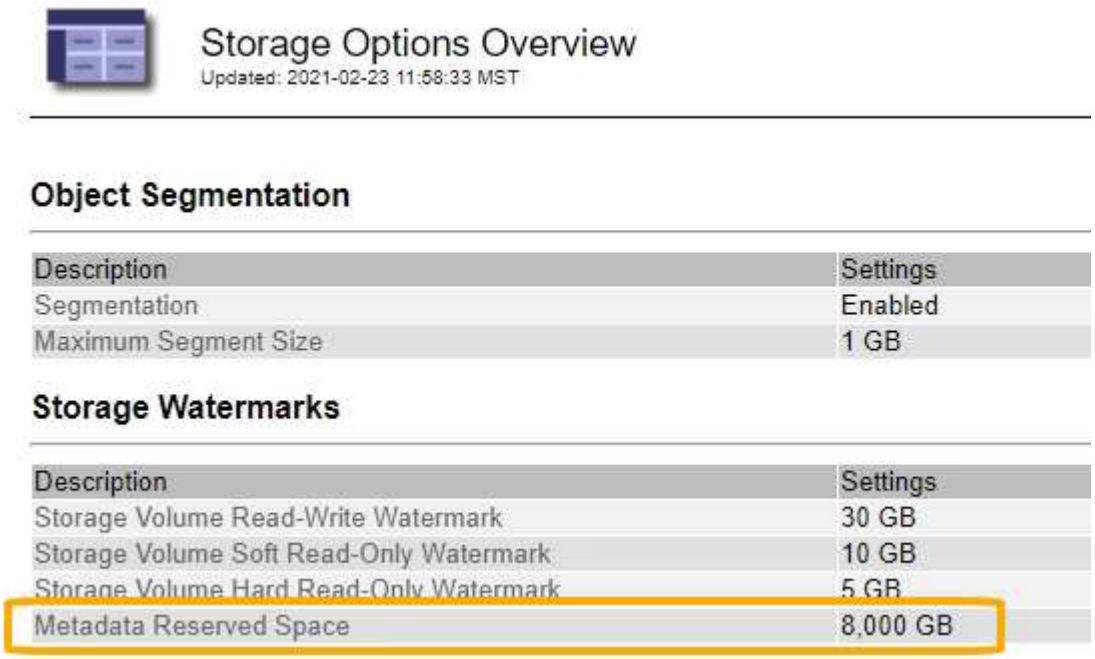
- A versão de software que você estava usando quando você instalou o StorageGRID inicialmente.
- A quantidade de RAM em cada nó de armazenamento.

Versão utilizada para a instalação inicial do StorageGRID	Quantidade de RAM nos nós de storage	Configuração de espaço reservado de metadados padrão para o StorageGRID 11,5
11,5	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)

Versão utilizada para a instalação inicial do StorageGRID	Quantidade de RAM nos nós de storage	Configuração de espaço reservado de metadados padrão para o StorageGRID 11,5
	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)

Para visualizar a definição espaço reservado metadados para o seu sistema StorageGRID:

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de armazenamento**.
2. Na tabela Storage Watermarks (marcas de água de armazenamento), localize **Metadata Reserved Space** (espaço reservado de metadados).



Na captura de tela, o valor **espaço reservado de metadados** é de 8.000 GB (8 TB). Esta é a configuração padrão para uma nova instalação do StorageGRID 11,5 na qual cada nó de armazenamento tem 128 GB ou mais de RAM.

Espaço reservado real para metadados

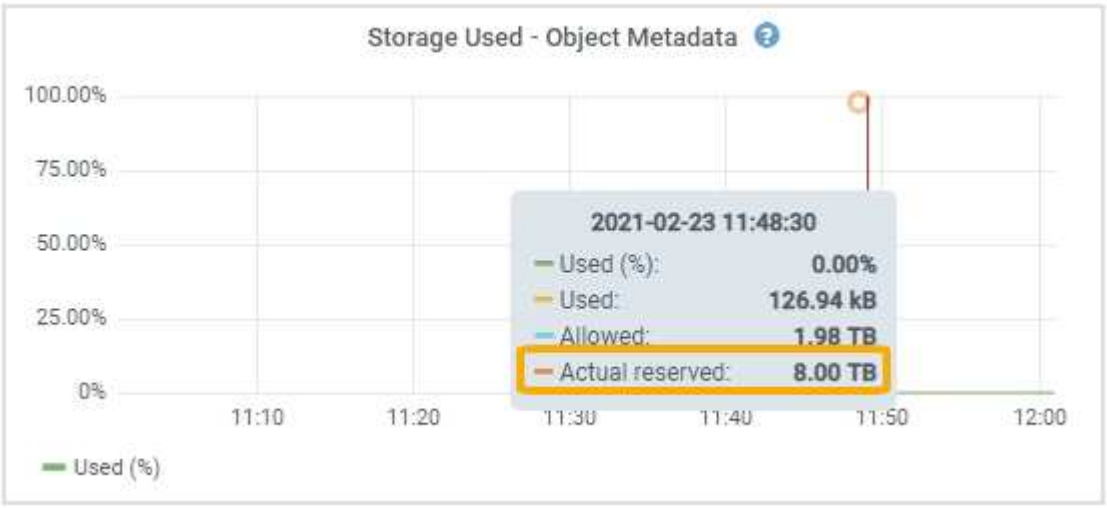
Em contraste com a configuração espaço reservado de metadados em todo o sistema, o *espaço reservado real* para metadados de objetos é determinado para cada nó de armazenamento. Para qualquer nó de armazenamento, o espaço reservado real para metadados depende do tamanho do volume 0 para o nó e da configuração **espaço reservado de 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

Tamanho do volume 0 para o nó	Espaço reservado real para metadados
500 GB ou mais	O menor desses valores: • Volume 0 • Definição de espaço reservado metadados

Para exibir o espaço reservado real para metadados em um nó de storage específico:

1. No Gerenciador de Grade, selecione **nós** > ***Storage Node***.
2. Selecione a guia **armazenamento**.
3. Passe o cursor sobre o gráfico armazenamento usado — metadados de objetos e localize o valor **atual 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 11,5. 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 este nó é igual à configuração espaço reservado de metadados.

O valor **atual reservado** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

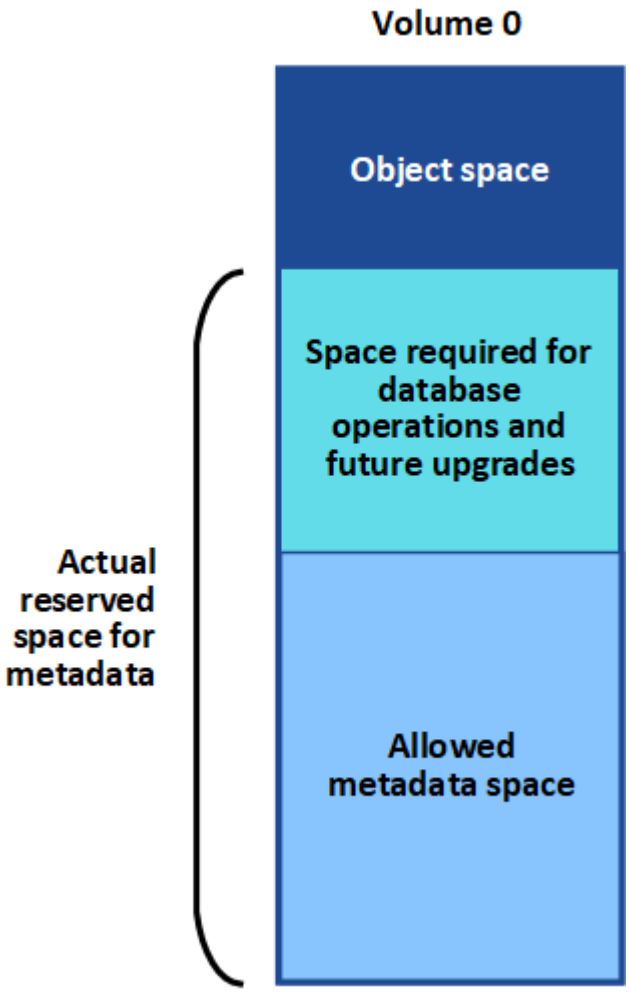
Exemplo de espaço reservado real de metadados

Suponha que você instale um novo sistema StorageGRID usando a versão 11,5. 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 **Metadata Reserved Space** em todo o sistema está definido para 8 TB. (Este é o valor padrão para uma nova instalação do StorageGRID 11,5 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.



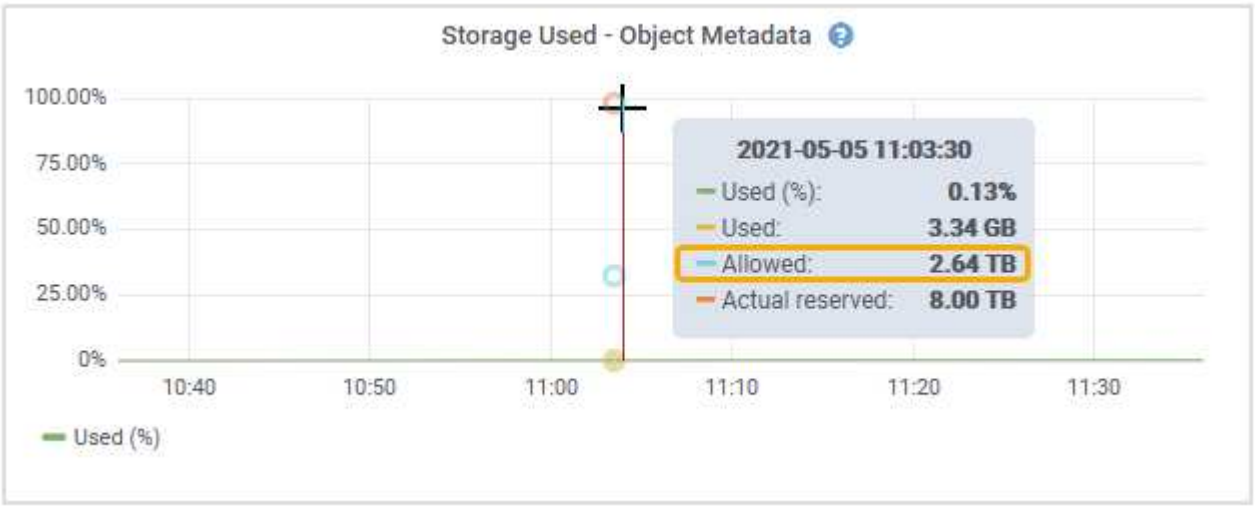
A tabela a seguir resume como o StorageGRID determina o valor de espaço de metadados permitido para um nó de storage.

Espaço reservado real para metadados	Espaço de metadados permitido
4 TB ou menos	60% do espaço reservado real para metadados, até um máximo de 1,98 TB
Mais de 4 TB	(Espaço reservado real para metadados - 1 TB) x 60%, até um máximo de 2,64 TB

Se o seu sistema StorageGRID armazenar (ou é esperado que armazene) mais de 2,64 TB de metadados em qualquer nó de armazenamento, o espaço permitido de metadados pode ser aumentado em alguns casos. Se cada um dos nós de storage tiver mais de 128 GB de RAM e espaço livre disponível no volume de armazenamento 0, entre em Contato com o representante da conta do NetApp. O NetApp analisará seus requisitos e aumentará o espaço de metadados permitido para cada nó de storage, se possível.

Para exibir o espaço de metadados permitido para um nó de storage:

1. No Gerenciador de Grade, selecione **Node** > ***Storage Node***.
2. Selecione a guia **armazenamento**.
3. Passe o cursor sobre o gráfico armazenamento usado — metadados de objetos e localize o valor **permitido**.



Na captura de tela, o valor **permitido** é de 2,64 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 11,5. 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 **Metadata Reserved Space** em todo o sistema está definido para 8 TB. (Este é o valor padrão para o StorageGRID 11,5 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 2,64 TB. (Este é o valor máximo para o espaço reservado real.)

Como os nós de storage de diferentes tamanhos afetam a capacidade do objeto

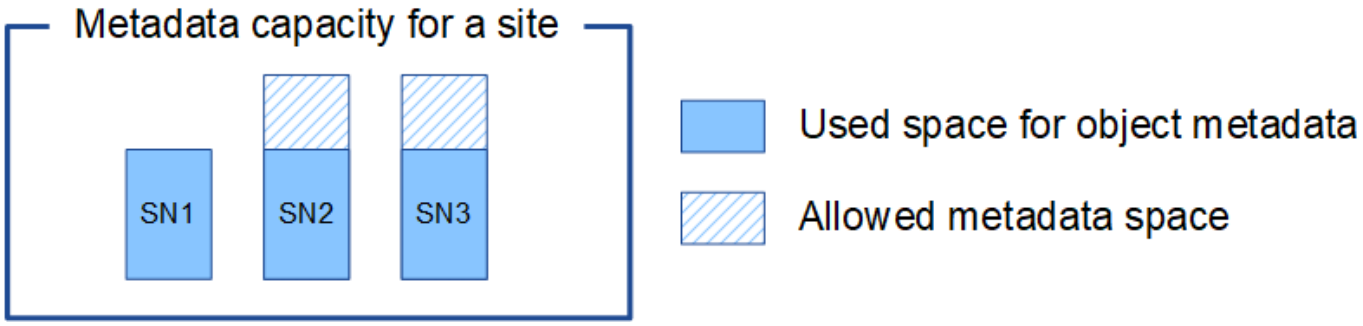
Como descrito acima, o StorageGRID distribui uniformemente os metadados de objetos nos nós de storage em cada local. Por esse motivo, se um site contiver nós de storage de tamanhos diferentes, o menor nó do local determinará a capacidade de metadados do local.

Considere o seguinte exemplo:

- Você tem uma grade de local único que contém três nós de storage de tamanhos diferentes.
- A configuração **Metadata Reserved Space** 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:

  "Monitorizar Resolução de problemas"

- Para aumentar a capacidade dos metadados de objetos do seu sistema, é necessário adicionar novos nós de storage:

  "Expanda sua grade"

Configuração de configurações globais para objetos armazenados

Você pode usar Opções de Grade para configurar as configurações de todos os objetos armazenados no seu sistema StorageGRID, incluindo compactação de objetos armazenados, criptografia de objetos armazenados e hash de objetos armazenados.

- "Configurando a compactação de objetos armazenados"
- "Configurando a criptografia de objeto armazenado"
- "Configurando hash de objeto armazenado"

Configurando a compactação de objetos armazenados

Você pode usar a opção Compress Stored Objects Grid para reduzir o tamanho dos objetos armazenados no StorageGRID, de modo que os objetos consumam menos storage.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

A opção Compress Stored Objects Grid (compactar objetos armazenados) está desativada por padrão. Se você habilitar essa opção, o StorageGRID tentará compactar cada objeto ao salvá-lo, usando compactação sem perdas.

> 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 esta opção, tenha em atenção o seguinte:

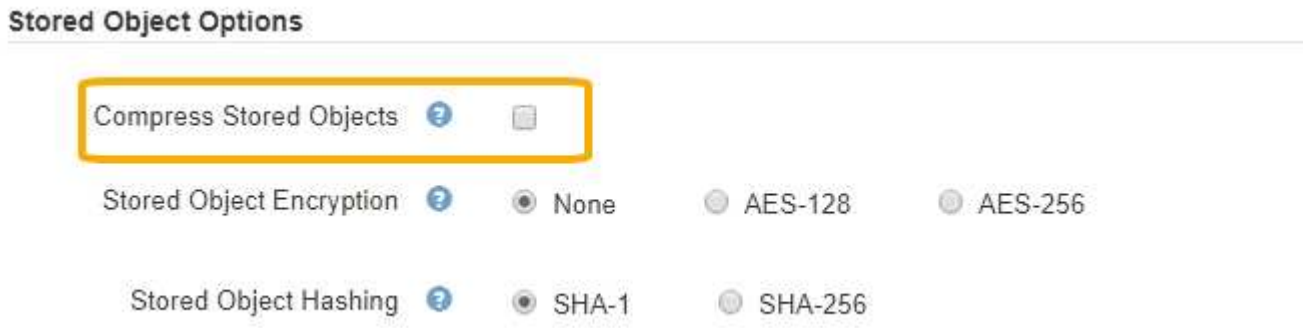
- Você não deve ativar a compactação a menos que você saiba que os dados que estão sendo armazenados são compressíveis.
- Os aplicativos que salvam objetos no StorageGRID podem compactar objetos antes de salvá-los. Se um aplicativo cliente já tiver compactado um objeto antes de salvá-lo no StorageGRID, ativar a compactação de objetos armazenados não reduzirá ainda mais o tamanho de um objeto.
- Não ative a compressão se estiver a utilizar o NetApp FabricPool com o StorageGRID.
- Se a opção Compress Stored Objects Grid estiver ativada, os aplicativos cliente S3 e Swift devem evitar executar operações GET Object que especificam um intervalo de bytes serão retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object 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 a partir 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 **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de objetos armazenados, marque a caixa de seleção **Compress Stored Objects**.



3. Clique em **Salvar**.

Configurando a criptografia de objeto armazenado

Você pode criptografar objetos armazenados se quiser garantir que os dados não possam ser recuperados de forma legível se um armazenamento de objetos for comprometido. Por padrão, os objetos não são criptografados.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

A criptografia de objetos armazenados permite a criptografia de todos os dados de objetos à medida que são ingeridos através do S3 ou Swift. 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.

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.

Os objetos armazenados podem ser criptografados usando o algoritmo de criptografia AES-128 ou AES-256.

A configuração 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.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de objetos armazenados, altere criptografia de objetos armazenados para **nenhum** (padrão), **AES-128** ou **AES-256**.

3. Clique em **Salvar**.

Configurando hash de objeto armazenado

A opção hash de objeto armazenado especifica o algoritmo de hash usado para verificar a integridade do objeto.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

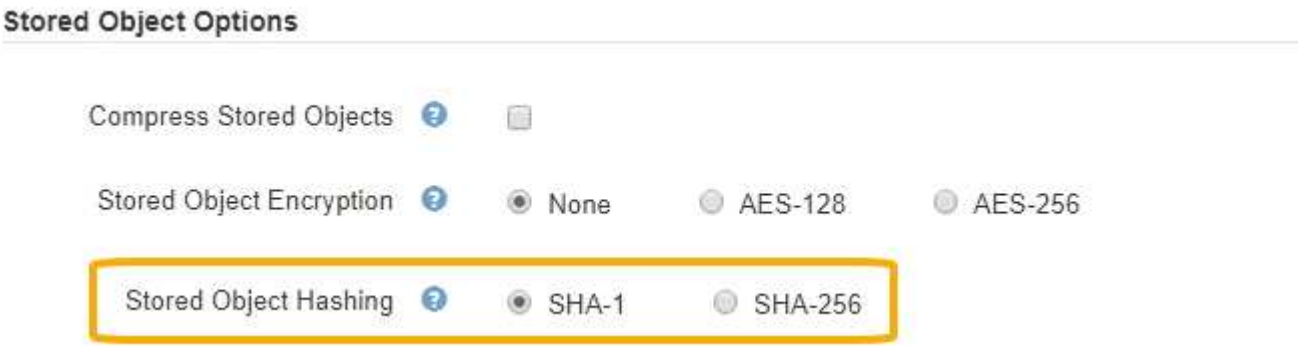
Sobre esta tarefa

Por padrão, os dados do objeto são hash usando o algoritmo SHA-1. O algoritmo SHA-256 requer recursos adicionais de CPU e geralmente não é recomendado para verificação de integridade.

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.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de objetos armazenados, altere o hash de objetos armazenados para **SHA-1** (padrão) ou **SHA-256**.



3. Clique em **Salvar**.

Configurações do nó de storage

Cada nó de armazenamento usa várias configurações e contadores. Talvez seja

necessário exibir as configurações atuais ou redefinir contadores para apagar alarmes (sistema legado).

> Exceto quando especificamente instruído na documentação, você deve consultar o suporte técnico antes de modificar qualquer configuração do nó de armazenamento. Conforme necessário, você pode redefinir contadores de eventos para limpar alarmes legados.

Para acessar as configurações e contadores de um nó de armazenamento:

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site*** > ***Storage Node***.
3. Expanda o nó de armazenamento e selecione o serviço ou componente.
4. Selecione a guia **Configuração**.

As tabelas a seguir resumem as configurações do nó de armazenamento.

LDR

Nome do atributo	Código	Descrição
Estado HTTP	HSTE	O estado atual do protocolo HTTP para S3, Swift e outro tráfego StorageGRID interno: • Offline: Não são permitidas operações e qualquer aplicativo cliente que tente abrir uma sessão HTTP para o serviço LDR recebe uma mensagem de erro. As sessões ativas estão graciosamente fechadas. • Online: A operação continua normalmente
Auto-Iniciar HTTP	HTAS	• Se selecionado, o estado do sistema ao reiniciar depende do estado do componente **LDR** > **Storage**. Se o componente **LDR** > **Storage** for somente leitura ao reiniciar, a interface HTTP também será somente leitura. Se o componente **LDR** > **Storage** estiver Online, o HTTP também estará Online. Caso contrário, a interface HTTP permanece no estado Offline. • Se não estiver selecionada, a interface HTTP permanece Offline até explicitamente ativada.

LDR > armazenamento de dados

Nome do atributo	Código	Descrição
Repor contagem de objetos perdidos	RCOR	Redefina o contador para o número de objetos perdidos neste serviço.

LDR > armazenamento

Nome do atributo	Código	Descrição
Estado de armazenamento — desejado	SSDS	Uma configuração configurável pelo usuário para o estado desejado do componente de armazenamento. O serviço LDR lê este valor e tenta corresponder ao estado indicado por este atributo. O valor é persistente entre as reinicializações. Por exemplo, você pode usar essa configuração para forçar o armazenamento a se tornar somente leitura, mesmo quando houver amplo espaço de armazenamento disponível. Isso pode ser útil para a solução de problemas. O atributo pode ter um dos seguintes valores: • Offline: Quando o estado desejado é Offline, o serviço LDR coloca o componente **LDR** > **Storage** offline. • Somente leitura: Quando o estado desejado é somente leitura, o serviço LDR move o estado de armazenamento para somente leitura e pára de aceitar novo conteúdo. Observe que o conteúdo pode continuar sendo salvo no nó de armazenamento por um curto período de tempo até que as sessões abertas sejam fechadas. • Online: Deixe o valor em Online durante as operações normais do sistema. O estado de armazenamento — a corrente do componente de armazenamento será definida dinamicamente pelo serviço com base na condição do serviço LDR, como a quantidade de espaço de armazenamento de objetos disponível. Se o espaço for baixo, o componente torna-se somente leitura.
Tempo limite de verificação de integridade	SHCT	O limite de tempo em segundos no qual um teste de verificação de integridade deve ser concluído para que um volume de armazenamento seja considerado saudável. Altere este valor apenas quando direcionado para o fazer pelo suporte.

LDR > Verificação

Nome do atributo	Código	Descrição
Repor contagem de objetos em falta	VCMI	Redefine a contagem de objetos perdidos detetados (OMIS). Utilize apenas após a conclusão da verificação em primeiro plano. Os dados de objeto replicado em falta são restaurados automaticamente pelo sistema StorageGRID.
Verifique	FVOV	Selecione armazenamentos de objetos nos quais executar a verificação de primeiro plano.
Taxa de verificação	VPRI	Defina a taxa em que a verificação de fundo ocorre. Consulte informações sobre como configurar a taxa de verificação em segundo plano.
Repor contagem de objetos corrompidos	VCCR	Redefina o contador para obter dados de objeto replicado corrompidos encontrados durante a verificação em segundo plano. Esta opção pode ser usada para limpar a condição de alarme objetos corrompidos detetados (OCOR). Para obter detalhes, consulte as instruções para monitoramento e solução de problemas do StorageGRID.
Excluir objetos em quarentena	OQRT	Exclua objetos corrompidos do diretório de quarentena, redefina a contagem de objetos em quarentena para zero e limpe o alarme objetos em quarentena detetados (OQRT). Esta opção é usada depois que objetos corrompidos foram restaurados automaticamente pelo sistema StorageGRID. Se um alarme de objetos perdidos for acionado, o suporte técnico pode querer acessar os objetos em quarentena. Em alguns casos, objetos em quarentena podem ser úteis para a recuperação de dados ou para depurar os problemas subjacentes que causaram as cópias de objetos corrompidas.

LDR > codificação de apagamento

Nome do atributo	Código	Descrição
Repor gravações contagem de falhas	RSWF	Redefina o contador para falhas de gravação de dados de objetos codificados por apagamento no nó de storage.
A reinicialização lê a contagem de falhas	RSRF	Redefina o contador para falhas de leitura de dados de objetos codificados por apagamento a partir do nó de armazenamento.

Nome do atributo	Código	Descrição
A reposição elimina a contagem de falhas	RSDF	Redefina o contador para falhas de exclusão de dados de objetos codificados por apagamento do nó de storage.
Repor contagem de cópias corrompidas detetadas	RSCC	Redefina o contador para o número de cópias corrompidas de dados de objetos codificados por apagamento no nó de storage.
Repor a contagem de fragmentos corrompidos detetados	RSCD	Redefina o contador de fragmentos corrompidos de dados de objetos codificados por apagamento no nó de storage.
Repor contagem de fragmentos detetados em falta	RSMD	Redefina o contador de fragmentos ausentes de dados de objetos codificados por apagamento no nó de storage. Utilize apenas após a conclusão da verificação em primeiro plano.

LDR > replicação

Nome do atributo	Código	Descrição
Repor contagem de falhas de replicação de entrada	RICR	Redefina o contador para falhas de replicação de entrada. Isso pode ser usado para limpar o alarme RIRF (replicação de entrada — Falha).
Repor contagem de falhas de replicação efetuada	ROCR	Redefina o contador para falhas de replicação de saída. Isso pode ser usado para limpar o alarme RORF (Outbound replicações — Failed).
Desativar replicação de entrada	DSIR	Selecione para desativar a replicação de entrada como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal. Quando a replicação de entrada é desativada, os objetos podem ser recuperados do nó de armazenamento para cópia para outros locais no sistema StorageGRID, mas os objetos não podem ser copiados para este nó de armazenamento a partir de outros locais: O serviço LDR é somente leitura.

Nome do atributo	Código	Descrição
Desativar replicação efetuada	DSOR	Selecione para desativar a replicação de saída (incluindo solicitações de conteúdo para recuperações HTTP) como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal. Quando a replicação de saída é desativada, os objetos podem ser copiados para este nó de armazenamento, mas os objetos não podem ser recuperados do nó de armazenamento para serem copiados para outros locais no sistema StorageGRID. O serviço LDR é apenas de escrita.

Informações relacionadas

"Monitorizar Resolução de problemas"

Gerenciamento de 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.

Adição de 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 expandir um sistema StorageGRID.

Adição de gavetas de expansão de storage

Alguns nós de storage de dispositivos StorageGRID, como o SG6060, 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 expandir um sistema StorageGRID.

Adição de 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 expandir um sistema StorageGRID.

Informações relacionadas

"Expanda sua grade"

Gerenciando nós de administração

Cada local em uma implantação do StorageGRID pode ter um ou mais nós de administração.

- "O que é um nó Admin"
- "Usando vários nós de administração"
- "Identificando o nó de administração principal"
- "Selecionar um remetente preferido"
- "Exibindo status de notificação e filas"
- "Como os nós de administração mostram alarmes reconhecidos (sistema legado)"
- "Configurando o acesso de cliente de auditoria"

O que é um nó Admin

Os nós de administração fornecem serviços de gerenciamento, como configuração, monitoramento e log do sistema. Cada grade deve ter um nó de administração principal e pode ter qualquer número de nós de administração não primários para redundância.

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, os procedimentos de manutenção devem ser executados usando o nó de administração principal.

Os nós Admin também podem ser usados para equilibrar o tráfego de clientes S3 e Swift.

Os nós de administração hospedam os seguintes serviços:

- Serviço AMS
- Serviço CMN
- Serviço NMS
- Prometheus serviço
- Load Balancer e serviços de alta disponibilidade (para suportar tráfego de clientes S3 e Swift)

Os Admin Nodes também suportam a Management Application Program Interface (mgmt-api) para processar solicitações da API Grid Management e da API Tenant Management.

O que é o serviço AMS

O serviço do sistema de Gestão de Auditoria (AMS) controla a atividade e os eventos do sistema.

O que é o serviço CMN

O serviço CMN (Configuration Management Node) gerencia configurações de conetividade e recursos de protocolo em todo o sistema necessárias para todos os serviços. Além disso, o serviço CMN é usado para executar e monitorar tarefas de grade. Há apenas um serviço CMN por implantação do StorageGRID. O nó Admin que hospeda o serviço CMN é conhecido como nó Admin principal.

O que é o serviço NMS

O serviço do sistema de Gerenciamento de rede (NMS) alimenta as opções de monitoramento, relatórios e configuração que são exibidas através do Gerenciador de Grade, a interface baseada no navegador do sistema StorageGRID.

O que é o serviço Prometheus

O serviço Prometheus coleta métricas de séries temporais dos serviços em todos os nós.

Informações relacionadas

"Usando a API de gerenciamento de grade"

"Use uma conta de locatário"

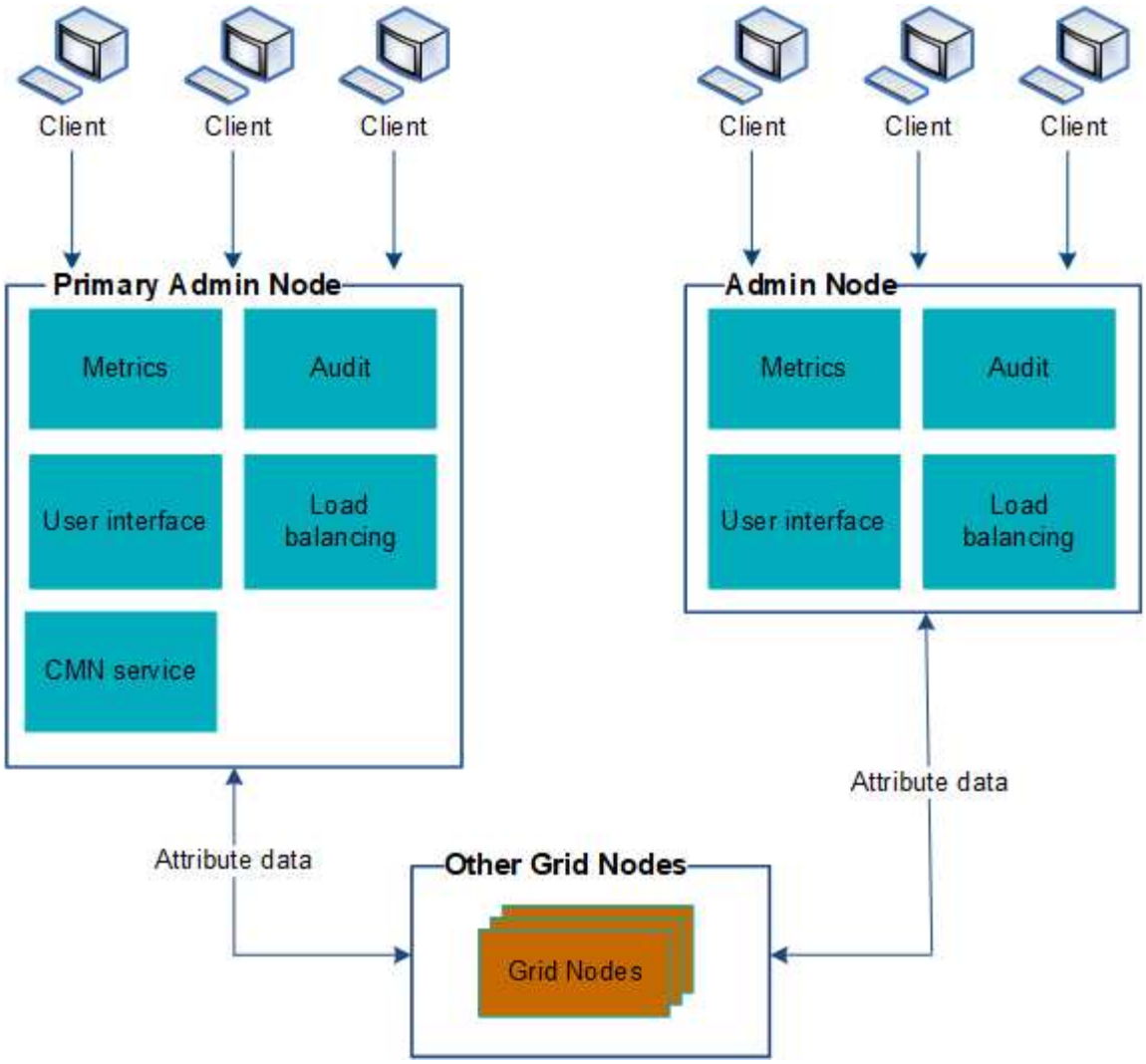
"Gerenciamento do balanceamento de carga"

"Gerenciamento de grupos de alta disponibilidade"

Usando 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 continuará, alertas e alarmes (sistema legado) ainda serão acionados e notificações de e-mail e mensagens AutoSupport ainda serão enviadas. No entanto, ter vários nós de administração não fornece proteção contra failover, exceto notificações e mensagens AutoSupport. Em particular, os reconhecimentos de alarmes feitos de um nó Admin não são copiados para outros nós Admin.



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.

> Ao usar um grupo de HA, o acesso é interrompido se o nó de administração principal 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.

Informações relacionadas

"Gerenciamento de grupos de alta disponibilidade"

Identificando o nó de administração principal

O nó de administração principal hospeda o serviço CMN. Alguns procedimentos de manutenção só podem ser executados usando o nó de administração principal.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site*** > **Admin Node** e, em seguida, clique ➕ para expandir a árvore de topologia e mostrar os serviços hospedados neste Admin Node.

   O nó de administração principal hospeda o serviço CMN.

3. Se este nó Admin não hospedar o serviço CMN, verifique os outros nós Admin.

Selecionar um remetente preferido

Se a implantação do StorageGRID incluir vários nós de administração, você poderá selecionar qual nó de administração deve ser o remetente preferido de notificações. Por padrão, o nó Admin principal é selecionado, mas qualquer nó Admin pode ser o remetente preferido.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

A página **Configuração** > **Configurações do sistema** > **Opções de exibição** mostra qual nó Admin está selecionado atualmente para ser o remetente preferido. O nó de administração principal é selecionado por padrão.

Em operações normais do sistema, apenas o remetente preferido envia as seguintes notificações:

- Mensagens AutoSupport
- Notificações SNMP
- E-mails de alerta
- E-mails de alarme (sistema legado)

No entanto, todos os outros nós Admin (remetentes de reserva) monitoram o remetente preferido. Se for detetado um problema, um remetente em espera também pode enviar essas notificações.

Tanto o remetente preferido quanto um remetente em espera podem enviar notificações nestes casos:

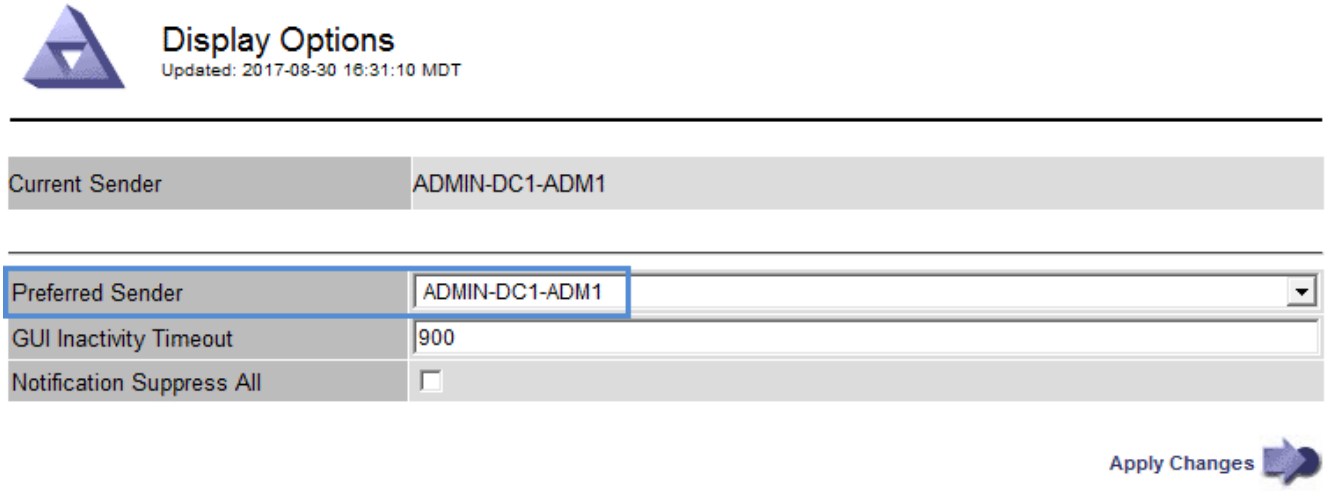
- Se os nós de administrador se tornarem "'desembarcados'" uns dos outros, tanto o remetente preferido quanto o remetente de reserva tentarão enviar notificações, e várias cópias de notificações podem ser recebidas.

- Depois que um 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 notificações de alarme e mensagens AutoSupport, todos os nós de administração enviam o e-mail de teste. Ao testar notificações de alerta, você deve entrar em cada nó de administração para verificar a conetividade.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**.
2. No menu Opções de exibição, selecione **Opções**.
3. Selecione o nó Admin que deseja definir como o remetente preferido na lista suspensa.



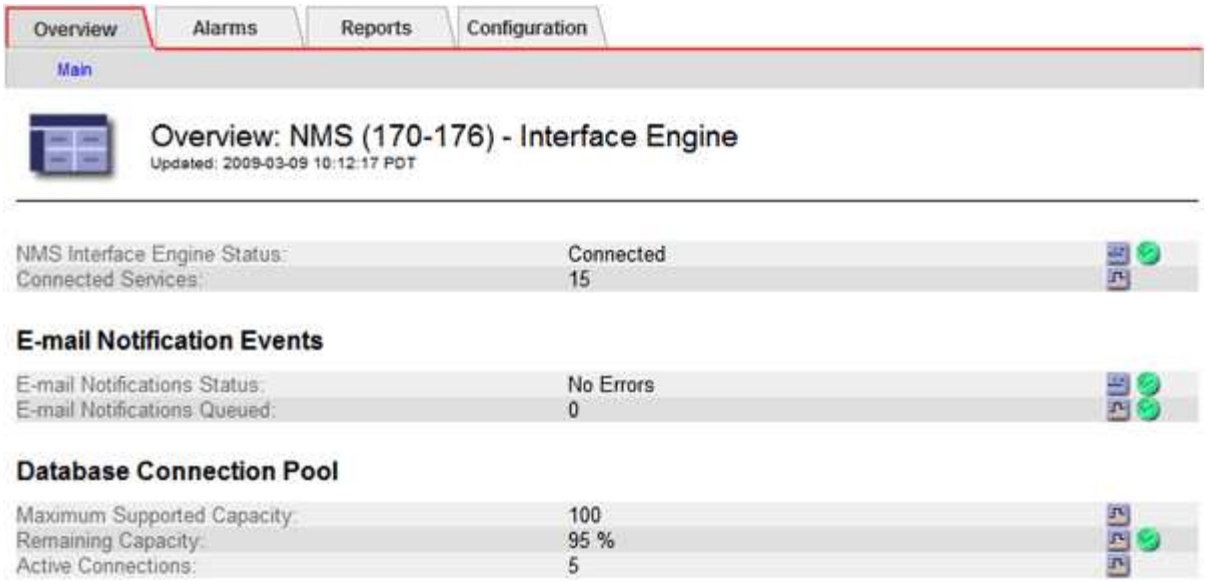
4. Clique em **aplicar alterações**.

   O Admin Node é definido como o remetente preferido de notificações.

Exibindo status de notificação e filas

O serviço NMS nos Admin Nodes 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 **suporte** > **Ferramentas** > **topologia de grade**. Finalmente, selecione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.

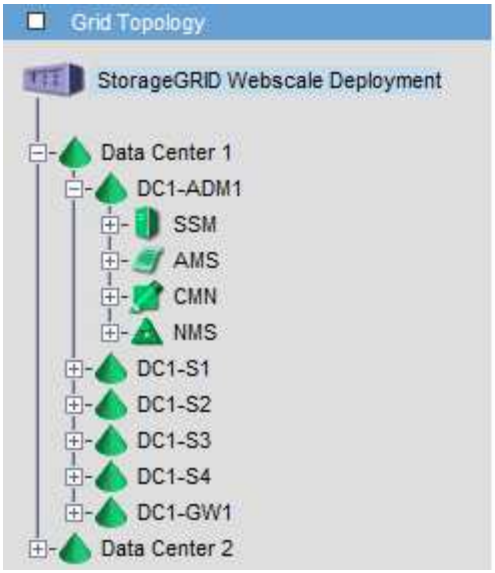


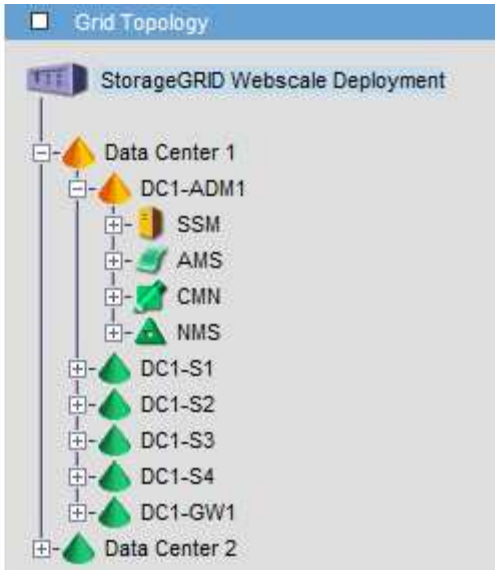
As notificações são processadas através da fila de notificações de e-mail e são enviadas para o servidor de e-mail uma após a outra na ordem em que são acionadas. Se houver um problema (por exemplo, um erro de conexão de rede) e o servidor de e-mail não estiver disponível quando a tentativa for feita 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. Como as notificações podem ser retiradas da fila de notificações sem serem enviadas, é possível que um alarme possa ser acionado sem que uma notificação seja enviada. No caso de uma notificação ser retirada da fila sem ser enviada, o alarme Minor MINS (Status da notificação por e-mail) é acionado.

Como os nós de administração mostram alarmes reconhecidos (sistema legado)

Quando você reconhece um alarme em um nó Admin, o alarme reconhecido não é copiado para nenhum outro nó Admin. Como os reconhecimentos não são copiados para outros nós de administração, a árvore de topologia de grade pode não ter a mesma aparência para cada nó de administração.

Essa diferença pode ser útil ao conetar clientes da Web. Os clientes da Web podem ter visualizações diferentes do sistema StorageGRID com base nas necessidades do administrador.





Observe que as notificações são enviadas do nó Admin onde a confirmação ocorre.

Configurando o acesso de cliente de auditoria

O Admin Node, por meio do serviço do Audit Management System (AMS), Registra todos os eventos do sistema auditados em um arquivo de log disponível por meio do compartilhamento de auditoria, que é adicionado a cada Admin Node na instalação. Para facilitar o acesso aos logs de auditoria, você pode configurar o acesso do cliente para compartilhamentos de auditoria para CIFS e NFS.

O sistema StorageGRID usa reconhecimento positivo para evitar a perda de mensagens de auditoria antes de serem gravadas no arquivo de log. Uma mensagem permanece na fila em um serviço até que o serviço AMS ou um serviço de relé de auditoria intermediária tenha reconhecido o controle dele.

Para obter mais informações, consulte as instruções para entender as mensagens de auditoria.

Se você tiver a opção de usar CIFS ou NFS, escolha NFS.

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

Informações relacionadas

"O que é um nó Admin"

"Rever registos de auditoria"

"Atualizar o software"

Configurando clientes de auditoria para CIFS

O procedimento usado para configurar um cliente de auditoria depende do método de autenticação: Windows Workgroup ou Windows ative Directory (AD). Quando adicionado, o compartilhamento de auditoria é ativado automaticamente como um compartilhamento somente leitura.

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

Informações relacionadas

"Atualizar o software"

Configurando clientes de auditoria para o Workgroup

Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

Sobre esta tarefa

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

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. Confirme se todos os serviços têm estado em execução ou verificado: `storagegrid-status`

   Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
-------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------
```

5. Defina a autenticação para o grupo de trabalho do Windows:

   Se a autenticação já tiver sido definida, é apresentada uma mensagem de aviso. Se a autenticação já tiver sido definida, vá para a próxima etapa.

   a. Introduza: `set-authentication`
   b. Quando solicitado para a instalação do Windows Workgroup ou do ative Directory, digite: `workgroup`
   c. Quando solicitado, insira um nome do grupo de trabalho: *`workgroup_name`*
   d. Quando solicitado, crie um nome NetBIOS significativo: *`netbios_name`*

      ou

      Pressione **Enter** para usar o nome do host do Admin Node como o nome NetBIOS.

   O script reinicia o servidor Samba e as alterações são aplicadas. Isso deve levar menos de um minuto. Depois de definir a autenticação, adicione um cliente de auditoria.

   a. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

6. Adicionar um cliente de auditoria:

   a. Introduza: `add-audit-share`

      ⓘ O compartilhamento é adicionado automaticamente como somente leitura.

   b. Quando solicitado, adicione um usuário ou grupo: *`user`*
   c. Quando solicitado, insira o nome de usuário da auditoria: *`audit_user_name`*
   d. Quando solicitado, insira uma senha para o usuário de auditoria: *`password`*
   e. Quando solicitado, digite novamente a mesma senha para confirmá-la: *`password`*
   f. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

Não há necessidade de inserir um diretório. O nome do diretório de auditoria é predefinido.

7. Se mais de um usuário ou grupo tiver permissão para acessar o compartilhamento de auditoria, adicione os usuários adicionais:
   a. Introduza: `add-user-to-share`

      É apresentada uma lista numerada de partilhas ativadas.

   b. Quando solicitado, insira o número do compartilhamento de auditoria-exportação: *`share_number`*
   c. Quando solicitado, adicione um usuário ou grupo: `user`

      ou `group`

   d. Quando solicitado, insira o nome do usuário ou grupo de auditoria: *`audit_user or audit_group`*
   e. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

   f. Repita essas subetapas para cada usuário ou grupo adicional que tenha acesso ao compartilhamento de auditoria.
8. Opcionalmente, verifique sua configuração: `validate-config`

   Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

   ```
   Can't find include file /etc/samba/includes/cifs-interfaces.inc
   Can't find include file /etc/samba/includes/cifs-filesystem.inc
   Can't find include file /etc/samba/includes/cifs-custom-config.inc
   Can't find include file /etc/samba/includes/cifs-shares.inc
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
   (16384)
   ```

   a. Quando solicitado, pressione **Enter**.

      A configuração do cliente de auditoria é exibida.

   b. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.
9. Feche o utilitário de configuração CIFS: `exit`
10. Inicie o serviço Samba: `service smbd start`
11. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

    ou

    Opcionalmente, se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esse compartilhamento de auditoria conforme necessário:

a. Faça login remotamente no Admin Node de um site:
   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. Repita as etapas para configurar o compartilhamento de auditoria para cada nó Admin adicional.
c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`

12. Faça logout do shell de comando: `exit`

Informações relacionadas

"Atualizar o software"

Configurando clientes de auditoria para o ative Directory

Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o nome de usuário e a senha do CIFS ative Directory.
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

> A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

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. Confirme se todos os serviços têm estado em execução ou verificado: `storagegrid-status`

   Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

5. Defina a autenticação para o ative Directory: `set-authentication`

   Na maioria das implantações, você deve definir a autenticação antes de adicionar o cliente de auditoria. Se a autenticação já tiver sido definida, é apresentada uma mensagem de aviso. Se a autenticação já tiver sido definida, vá para a próxima etapa.

   a. Quando solicitado para a instalação do Workgroup ou do ative Directory: `ad`
   b. Quando solicitado, insira o nome do domínio AD (nome de domínio curto).
   c. Quando solicitado, insira o endereço IP do controlador de domínio ou o nome de host DNS.
   d. Quando solicitado, insira o nome completo do domínio realm.

      Use letras maiúsculas.

   e. Quando solicitado a ativar o suporte winbind, digite **y**.

      O Winbind é usado para resolver informações de usuários e grupos de servidores AD.

   f. Quando solicitado, insira o nome NetBIOS.
   g. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

6. Junte-se ao domínio:

   a. Se ainda não tiver sido iniciado, inicie o utilitário de configuração CIFS: `config_cifs.rb`
   b. Junte-se ao domínio: `join-domain`
   c. Você será solicitado a testar se o nó Admin é atualmente um membro válido do domínio. Se este nó Admin não tiver aderido anteriormente ao domínio, introduza: `no`
   d. Quando solicitado, forneça o nome de usuário do Administrador: *`administrator_username`*

      ```
      `_administrator_username_`Onde está o nome de usuário do CIFS ative
      Directory, não o nome de usuário do StorageGRID.
      ```

   e. Quando solicitado, forneça a senha do administrador: *`administrator_password`*

Was *administrator_password* é o nome de usuário do CIFS ative Directory, não a senha do StorageGRID.

f. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

7. Verifique se você entrou corretamente no domínio:
   a. Junte-se ao domínio: `join-domain`
   b. Quando solicitado a testar se o servidor é atualmente um membro válido do domínio, digite: `y`

      Se você receber a mensagem ""Join is OK"", você se juntou com sucesso ao domínio. Se você não receber essa resposta, tente configurar a autenticação e ingressar no domínio novamente.

   c. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

8. Adicionar um cliente de auditoria: `add-audit-share`
   a. Quando solicitado a adicionar um usuário ou grupo, digite: `user`
   b. Quando solicitado a inserir o nome de usuário da auditoria, insira o nome de usuário da auditoria.
   c. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

9. Se mais de um usuário ou grupo tiver permissão para acessar o compartilhamento de auditoria, adicione usuários adicionais: `add-user-to-share`

   É apresentada uma lista numerada de partilhas ativadas.

   a. Introduza o número da partilha de auditoria-exportação.
   b. Quando solicitado a adicionar um usuário ou grupo, digite: `group`

      Você será solicitado a fornecer o nome do grupo de auditoria.

   c. Quando solicitado o nome do grupo de auditoria, insira o nome do grupo de usuários de auditoria.
   d. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

   e. Repita esta etapa para cada usuário ou grupo adicional que tenha acesso ao compartilhamento de auditoria.

10. Opcionalmente, verifique sua configuração: `validate-config`

    Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

    - Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-interfaces.inc`
    - Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-filesystem.inc`
    - Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-interfaces.inc`

- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-custom-config.inc`
- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-shares.inc`
- Rlimit_Max: Aumentando rlimit_Max (1024) para o limite mínimo de Windows (16384)

> Não combine a configuração 'anúncios' com o parâmetro 'servidor de senha'. (Por padrão, o Samba irá descobrir o DC correto para entrar em Contato automaticamente).

i. Quando solicitado, pressione **Enter** para exibir a configuração do cliente de auditoria.

ii. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

11. Feche o utilitário de configuração CIFS: `exit`
12. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

ou

Opcionalmente, se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:

a. Faça login remotamente no Admin Node de um site:
   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. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.
c. Feche o login remoto do shell seguro para o Admin Node: `exit`

13. Faça logout do shell de comando: `exit`

Informações relacionadas

"Atualizar o software"

Adicionando um usuário ou grupo a um compartilhamento de auditoria CIFS

Você pode adicionar um usuário ou grupo a um compartilhamento de auditoria CIFS integrado à autenticação AD.

O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

Sobre esta tarefa

O procedimento a seguir é para um compartilhamento de auditoria integrado com autenticação AD.

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

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. Confirme se todos os serviços têm estado em execução ou verificado. Introduza: `storagegrid-status`

   Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Comece a adicionar um usuário ou grupo: `add-user-to-share`

   Uma lista numerada de compartilhamentos de auditoria que foram configurados é exibida.

6. Quando solicitado, insira o número para o compartilhamento de auditoria (auditoria-exportação): *`audit_share_number`*

   Você será perguntado se deseja dar a um usuário ou a um grupo acesso a esse compartilhamento de auditoria.

7. Quando solicitado, adicione um usuário ou grupo: `user` Ou `group`
8. Quando for solicitado o nome do usuário ou grupo para este compartilhamento de auditoria do AD, digite o nome.

   O usuário ou grupo é adicionado como somente leitura para o compartilhamento de auditoria tanto no

sistema operacional do servidor quanto no serviço CIFS. A configuração do Samba é recarregada para permitir que o usuário ou grupo acesse o compartilhamento de cliente de auditoria.

9. Quando solicitado, pressione **Enter**.

   O utilitário de configuração CIFS é exibido.

10. Repita estas etapas para cada usuário ou grupo que tenha acesso ao compartilhamento de auditoria.
11. Opcionalmente, verifique sua configuração: `validate-config`

    Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

    - Não foi possível encontrar include file /etc/samba/includes/cifs-interfaces.inc
    - Não foi possível encontrar include file /etc/samba/includes/cifs-filesystem.inc
    - Não foi possível encontrar include file /etc/samba/includes/cifs-custom-config.inc
    - Não foi possível encontrar include file /etc/samba/includes/cifs-shares.inc

      i. Quando solicitado, pressione **Enter** para exibir a configuração do cliente de auditoria.

      ii. Quando solicitado, pressione **Enter**.

12. Feche o utilitário de configuração CIFS: `exit`
13. Determine se você precisa habilitar compartilhamentos de auditoria adicionais, como a seguir:
    - Se a implantação do StorageGRID for um único local, vá para a próxima etapa.
    - Se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:

      i. Faça login remotamente no Admin Node de um site:

         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.

      ii. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.

      iii. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`

14. Faça logout do shell de comando: `exit`

Removendo um usuário ou grupo de um compartilhamento de auditoria CIFS

Não é possível remover o último usuário ou grupo permitido para acessar o compartilhamento de auditoria.

O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com as senhas da conta root (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

Sobre esta tarefa

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

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 o utilitário de configuração CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

3. Comece a remover um usuário ou grupo: `remove-user-from-share`

   Uma lista numerada de compartilhamentos de auditoria disponíveis para o nó Admin é exibida. O compartilhamento de auditoria é rotulado auditoria-exportação.

4. Introduza o número da partilha de auditoria: *`audit_share_number`*
5. Quando solicitado a remover um usuário ou um grupo: `user` Ou `group`

   É apresentada uma lista numerada de utilizadores ou grupos para a partilha de auditoria.

6. Introduza o número correspondente ao utilizador ou grupo que pretende remover: *`number`*

   O compartilhamento de auditoria é atualizado e o usuário ou grupo não tem mais permissão para acessar o compartilhamento de auditoria. Por exemplo:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Feche o utilitário de configuração CIFS: `exit`
8. Se a implantação do StorageGRID incluir nós de administração em outros sites, desative o compartilhamento de auditoria em cada site, conforme necessário.
9. Faça logout de cada shell de comando quando a configuração estiver concluída: `exit`

Informações relacionadas

"Atualizar o software"

Alterando um nome de usuário ou grupo de compartilhamento de auditoria CIFS

Você pode alterar o nome de um usuário ou grupo para um compartilhamento de auditoria CIFS adicionando um novo usuário ou grupo e excluindo o antigo.

Sobre esta tarefa

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

Passos

1. Adicione um novo usuário ou grupo com o nome atualizado ao compartilhamento de auditoria.
2. Exclua o nome de usuário ou grupo antigo.

Informações relacionadas

"Atualizar o software"

"Adicionando um usuário ou grupo a um compartilhamento de auditoria CIFS"

"Removendo um usuário ou grupo de um compartilhamento de auditoria CIFS"

Verificação da integração da auditoria CIFS

O compartilhamento de auditoria é somente leitura. Os ficheiros de registo destinam-se a ser lidos por aplicações de computador e a verificação não inclui a abertura de um ficheiro. Considera-se verificação suficiente que os arquivos de log de auditoria apareçam em uma janela do Windows Explorer. Após a verificação de conexão, feche

todas as janelas.

Configurando o cliente de auditoria para NFS

O compartilhamento de auditoria é ativado automaticamente como um compartilhamento somente leitura.

O que você vai precisar

- Tem de ter o `Passwords.txt` ficheiro com a palavra-passe root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).
- O cliente de auditoria deve estar usando o NFS versão 3 (NFSv3).

Sobre esta tarefa

Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

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. Confirme se todos os serviços têm estado em execução ou verificado. Introduza: `storagegrid-status`

   Se algum serviço não estiver listado como em execução ou verificado, resolva problemas antes de continuar.

3. Retorne à linha de comando. Pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração NFS. Introduza: `config_nfs.rb`

```
-----------------------------------------------------------------
| Shares                | Clients              | Config         |
-----------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
-----------------------------------------------------------------
```

5. Adicione o cliente de auditoria: `add-audit-share`
   a. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o

compartilhamento de auditoria: `client_IP_address`

b. Quando solicitado, pressione **Enter**.

6. Se mais de um cliente de auditoria tiver permissão para acessar o compartilhamento de auditoria, adicione o endereço IP do usuário adicional: `add-ip-to-share`

   a. Introduza o número da partilha de auditoria: *`audit_share_number`*

   b. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: *`client_IP_address`*

   c. Quando solicitado, pressione **Enter**.

      O utilitário de configuração NFS é exibido.

   d. Repita essas subetapas para cada cliente de auditoria adicional que tenha acesso ao compartilhamento de auditoria.

7. Opcionalmente, verifique sua configuração.

   a. Introduza o seguinte: `validate-config`

      Os serviços são verificados e exibidos.

   b. Quando solicitado, pressione **Enter**.

      O utilitário de configuração NFS é exibido.

   c. Feche o utilitário de configuração NFS: `exit`

8. Determine se você deve habilitar compartilhamentos de auditoria em outros sites.

   - Se a implantação do StorageGRID for um único local, vá para a próxima etapa.
   - Se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:

     i. Inicie sessão remotamente no Admin Node do site:

        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.

     ii. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó Admin adicional.

     iii. Feche o login de shell seguro remoto para o Admin Node remoto. Introduza: `exit`

9. Faça logout do shell de comando: `exit`

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Conceda acesso ao compartilhamento de auditoria a um novo cliente de auditoria NFS adicionando seu endereço IP ao compartilhamento ou remova um cliente de auditoria existente removendo seu endereço IP.

Adicionar um cliente de auditoria NFS a um compartilhamento de auditoria

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Conceda acesso ao compartilhamento de auditoria a um novo cliente de auditoria NFS adicionando seu endereço IP ao compartilhamento de auditoria.

O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).
- O cliente de auditoria deve estar usando o NFS versão 3 (NFSv3).

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 o utilitário de configuração NFS: `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients              | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config  |
| enable-disable-share  | remove-ip-from-share | refresh-config   |
|                       |                      | help             |
|                       |                      | exit             |
----------------------------------------------------------------------
```

3. Introduza: `add-ip-to-share`

   Uma lista de compartilhamentos de auditoria NFS habilitados no Admin Node é exibida. O compartilhamento de auditoria é listado como: `/var/local/audit/export`

4. Introduza o número da partilha de auditoria: *`audit_share_number`*
5. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: *`client_IP_address`*

   O cliente de auditoria é adicionado ao compartilhamento de auditoria.

6. Quando solicitado, pressione **Enter**.

   O utilitário de configuração NFS é exibido.

7. Repita as etapas para cada cliente de auditoria que deve ser adicionado ao compartilhamento de auditoria.
8. Opcionalmente, verifique sua configuração: `validate-config`

   Os serviços são verificados e exibidos.

   a. Quando solicitado, pressione **Enter**.

      O utilitário de configuração NFS é exibido.

9. Feche o utilitário de configuração NFS: `exit`
10. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

    Caso contrário, se a implantação do StorageGRID incluir nós de administração em outros sites, ative opcionalmente esses compartilhamentos de auditoria, conforme necessário:

    a. Faça login remotamente no Admin Node de um site:
       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. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.
    c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`
11. Faça logout do shell de comando: `exit`

Verificação da integração da auditoria NFS

Depois de configurar um compartilhamento de auditoria e adicionar um cliente de auditoria NFS, você pode montar o compartilhamento de cliente de auditoria e verificar se os arquivos estão disponíveis no compartilhamento de auditoria.

Passos

1. Verifique a conetividade (ou variante para o sistema cliente) usando o endereço IP do lado do cliente do nó Admin que hospeda o serviço AMS. Introduza: `ping IP_address`

   Verifique se o servidor responde, indicando conetividade.

2. Monte o compartilhamento de auditoria somente leitura usando um comando apropriado ao sistema operacional cliente. Um exemplo de comando Linux é (Enter em uma linha):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Use o endereço IP do nó de administração que hospeda o serviço AMS e o nome de compartilhamento predefinido para o sistema de auditoria. O ponto de montagem pode ser qualquer nome selecionado pelo cliente (por exemplo, `myAudit` no comando anterior).

3. Verifique se os arquivos estão disponíveis no compartilhamento de auditoria. Introduza: `ls myAudit /*`

```
`_myAudit_`onde está o ponto de montagem da partilha de auditoria. Deve
haver pelo menos um arquivo de log listado.
```

Remover um cliente de auditoria NFS do compartilhamento de auditoria

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Você pode remover um cliente de auditoria existente removendo seu endereço IP.

O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

Sobre esta tarefa

Não é possível remover o último endereço IP permitido para acessar o compartilhamento de auditoria.

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 o utilitário de configuração NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares               | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share      | add-ip-to-share      | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                      |                      | help            |
|                      |                      | exit            |
------------------------------------------------------------------
```

3. Remova o endereço IP do compartilhamento de auditoria: `remove-ip-from-share`

   Uma lista numerada de compartilhamentos de auditoria configurados no servidor é exibida. O compartilhamento de auditoria é listado como: `/var/local/audit/export`

4. Introduza o número correspondente à partilha de auditoria: *`audit_share_number`*

É apresentada uma lista numerada de endereços IP permitidos para aceder à partilha de auditoria.

5. Introduza o número correspondente ao endereço IP que pretende remover.

   O compartilhamento de auditoria é atualizado e o acesso não é mais permitido a partir de qualquer cliente de auditoria com este endereço IP.

6. Quando solicitado, pressione **Enter**.

   O utilitário de configuração NFS é exibido.

7. Feche o utilitário de configuração NFS: `exit`
8. Se a implantação do StorageGRID for uma implantação de vários locais de data center com nós de administração adicionais nos outros sites, desative esses compartilhamentos de auditoria conforme necessário:
   a. Faça login remotamente no Admin Node de cada site:
      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. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó Admin adicional.
   c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`
9. Faça logout do shell de comando: `exit`

Alterar o endereço IP de um cliente de auditoria NFS

1. Adicione um novo endereço IP a um compartilhamento de auditoria NFS existente.
2. Remova o endereço IP original.

Informações relacionadas

"Adicionar um cliente de auditoria NFS a um compartilhamento de auditoria"

"Remover um cliente de auditoria NFS do compartilhamento de auditoria"

Gerenciando nós de arquivamento

Opcionalmente, cada um dos locais de data center do seu sistema StorageGRID pode ser implantado com um nó de arquivo, que permite que você se conete a um sistema de armazenamento de arquivamento externo direcionado, como o Gerenciador de armazenamento Tivoli (TSM).

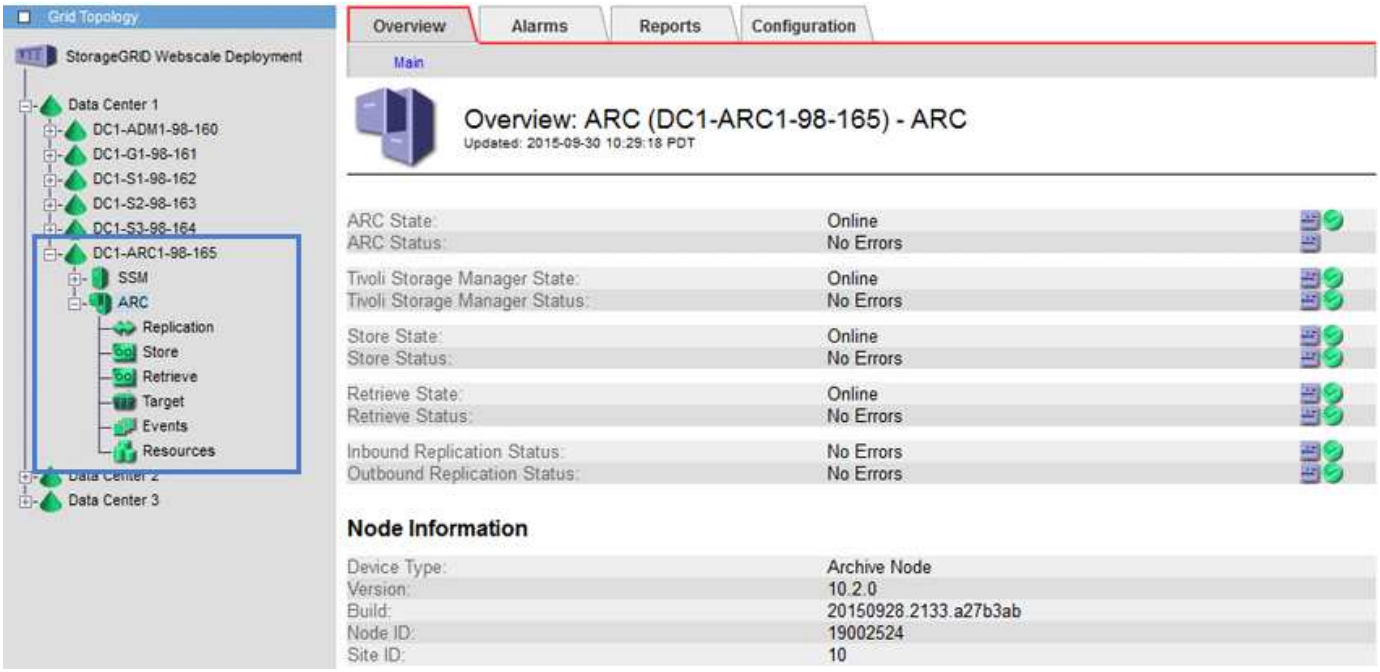
Depois de configurar as ligações ao destino externo, pode configurar o nó de arquivo para otimizar o desempenho do TSM, colocar um nó de arquivo offline quando um servidor TSM estiver a aproximar-se da capacidade ou indisponível, e configurar as definições de replicação e recuperação. Também pode definir alarmes personalizados para o nó de arquivo.

- "O que é um nó de arquivo"

- "Configurando conexões de nó de arquivo para armazenamento de arquivamento"
- "Definir alarmes personalizados para o nó de arquivo"
- "Integração do Tivoli Storage Manager"

O que é um nó de arquivo

O Archive Node fornece uma interface através da qual você pode segmentar um sistema de storage de arquivamento externo para o armazenamento de dados de objetos a longo prazo. O nó de arquivo também monitora essa conexão e a transferência de dados de objetos entre o sistema StorageGRID e o sistema de armazenamento de arquivamento externo direcionado.



Os dados de objetos que não podem ser excluídos, mas não são acessados regularmente, podem, a qualquer momento, ser movidos dos discos giratórios de um nó de storage e para um storage de arquivamento externo, como a nuvem ou a fita. Este arquivamento de dados de objetos é realizado através da configuração do nó de arquivo de um site de data center e, em seguida, a configuração de regras ILM em que este nó de arquivo é selecionado como o "destino" para instruções de posicionamento de conteúdo. O nó de arquivo não gerencia os dados de objeto arquivados em si; isso é obtido pelo dispositivo de arquivamento externo.

Os metadados de objetos não são arquivados, mas permanecem em nós de storage.

O que é o serviço ARC

O serviço Archive Node (ARC) fornece a interface de gerenciamento que você pode usar para configurar conexões com armazenamento de arquivos externo, como fita por meio do middleware TSM.

É o serviço ARC que interage com um sistema de armazenamento de arquivos externo, enviando dados de objetos para armazenamento near-line e realizando recuperações quando um aplicativo cliente solicita um objeto arquivado. Quando um aplicativo cliente solicita um objeto arquivado, um nó de armazenamento solicita os dados do objeto do serviço ARC. O serviço ARC faz uma solicitação para o sistema de armazenamento de

arquivos externo, que recupera os dados de objeto solicitados e os envia para o serviço ARC. O serviço ARC verifica os dados do objeto e os encaminha para o nó de armazenamento, que por sua vez retorna o objeto para o aplicativo cliente solicitante.

As solicitações de dados de objetos arquivados em fita por meio do middleware TSM são gerenciadas para eficiência de recuperações. As solicitações podem ser solicitadas para que os objetos armazenados em ordem sequencial na fita sejam solicitados na mesma ordem sequencial. As solicitações são então enfileiradas para envio para o dispositivo de armazenamento. Dependendo do dispositivo de arquivamento, várias solicitações de objetos em diferentes volumes podem ser processadas simultaneamente.

Configurando conexões de nó de arquivo para armazenamento de arquivamento

Ao configurar um nó de arquivo para se conetar a um arquivo externo, você deve selecionar o tipo de destino.

O sistema StorageGRID suporta o arquivamento de dados de objetos para a nuvem através de uma interface S3 ou fita através do middleware Tivoli Storage Manager (TSM).

> Uma vez configurado o tipo de destino de arquivo para um nó de arquivo, o tipo de destino não pode ser alterado.

- "Arquivamento na nuvem por meio da API S3"
- "Arquivamento para fita através do middleware TSM"
- "Configurar as definições de recuperação do nó de arquivo"
- "Configurando a replicação do Archive Node"

Arquivamento na nuvem por meio da API S3

Você pode configurar um nó de arquivo para se conetar diretamente à Amazon Web Services (AWS) ou a qualquer outro sistema que possa fazer interface com o sistema StorageGRID por meio da API S3.

> Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo por meio da API S3 foi substituído por ILM Cloud Storage Pools, que oferecem mais funcionalidade. A opção **Cloud Tiering - Simple Storage Service (S3)** ainda é suportada, mas você pode preferir implementar Cloud Storage Pools.

Se você estiver usando um nó de arquivamento com a opção **Cloud Tiering - Simple Storage Service (S3)**, considere migrar seus objetos para um pool de armazenamento em nuvem. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Informações relacionadas

"Gerenciar objetos com ILM"

Configuração das configurações de conexão para a API S3

Se você estiver se conetando a um nó de Arquivo usando a interface S3, você deverá configurar as configurações de conexão para a API S3. Até que essas configurações sejam configuradas, o serviço ARC permanece em um estado de alarme principal, pois não é possível se comunicar com o sistema de armazenamento de arquivos externo.

Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo por meio da API S3 foi substituído por ILM Cloud Storage Pools, que oferecem mais funcionalidade. A opção **Cloud Tiering - Simple Storage Service (S3)** ainda é suportada, mas você pode preferir implementar Cloud Storage Pools.

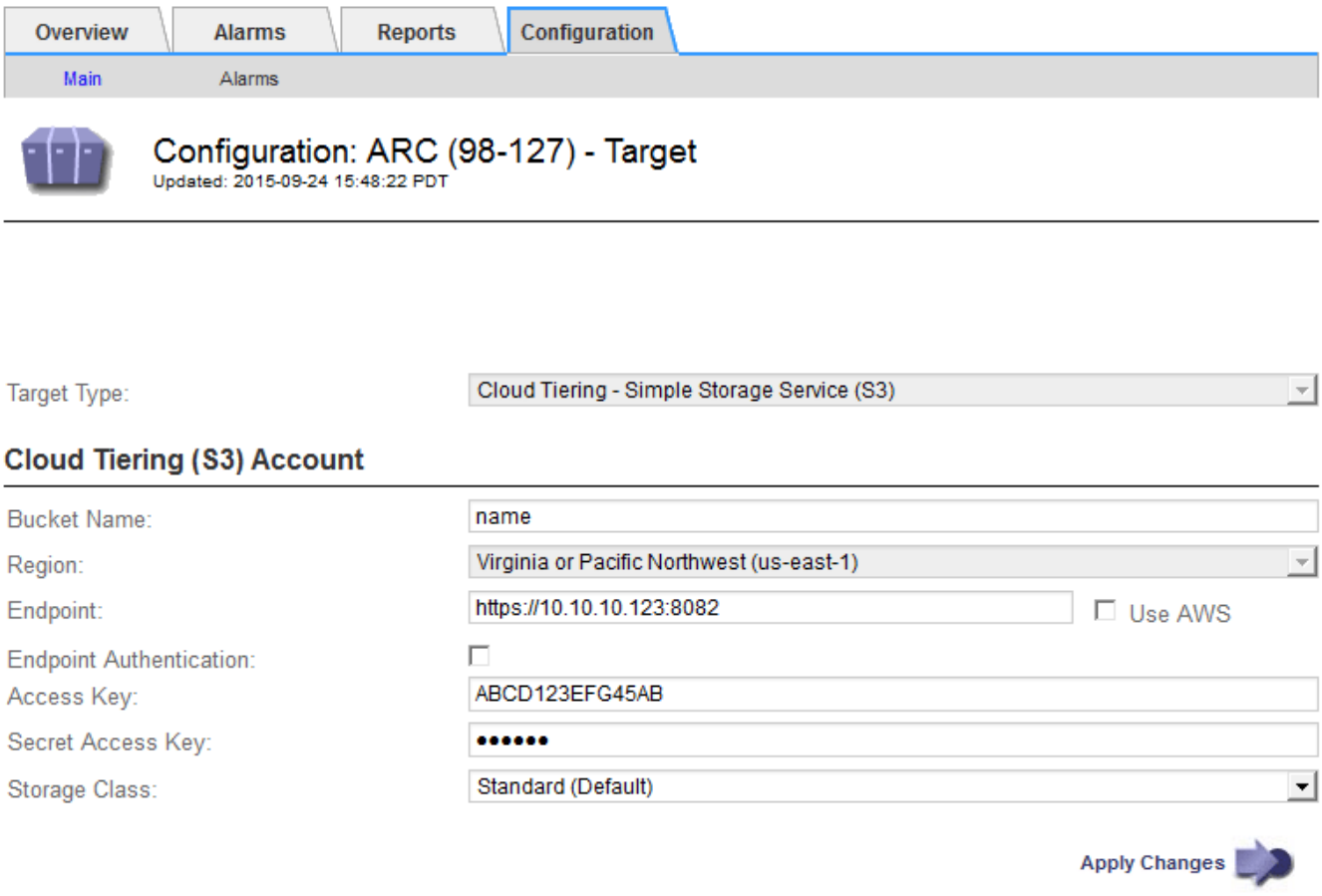
Se você estiver usando um nó de arquivamento com a opção **Cloud Tiering - Simple Storage Service (S3)**, considere migrar seus objetos para um pool de armazenamento em nuvem. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você precisa ter criado um bucket no sistema de storage de arquivamento de destino:
  - O bucket deve ser dedicado a um único nó de arquivo. Ele não pode ser usado por outros nós de arquivamento ou outras aplicações.
  - O balde tem de ter a região adequada selecionada para a sua localização.
  - O bucket deve ser configurado com o controle de versão suspenso.
- A Segmentação de objetos deve estar ativada e o tamanho máximo do segmento deve ser menor ou igual a 4,5 GiB (4.831.838.208 bytes). S3 solicitações de API que excederem esse valor falharão se S3 for usado como sistema de armazenamento de arquivamento externo.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione **Archive Node** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.



4. Selecione **disposição em camadas na nuvem - Serviço de armazenamento simples (S3)** na lista suspensa tipo de destino.

   As configurações ficam indisponíveis até que você selecione um tipo de destino.

5. Configurar a conta Cloud Tiering (S3) através da qual o Archive Node se conetará ao sistema de storage de arquivamento externo de destino com capacidade para S3.

   A maioria dos campos nesta página são auto-explicativos. A seguir descreve os campos para os quais você pode precisar de orientação.

   - **Região**: Disponível somente se **usar AWS** estiver selecionado. A região selecionada tem de corresponder à região do balde.
   - **Endpoint** e **Use AWS**: Para Amazon Web Services (AWS), selecione **Use AWS**. **Endpoint** é então preenchido automaticamente com um URL de endpoint baseado nos atributos Nome do bucket e região. Por exemplo:

     ```
     https://bucket.region.amazonaws.com
     ```

     Para um destino que não seja AWS, insira o URL do sistema que hospeda o bucket, incluindo o número da porta. Por exemplo:

```
https://system.com:1080
```

   - **Autenticação de ponto final**: Ativada por padrão. Se a rede para o sistema de armazenamento de arquivos externo for confiável, você poderá desmarcar a caixa de seleção para desativar o certificado SSL de endpoint e a verificação de nome de host para o sistema de armazenamento de arquivos

externo de destino. Se outra instância de um sistema StorageGRID for o dispositivo de armazenamento de arquivamento de destino e o sistema estiver configurado com certificados assinados publicamente, você poderá manter a caixa de seleção selecionada.

- **Classe de armazenamento**: Selecione **Standard (padrão)** para armazenamento regular. Selecione **redundância reduzida** apenas para objetos que possam ser facilmente recriados. **Redundância reduzida** fornece armazenamento de menor custo com menos confiabilidade. Se o sistema de armazenamento de arquivos de destino for outra instância do sistema StorageGRID, **Classe de armazenamento** controla quantas cópias provisórias do objeto são feitas na ingestão no sistema de destino, se a confirmação dupla for usada quando os objetos forem ingeridos lá.

6. Clique em **aplicar alterações**.

   As configurações especificadas são validadas e aplicadas ao seu sistema StorageGRID. Uma vez configurado, o destino não pode ser alterado.

Informações relacionadas

"Gerenciar objetos com ILM"

Modificação das configurações de conexão para a API S3

Depois que o nó de arquivo é configurado para se conetar a um sistema de armazenamento de arquivos externo através da API S3, você pode modificar algumas configurações caso a conexão seja alterada.

O que você vai precisar

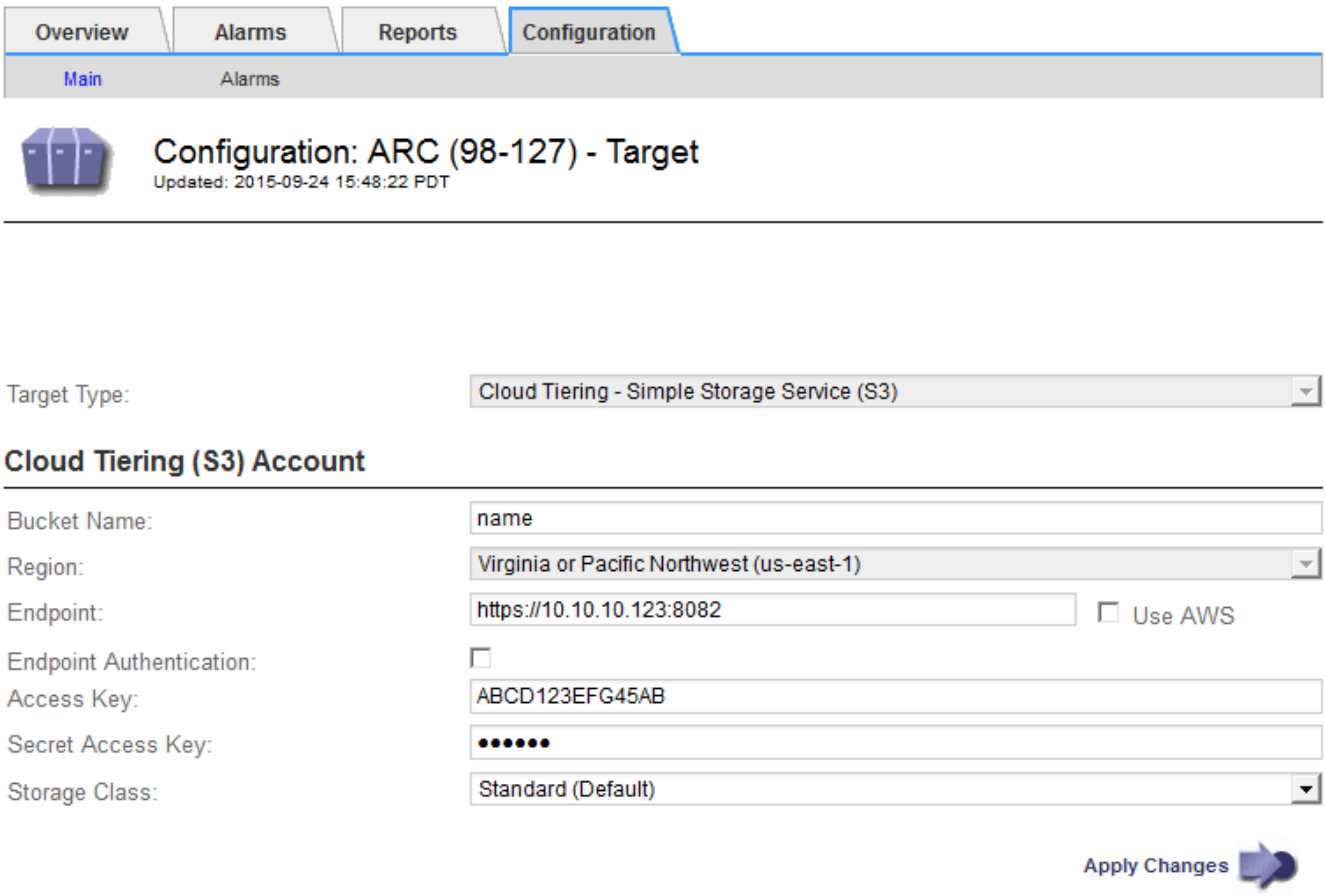
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Se você alterar a conta do Cloud Tiering (S3), deverá garantir que as credenciais de acesso do usuário tenham acesso de leitura/gravação ao bucket, incluindo todos os objetos que foram ingeridos anteriormente pelo Archive Node ao bucket.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.



4. Modifique as informações da conta, conforme necessário.

   Se você alterar a classe de armazenamento, os novos dados de objeto serão armazenados com a nova classe de armazenamento. O objeto existente continua a ser armazenado sob o conjunto de classes de armazenamento quando ingerido.

   Nome do bucket, região e ponto final, use valores da AWS e não pode ser alterado.

5. Clique em **aplicar alterações**.

Modificação do estado Cloud Tiering Service

Você pode controlar a capacidade de leitura e gravação do nó de arquivamento no sistema de storage de arquivamento externo de destino que se conecta pela API S3, alterando o estado do Cloud Tiering Service.

O que você vai precisar

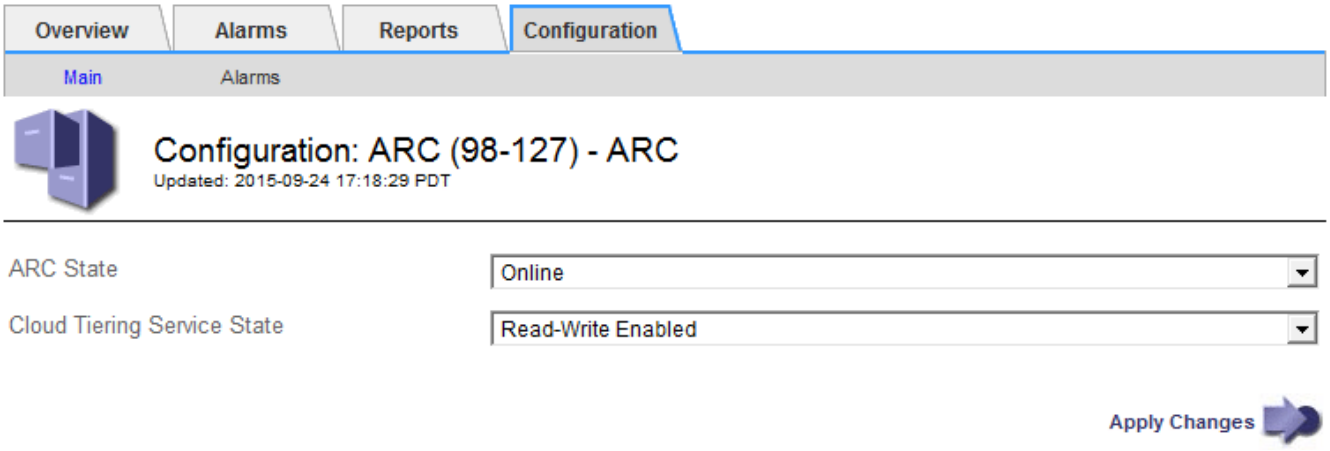
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- O nó de arquivo deve ser configurado.

Sobre esta tarefa

Você pode efetivamente colocar o nó de arquivo offline alterando o estado do Serviço de disposição em categorias na nuvem para **leitura-escrita desativada**.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC**.
3. Selecione **Configuração** > **Principal**.



4. Selecione um **Estado do Serviço de disposição em camadas na nuvem**.
5. Clique em **aplicar alterações**.

Redefinir a contagem de falhas de armazenamento para conexão com a API S3

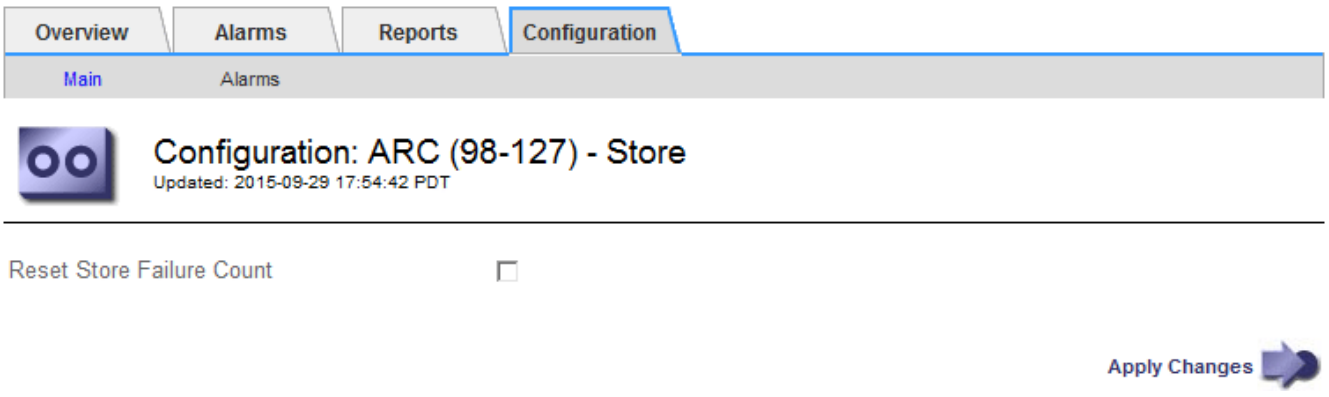
Se o seu nó de arquivo se conetar a um sistema de armazenamento de arquivos por meio da API S3, você poderá redefinir a contagem de falhas de armazenamento, que pode ser usada para limpar o alarme ARVF (falhas de armazenamento).

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.



4. Selecione **Repor contagem de falhas de armazenamento**.

5. Clique em **aplicar alterações**.

   O atributo Store Failures (falhas de armazenamento) é reposto a zero.

Migração de objetos do Cloud Tiering - S3 para um Cloud Storage Pool

Se você estiver usando o recurso **Cloud Tiering - Simple Storage Service (S3)** para categorizar dados de objetos em um bucket do S3, considere migrar seus objetos para um pool de armazenamento em nuvem. Os pools de storage em nuvem fornecem uma abordagem dimensionável que aproveita todos os nós de storage do seu sistema StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você já armazenou objetos no bucket do S3 configurado para o Cloud Tiering.

> Antes de migrar dados de objeto, entre em Contato com o representante da conta do NetApp para entender e gerenciar quaisquer custos associados.

Sobre esta tarefa

Do ponto de vista do ILM, um Cloud Storage Pool é semelhante a um pool de storage. No entanto, embora os pools de storage consistam em nós de storage ou nós de arquivamento no sistema StorageGRID, um pool de storage de nuvem consiste em um bucket externo do S3.

Antes de migrar objetos do Cloud Tiering - S3 para um pool de armazenamento em nuvem, primeiro você deve criar um bucket do S3 e, em seguida, criar o pool de armazenamento em nuvem no StorageGRID. Em seguida, você pode criar uma nova política de ILM e substituir a regra ILM usada para armazenar objetos no bucket do Cloud Tiering por uma regra ILM clonada que armazena os mesmos objetos no Cloud Storage Pool.

> Quando os objetos são armazenados em um pool de storage de nuvem, as cópias desses objetos também não podem ser armazenadas no StorageGRID. Se a regra ILM que você está usando atualmente para o Cloud Tiering estiver configurada para armazenar objetos em vários locais ao mesmo tempo, considere se você ainda deseja executar essa migração opcional porque perderá essa funcionalidade. Se você continuar com essa migração, crie novas regras em vez de clonar as existentes.

Passos

1. Crie um pool de storage em nuvem.

   Use um novo bucket do S3 para o Cloud Storage Pool para garantir que ele contenha apenas os dados gerenciados pelo Cloud Storage Pool.

2. Localize quaisquer regras de ILM na política de ILM ativa que façam com que os objetos sejam armazenados no bucket do Cloud Tiering.
3. Clone cada uma dessas regras.
4. Nas regras clonadas, altere o local de posicionamento para o novo Cloud Storage Pool.
5. Salve as regras clonadas.

6. Crie uma nova política que use as novas regras.
7. Simule e ative a nova política.

   Quando a nova política é ativada e a avaliação ILM ocorre, os objetos são movidos do bucket do S3 configurado para o bucket do Cloud Tiering para o bucket do S3 configurado para o pool de armazenamento em nuvem. O espaço utilizável na grade não é afetado. Depois que os objetos são movidos para o Cloud Storage Pool, eles são removidos do bucket do Cloud Tiering.

Informações relacionadas

"Gerenciar objetos com ILM"

Arquivamento para fita através de middleware TSM

Você pode configurar um nó de arquivo para segmentar um servidor Tivoli Storage Manager (TSM) que fornece uma interface lógica para armazenar e recuperar dados de objetos em dispositivos de armazenamento de acesso aleatório ou sequencial, incluindo bibliotecas de fitas.

O serviço ARC do Archive Node atua como um cliente para o servidor TSM, usando o Tivoli Storage Manager como middleware para comunicação com o sistema de armazenamento de arquivos.

Classes de gestão TSM

As classes de gerenciamento definidas pelo middleware TSM descrevem como as operações de backup e arquivamento do TSMs funcionam e podem ser usadas para especificar regras para conteúdo que são aplicadas pelo servidor TSM. Essas regras operam independentemente da política ILM do sistema StorageGRID e devem ser consistentes com o requisito do sistema StorageGRID de que os objetos são armazenados permanentemente e estão sempre disponíveis para recuperação pelo nó de arquivo. Depois que os dados do objeto são enviados para um servidor TSM pelo nó de arquivo, as regras de ciclo de vida e retenção do TSM são aplicadas enquanto os dados do objeto são armazenados em fita gerenciada pelo servidor TSM.

A classe de gerenciamento TSM é usada pelo servidor TSM para aplicar regras de localização ou retenção de dados depois que os objetos são enviados para o servidor TSM pelo nó de arquivamento. Por exemplo, os objetos identificados como backups de banco de dados (conteúdo temporário que pode ser substituído por dados mais recentes) podem ser tratados de forma diferente dos dados da aplicação (conteúdo fixo que deve ser mantido indefinidamente).

Configurando conexões com middleware TSM

Antes que o nó de arquivo possa se comunicar com o middleware Tivoli Storage Manager (TSM), você deve configurar várias configurações.

O que você vai precisar

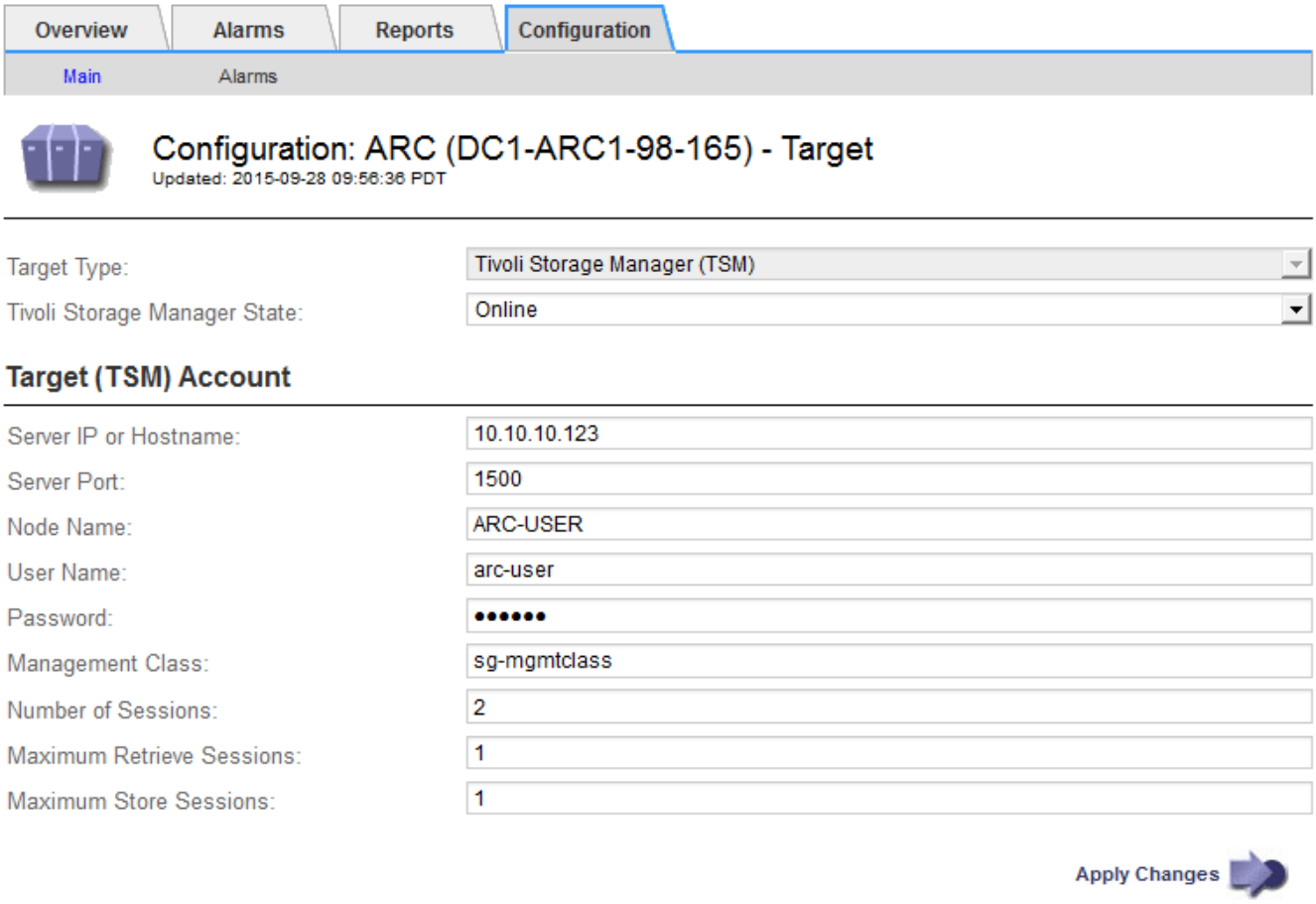
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Até que essas configurações sejam configuradas, o serviço ARC permanece em um estado de alarme principal, pois não é possível se comunicar com o Tivoli Storage Manager.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.



4. Na lista suspensa **tipo de destino**, selecione **Tivoli Storage Manager (TSM)**.
5. Para o **Tivoli Storage Manager State**, selecione **Offline** para evitar recuperações do servidor de middleware TSM.

   Por padrão, o Tivoli Storage Manager State é definido como Online, o que significa que o Archive Node é capaz de recuperar dados de objetos do servidor middleware TSM.

6. Preencha as seguintes informações:

   - **IP do servidor ou Nome de host**: Especifique o endereço IP ou nome de domínio totalmente qualificado do servidor middleware TSM usado pelo serviço ARC. O endereço IP padrão é 127,0.0,1.
   - **Server Port**: Especifique o número da porta no servidor middleware TSM ao qual o serviço ARC se conetará. A predefinição é 1500.
   - **Nome do nó**: Especifique o nome do nó de arquivo. Você deve inserir o nome (usuário ARC) registrado no servidor de middleware TSM.
   - **Nome de usuário**: Especifique o nome de usuário que o serviço ARC usa para fazer login no servidor TSM. Introduza o nome de utilizador predefinido (ARC-user) ou o utilizador administrativo que especificou para o nó de arquivo.
   - **Senha**: Especifique a senha usada pelo serviço ARC para fazer login no servidor TSM.

- **Classe de gerenciamento**: Especifique a classe de gerenciamento padrão a ser usada se uma classe de gerenciamento não for especificada quando o objeto estiver sendo salvo no sistema StorageGRID, ou a classe de gerenciamento especificada não estiver definida no servidor de middleware TSM.
- **Número de sessões**: Especifique o número de unidades de fita no servidor middleware TSM que são dedicadas ao nó de arquivo. O nó de arquivo cria simultaneamente um máximo de uma sessão por ponto de montagem mais um pequeno número de sessões adicionais (menos de cinco).

  Tem de alterar este valor para ser o mesmo que o valor definido para MAXNUMMP (número máximo de pontos de montagem) quando o nó de arquivo foi registado ou atualizado. (No comando register, o valor predefinido de MAXNUMMP utilizado é 1, se nenhum valor estiver definido.)

Você também deve alterar o valor de MAXSESSIONS para o servidor TSM para um número que seja pelo menos tão grande quanto o número de sessões definido para o serviço ARC. O valor padrão de MAXSESSIONS no servidor TSM é 25.

- * Sessões de recuperação máxima*: Especifique o número máximo de sessões que o serviço ARC pode abrir para o servidor middleware TSM para operações de recuperação. Na maioria dos casos, o valor apropriado é o número de sessões menos sessões de armazenamento máximo. Se você precisar compartilhar uma unidade de fita para armazenamento e recuperação, especifique um valor igual ao número de sessões.
- **Maximum Store Sessions**: Especifique o número máximo de sessões simultâneas que o serviço ARC pode abrir para o servidor middleware TSM para operações de arquivamento.

  Esse valor deve ser definido como um, exceto quando o sistema de armazenamento de arquivos de destino estiver cheio e somente recuperações podem ser executadas. Defina esse valor como zero para usar todas as sessões para recuperações.

7. Clique em **aplicar alterações**.

Otimizando um nó de arquivo para sessões de middleware TSM

Você pode otimizar o desempenho de um nó de arquivo que se coneta ao Tivoli Server Manager (TSM) configurando as sessões do nó de arquivo.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

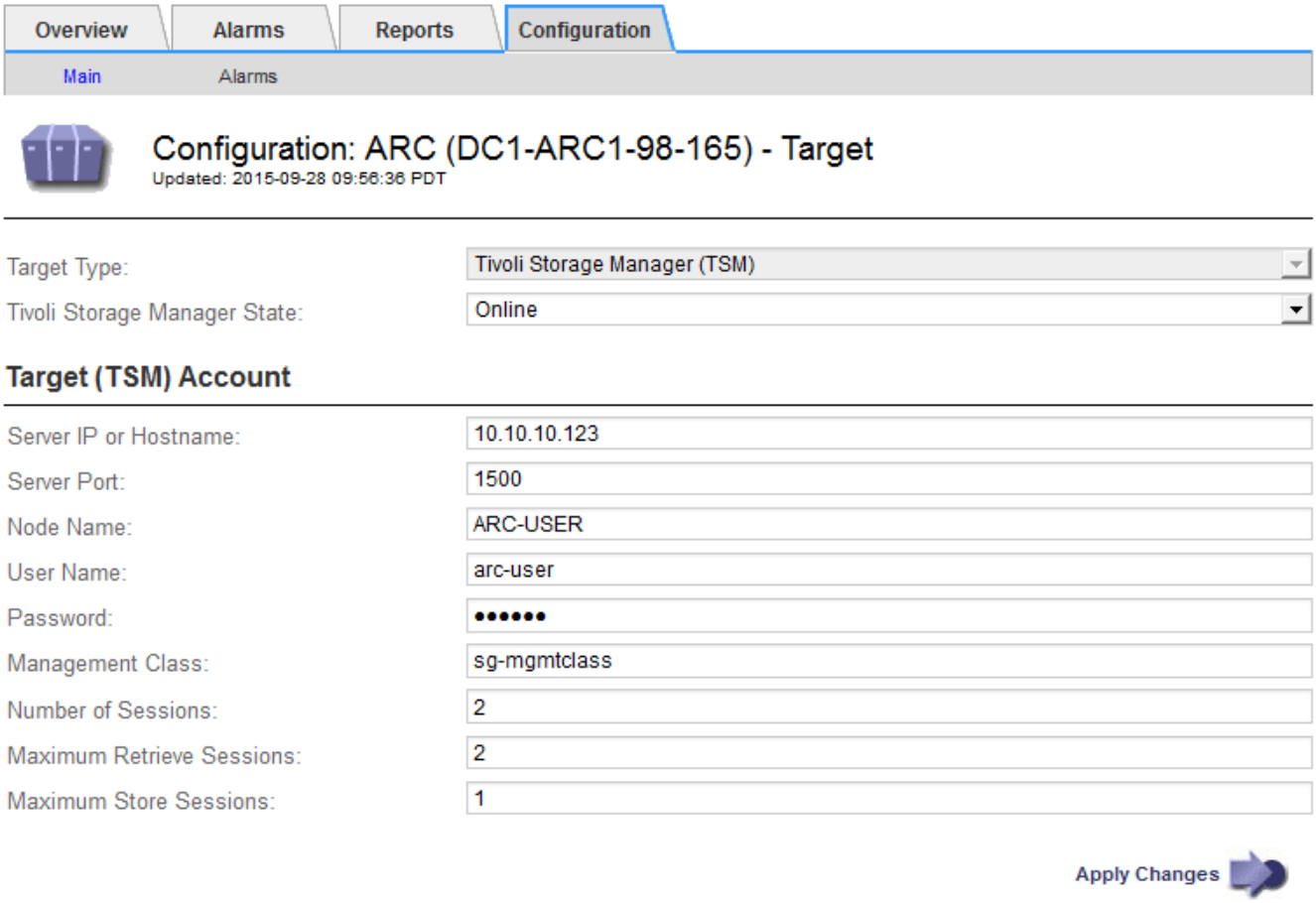
Sobre esta tarefa

Normalmente, o número de sessões simultâneas que o Archive Node tem aberto ao servidor middleware TSM é definido para o número de unidades de fita que o servidor TSM dedicou ao Archive Node. Uma unidade de fita é alocada para armazenamento enquanto o resto é alocado para recuperação. No entanto, em situações em que um nó de armazenamento está sendo reconstruído a partir de cópias do nó de arquivo ou o nó de arquivo está operando no modo somente leitura, você pode otimizar o desempenho do servidor TSM definindo o número máximo de sessões de recuperação para ser o mesmo que o número de sessões simultâneas. O resultado é que todas as unidades podem ser usadas simultaneamente para recuperação e, no máximo, uma dessas unidades também pode ser usada para armazenamento, se aplicável.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.

3. Selecione **Configuração** > **Principal**.
4. Altere **sessões de recuperação máxima** para ser o mesmo que **número de sessões**.



5. Clique em **aplicar alterações**.

Configurar o estado de arquivo e contadores para TSM

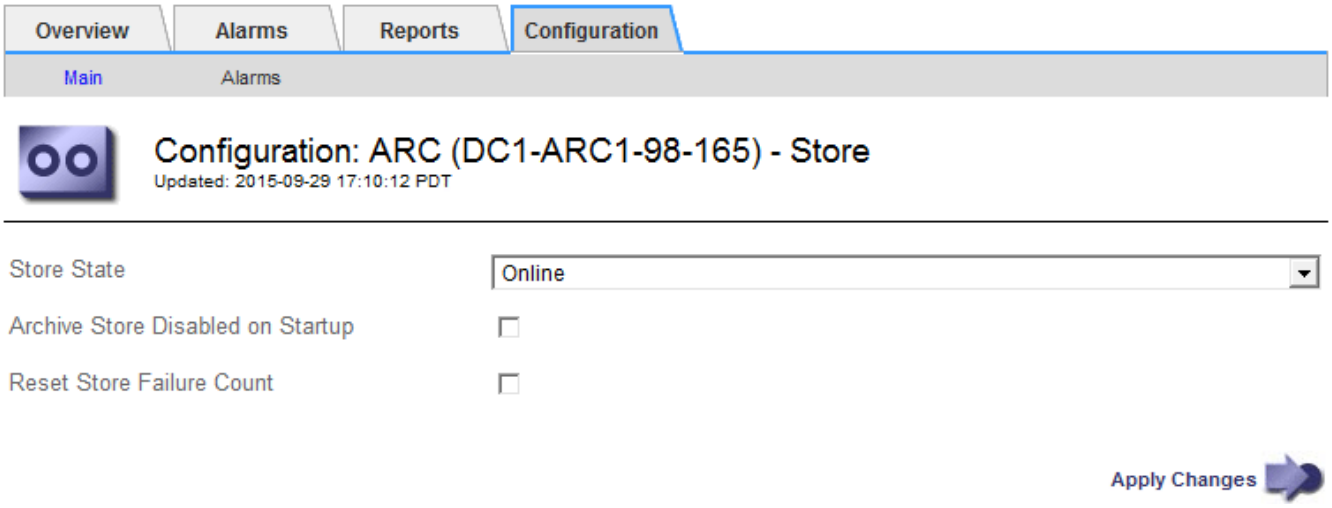
Se o seu Archive Node se conetar a um servidor middleware TSM, você poderá configurar o estado de armazenamento de arquivo de um Archive Node para Online ou Offline. Você também pode desativar o armazenamento de arquivos quando o nó de arquivo é iniciado pela primeira vez ou redefinir a contagem de falhas sendo rastreada para o alarme associado.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.



4. Modifique as seguintes definições, conforme necessário:
   - Estado da loja: Defina o estado do componente para:
     - On-line: O Archive Node está disponível para processar dados de objetos para armazenamento no sistema de armazenamento de arquivamento.
     - Offline: O nó de arquivo não está disponível para processar dados de objeto para armazenamento no sistema de armazenamento de arquivo.
   - Archive Store Disabled on Startup (armazenamento de arquivo desativado na inicialização): Quando selecionado, o componente Archive Store (armazenamento de arquivo) permanece no estado Read-Only (somente leitura) quando reiniciado. Usado para desativar persistentemente o armazenamento para o sistema de armazenamento de arquivo visado. Útil quando o sistema de armazenamento de arquivos visado não consegue aceitar conteúdo.
   - Repor contagem de falhas de armazenamento: Reponha o contador para falhas de armazenamento. Isso pode ser usado para limpar o alarme ARVF (falha de armazenamento).
5. Clique em **aplicar alterações**.

Informações relacionadas

"Gerenciando um nó de arquivo quando o servidor TSM atinge a capacidade"

Gerenciando um nó de arquivo quando o servidor TSM atinge a capacidade

O servidor TSM não tem como notificar o nó de arquivo quando o banco de dados TSM ou o armazenamento de Mídia de arquivamento gerenciado pelo servidor TSM estiver próximo da capacidade. O nó de arquivo continua a aceitar dados de objeto para transferência para o servidor TSM depois que o servidor TSM parar de aceitar novo conteúdo. Este conteúdo não pode ser gravado em Mídia gerenciada pelo servidor TSM. Um alarme é acionado se isso acontecer. Esta situação pode ser evitada através do monitoramento proativo do servidor TSM.

O que você vai precisar

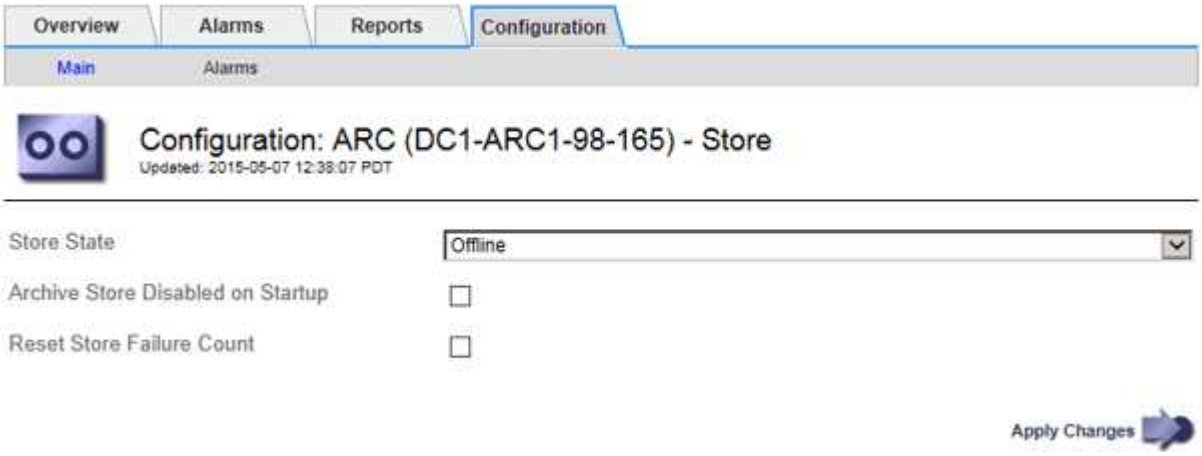
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Para evitar que o serviço ARC envie mais conteúdo para o servidor TSM, você pode colocar o nó de Arquivo offline, colocando o componente **ARC** > **Store** offline. Este procedimento também pode ser útil na prevenção de alarmes quando o servidor TSM não estiver disponível para manutenção.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.



4. Altere **Estado de armazenamento** para `Offline`.
5. Selecione **Archive Store Disabled on Startup**.
6. Clique em **aplicar alterações**.

Configurando o Archive Node para somente leitura se o middleware TSM atingir a capacidade

Se o servidor de middleware TSM visado atingir a capacidade, o nó de arquivo pode ser otimizado para executar apenas recuperações.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.
4. Altere as sessões de recuperação máxima para ser igual ao número de sessões simultâneas listadas em número de sessões.
5. Altere o máximo de sessões de armazenamento para 0.

> Não é necessário alterar o máximo de sessões de armazenamento para 0 se o nó de arquivo for apenas leitura. As sessões de armazenamento não serão criadas.

6. Clique em **aplicar alterações**.

Configurar as definições de recuperação do nó de arquivo

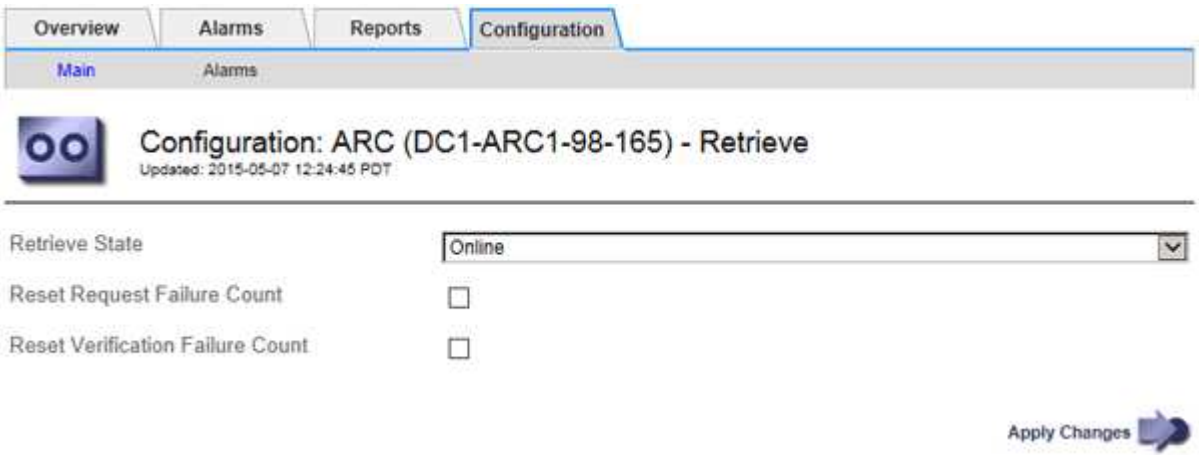
Você pode configurar as configurações de recuperação de um nó de arquivo para definir o estado como Online ou Offline, ou redefinir as contagens de falhas que estão sendo rastreadas para os alarmes associados.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione **Archive Node** > **ARC** > **Retrieve**.
3. Selecione **Configuração** > **Principal**.



4. Modifique as seguintes definições, conforme necessário:
   - **Retrieve State**: Defina o estado do componente para:
     - On-line: O nó de grade está disponível para recuperar dados de objeto do dispositivo de Mídia de arquivamento.
     - Offline: O nó de grade não está disponível para recuperar dados de objeto.
   - Reset Request Failures Count (Redefinir contagem de falhas de pedido): Selecione a caixa de verificação para repor o contador para falhas de pedido. Isso pode ser usado para limpar o alarme ARRF (falhas de solicitação).
   - Redefinir contagem de falhas de verificação: Marque a caixa de seleção para redefinir o contador para falhas de verificação em dados de objetos recuperados. Isso pode ser usado para limpar o alarme ARRV (falhas de verificação).
5. Clique em **aplicar alterações**.

Configurando a replicação do Archive Node

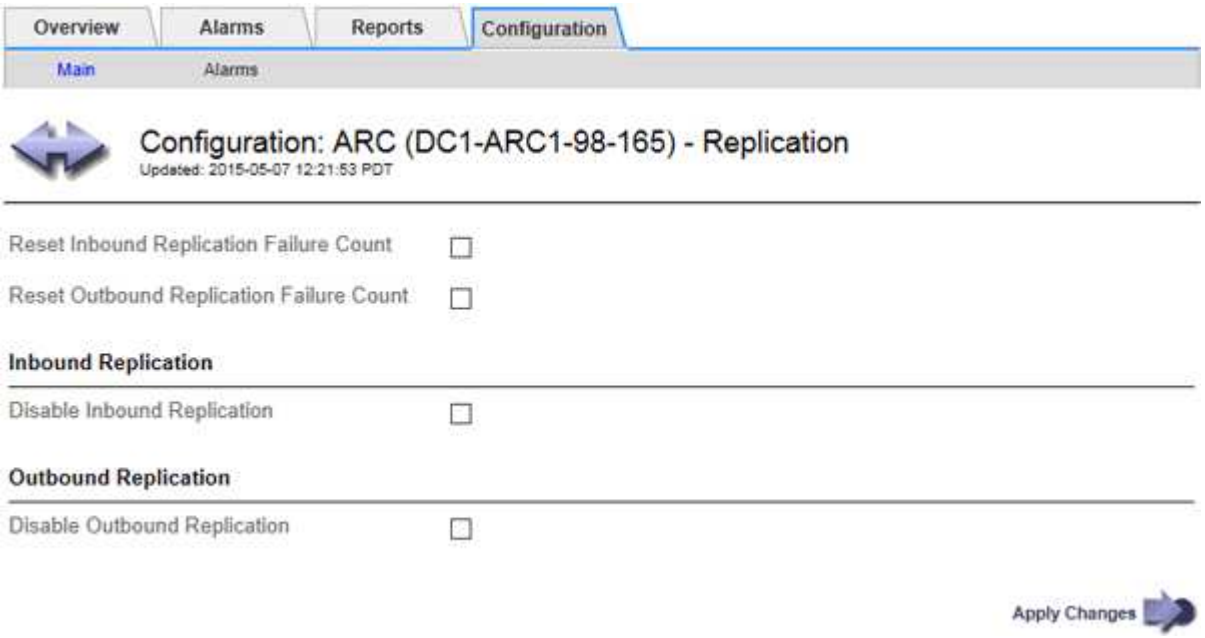
Você pode configurar as configurações de replicação para um nó de arquivo e desativar a replicação de entrada e saída ou redefinir as contagens de falha que estão sendo rastreadas para os alarmes associados.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Replication**.
3. Selecione **Configuração** > **Principal**.



4. Modifique as seguintes definições, conforme necessário:
   - **Redefinir contagem de falhas de replicação de entrada**: Selecione para redefinir o contador para falhas de replicação de entrada. Isso pode ser usado para limpar o alarme RIRF (replicações embutidas — Failed).
   - **Redefinir contagem de falhas de replicação de saída**: Selecione para redefinir o contador para falhas de replicação de saída. Isso pode ser usado para limpar o alarme RORF (Outbound replicações — Failed).
   - **Desativar replicação de entrada**: Selecione para desativar a replicação de entrada como parte de um procedimento de manutenção ou teste. Deixe limpo durante o funcionamento normal.

     Quando a replicação de entrada é desativada, os dados de objeto podem ser recuperados do serviço ARC para replicação para outros locais no sistema StorageGRID, mas os objetos não podem ser replicados para este serviço ARC a partir de outros locais do sistema. O serviço ARC é apenas de leitura.

   - **Desativar replicação de saída**: Marque a caixa de seleção para desativar a replicação de saída (incluindo solicitações de conteúdo para recuperações HTTP) como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal.

     Quando a replicação de saída é desativada, os dados de objeto podem ser copiados para este serviço ARC para satisfazer as regras ILM, mas os dados de objeto não podem ser recuperados do serviço ARC para serem copiados para outros locais no sistema StorageGRID. O serviço ARC é apenas de escrita.

5. Clique em **aplicar alterações**.

Definir alarmes personalizados para o nó de arquivo

Você deve estabelecer alarmes personalizados para os atributos ARQL e ARRL que são usados para monitorar a velocidade e eficiência da recuperação de dados de objetos do sistema de armazenamento de arquivos pelo nó Archive.

- ARQL: Comprimento médio da fila. O tempo médio, em microssegundos, em que os dados do objeto são enfileirados para recuperação do sistema de armazenamento de arquivamento.
- ARRL: Latência média da solicitação. O tempo médio, em microssegundos, necessário pelo nó de arquivo para recuperar dados de objetos do sistema de armazenamento de arquivamento.

Os valores aceitáveis para esses atributos dependem de como o sistema de armazenamento de arquivos é configurado e usado. (Vá para **ARC** > **Retrieve** > **Overview** > **Main**.) Os valores definidos para tempos limite de solicitação e o número de sessões disponibilizadas para solicitações de recuperação são particularmente influentes.

Depois que a integração estiver concluída, monitorize as recuperações de dados de objetos do nó de Arquivo para estabelecer valores para tempos de recuperação normais e comprimentos de fila. Em seguida, crie alarmes personalizados para ARQL e ARRL que serão acionados se surgir uma condição operacional anormal.

Informações relacionadas

"Monitorizar Resolução de problemas"

Integração do Tivoli Storage Manager

Esta seção inclui as melhores práticas e informações de configuração para integrar um nó de arquivo com um servidor Tivoli Storage Manager (TSM), incluindo detalhes operacionais do nó de arquivo que afetam a configuração do servidor TSM.

- "Configuração e operação do nó de arquivamento"
- "Práticas recomendadas de configuração"
- "Concluir a configuração do nó de arquivo"

Configuração e operação do nó de arquivamento

Seu sistema StorageGRID gerencia o nó de arquivo como um local onde os objetos são armazenados indefinidamente e são sempre acessíveis.

Quando um objeto é ingerido, cópias são feitas em todos os locais necessários, incluindo nós de arquivo, com base nas regras de gerenciamento do ciclo de vida da informação (ILM) definidas para o seu sistema StorageGRID. O nó de arquivo atua como um cliente para um servidor TSM, e as bibliotecas de cliente TSM são instaladas no nó de arquivo pelo processo de instalação do software StorageGRID. Os dados do objeto direcionados para o nó de arquivo para armazenamento são salvos diretamente no servidor TSM à medida que são recebidos. O nó de arquivo não armazena os dados do objeto antes de salvá-los no servidor TSM, nem realiza agregação de objetos. No entanto, o nó de arquivo pode enviar várias cópias para o servidor TSM em uma única transação quando as taxas de dados são garantidas.

Depois que o nó de arquivo salva os dados do objeto no servidor TSM, os dados do objeto são gerenciados

pelo servidor TSM usando suas políticas de ciclo de vida/retenção. Essas políticas de retenção devem ser definidas para serem compatíveis com a operação do nó de arquivo. Ou seja, os dados de objeto salvos pelo nó de arquivo devem ser armazenados indefinidamente e devem sempre ser acessíveis pelo nó de arquivo, a menos que sejam excluídos pelo nó de arquivo.

Não há conexão entre as regras de ILM do sistema StorageGRID e as políticas de ciclo de vida/retenção do servidor TSM. Cada um opera independentemente do outro; no entanto, à medida que cada objeto é ingerido no sistema StorageGRID, você pode atribuir a ele uma classe de gerenciamento TSM. Essa classe de gerenciamento é passada para o servidor TSM junto com os dados do objeto. A atribuição de diferentes classes de gerenciamento a diferentes tipos de objetos permite configurar o servidor TSM para colocar dados de objetos em diferentes pools de armazenamento ou aplicar diferentes políticas de migração ou retenção, conforme necessário. Por exemplo, os objetos identificados como backups de banco de dados (conteúdo temporário que pode ser substituído por dados mais recentes) podem ser tratados de forma diferente dos dados da aplicação (conteúdo fixo que deve ser mantido indefinidamente).

O nó de arquivo pode ser integrado a um servidor TSM novo ou existente; ele não requer um servidor TSM dedicado. Os servidores TSM podem ser compartilhados com outros clientes, desde que o servidor TSM seja dimensionado adequadamente para a carga máxima esperada. O TSM deve ser instalado em um servidor ou máquina virtual separado do nó de arquivo.

É possível configurar mais de um nó de arquivo para gravar no mesmo servidor TSM; no entanto, esta configuração só é recomendada se os nós de arquivo gravarem conjuntos diferentes de dados no servidor TSM. A configuração de mais de um nó de arquivo para gravação no mesmo servidor TSM não é recomendada quando cada nó de arquivo grava cópias dos mesmos dados de objeto no arquivo. No último cenário, ambas as cópias estão sujeitas a um único ponto de falha (o servidor TSM) para o que é suposto ser cópias independentes e redundantes de dados de objeto.

Os nós de arquivamento não fazem uso do componente HSM (Hierarchical Storage Management) do TSM.

Práticas recomendadas de configuração

Quando você está dimensionando e configurando seu servidor TSM, existem práticas recomendadas que você deve aplicar para otimizá-lo para trabalhar com o nó de Arquivo.

Ao dimensionar e configurar o servidor TSM, você deve considerar os seguintes fatores:

- Como o nó de arquivo não agrega objetos antes de salvá-los no servidor TSM, o banco de dados TSM deve ser dimensionado para conter referências a todos os objetos que serão gravados no nó de arquivo.
- O software Archive Node não pode tolerar a latência envolvida na gravação de objetos diretamente na fita ou em outra Mídia removível. Portanto, o servidor TSM deve ser configurado com um pool de armazenamento de disco para o armazenamento inicial de dados salvos pelo nó de arquivo sempre que Mídia removível for usada.
- Você deve configurar políticas de retenção de TSM para usar a retenção baseada em eventos. O nó de arquivo não suporta políticas de retenção de TSM baseadas na criação. Use as seguintes configurações recomendadas de retmin.0 e retver.0 na política de retenção (que indica que a retenção começa quando o nó de arquivamento aciona um evento de retenção e é mantido por 0 dias depois disso). No entanto, esses valores para retmin e retver são opcionais.

O pool de discos deve ser configurado para migrar dados para o pool de fitas (ou seja, o pool de fitas deve ser o NXTSTGPOOL do pool de discos). O pool de fitas não deve ser configurado como um pool de cópias do pool de discos com gravação simultânea em ambos os pools (ou seja, o pool de fitas não pode ser um COPYSTGPOOL para o pool de discos). Para criar cópias off-line das fitas que contêm dados do Archive Node, configure o servidor TSM com um segundo pool de fitas que é um pool de cópias do pool de fitas usado

para dados do Archive Node.

Concluir a configuração do nó de arquivo

O nó de arquivo não funciona depois de concluir o processo de instalação. Antes que o sistema StorageGRID possa salvar objetos no nó de arquivo TSM, você deve concluir a instalação e configuração do servidor TSM e configurar o nó de arquivo para se comunicar com o servidor TSM.

Para obter mais informações sobre como otimizar as sessões de recuperação e armazenamento do TSM, consulte informações sobre como gerenciar o armazenamento de arquivos.

- "Gerenciando nós de arquivamento"

Consulte a seguinte documentação da IBM, conforme necessário, enquanto prepara o servidor TSM para integração com o nó de arquivo em um sistema StorageGRID:

- "Guia de instalação e do usuário dos drivers de dispositivo de fita IBM"
- "Referência de programação de drivers de dispositivo de fita IBM"

Instalar um novo servidor TSM

Você pode integrar o nó de arquivo a um servidor TSM novo ou existente. Se você estiver instalando um novo servidor TSM, siga as instruções na documentação do TSM para concluir a instalação.

> Um nó de arquivo não pode ser co-hospedado com um servidor TSM.

Configurando o servidor TSM

Esta seção inclui instruções de exemplo para preparar um servidor TSM seguindo as práticas recomendadas do TSM.

As instruções a seguir o orientam durante o processo de:

- Definir um pool de armazenamento em disco e um pool de armazenamento em fita (se necessário) no servidor TSM
- Definir uma política de domínio que utilize a classe de gestão TSM para os dados guardados a partir do nó de arquivo e registar um nó para utilizar esta política de domínio

Estas instruções são fornecidas apenas para a sua orientação; não se destinam a substituir a documentação do TSM ou a fornecer instruções completas e abrangentes adequadas para todas as configurações. Instruções específicas de implantação devem ser fornecidas por um administrador do TSM que esteja familiarizado com seus requisitos detalhados e com o conjunto completo de documentação do TSM Server.

Definição de conjuntos de armazenamento em disco e fita TSM

O nó de arquivamento grava em um pool de armazenamento em disco. Para arquivar conteúdo em fita, você deve configurar o pool de armazenamento em disco para mover o conteúdo para um pool de armazenamento em fita.

Sobre esta tarefa

Para um servidor TSM, você deve definir um pool de armazenamento em fita e um pool de armazenamento em disco no Tivoli Storage Manager. Depois que o pool de discos for definido, crie um volume de disco e atribua-o ao pool de discos. Não é necessário um pool de fitas se o servidor TSM usar storage somente em disco.

Você deve concluir várias etapas em seu servidor TSM antes de criar um pool de armazenamento de fita. (Crie uma biblioteca de fitas e pelo menos uma unidade na biblioteca de fitas. Defina um caminho do servidor para a biblioteca e do servidor para as unidades e, em seguida, defina uma classe de dispositivo para as unidades.) Os detalhes dessas etapas podem variar dependendo da configuração de hardware e dos requisitos de armazenamento do site. Para obter mais informações, consulte a documentação do TSM.

O seguinte conjunto de instruções ilustra o processo. Você deve estar ciente de que os requisitos para o seu site podem ser diferentes, dependendo dos requisitos da sua implantação. Para obter detalhes de configuração e instruções, consulte a documentação do TSM.

Você deve fazer logon no servidor com Privileges administrativo e usar a ferramenta dsmadmc para executar os seguintes comandos.

Passos

1. Crie uma biblioteca de fitas.

   `define library tapelibrary libtype=scsi`

   `_tapelibrary_`Onde é escolhido um nome arbitrário para a biblioteca de fitas, e o valor de `libtype` pode variar dependendo do tipo de biblioteca de fitas.

2. Defina um caminho do servidor para a biblioteca de fitas.

   `define path servername tapelibrary srctype=server desttype=library device=lib-devicename`

   - *servername* É o nome do servidor TSM
   - *tapelibrary* é o nome da biblioteca de fitas que você definiu
   - *lib-devicename* é o nome do dispositivo para a biblioteca de fitas

3. Defina uma unidade para a biblioteca.

   `define drive tapelibrary drivename`

   - *drivename* é o nome que você deseja especificar para a unidade
   - *tapelibrary* é o nome da biblioteca de fitas que você definiu

     Você pode querer configurar uma unidade ou unidades adicionais, dependendo da configuração do hardware. (Por exemplo, se o servidor TSM estiver conetado a um switch Fibre Channel que tenha duas entradas de uma biblioteca de fitas, talvez você queira definir uma unidade para cada entrada.)

4. Defina um caminho do servidor para a unidade definida.

```
define path servername drivename srctype=server desttype=drive
library=tapelibrary device=drive-dname
```

- *drive-dname* é o nome do dispositivo para a unidade
- *tapelibrary* é o nome da biblioteca de fitas que você definiu

  Repita para cada unidade definida para a biblioteca de fitas, usando uma unidade *drivename* separada e *drive-dname* para cada unidade.

5. Defina uma classe de dispositivo para as unidades.

```
define devclass DeviceClassName devtype=lto library=tapelibrary
format=tapetype
```

- *DeviceClassName* é o nome da classe de dispositivo
- *lto* é o tipo de unidade conetada ao servidor
- *tapelibrary* é o nome da biblioteca de fitas que você definiu
- *tapetype* é o tipo de fita; por exemplo, ultrium3

6. Adicione volumes de fita ao inventário da biblioteca.

```
checkin libvolume tapelibrary
```

tapelibrary é o nome da biblioteca de fitas que você definiu.

7. Crie o pool de armazenamento de fita primário.

```
define stgpool SGWSTapePool DeviceClassName description=description
collocate=filespace maxscratch=XX
```

- *SGWSTapePool* É o nome do conjunto de armazenamento de fita do nó de arquivo. Você pode selecionar qualquer nome para o pool de armazenamento de fita (desde que o nome use as convenções de sintaxe esperadas pelo servidor TSM).
- *DeviceClassName* é o nome do nome da classe do dispositivo para a biblioteca de fitas.
- *description* É uma descrição do pool de armazenamento que pode ser exibido no servidor TSM usando o `query stgpool` comando. Por exemplo: "'conjunto de armazenamento de fita para o nó de arquivo.'"
- *collocate=filespace* Especifica que o servidor TSM deve gravar objetos do mesmo espaço de arquivo em uma única fita.
- `XX` é um dos seguintes:
  - O número de fitas vazias na biblioteca de fitas (caso o nó de arquivo seja o único aplicativo que usa a biblioteca).
  - O número de fitas alocadas para uso pelo sistema StorageGRID (nos casos em que a biblioteca de fitas é compartilhada).

8. Em um servidor TSM, crie um pool de armazenamento em disco. Na consola administrativa do servidor TSM, introduza

```
define stgpool SGWSDiskPool disk description=description
```

`maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high lowmig=percent_low`

- *SGWSDiskPool* É o nome do conjunto de discos do nó de arquivo. Você pode selecionar qualquer nome para o pool de armazenamento em disco (desde que o nome use as convenções de sintaxe esperadas pelo TSM).
- *description* É uma descrição do pool de armazenamento que pode ser exibido no servidor TSM usando o `query stgpool` comando. Por exemplo, ""conjunto de armazenamento em disco para o nó de arquivo".
- *maximum_file_size* força objetos maiores do que esse tamanho a serem gravados diretamente na fita, em vez de serem armazenados em cache no pool de discos. Recomenda-se definir *maximum_file_size* para 10 GB.
- *nextstgpool=SGWSTapePool* Refere o pool de armazenamento em disco ao pool de armazenamento em fita definido para o nó de arquivo.
- *percent_high* define o valor no qual o pool de discos começa a migrar seu conteúdo para o pool de fitas. Recomenda-se definir *percent_high* como 0 para que a migração de dados comece imediatamente
- *percent_low* define o valor no qual a migração para o conjunto de fitas pára. Recomenda-se definir *percent_low* como 0 para limpar o pool de discos.

9. Em um servidor TSM, crie um volume de disco (ou volumes) e atribua-o ao pool de discos.

   `define volume SGWSDiskPool volume_name formatsize=size`

   - *SGWSDiskPool* é o nome do pool de discos.
   - *volume_name* É o caminho completo para o local do volume (por exemplo, `/var/local/arc/stage6.dsm`) no servidor TSM onde grava o conteúdo do pool de discos em preparação para transferência para fita.
   - *size* É o tamanho, em MB, do volume do disco.

     Por exemplo, para criar um único volume de disco de modo que o conteúdo de um pool de discos preencha uma única fita, defina o valor de tamanho como 200000 quando o volume da fita tiver uma capacidade de 200 GB.

     No entanto, pode ser desejável criar vários volumes de disco de um tamanho menor, já que o servidor TSM pode gravar em cada volume no pool de discos. Por exemplo, se o tamanho da fita for de 250 GB, crie 25 volumes de disco com um tamanho de 10 GB (10000) cada.

   O servidor TSM prealoca espaço no diretório para o volume de disco. Isso pode levar algum tempo para ser concluído (mais de três horas para um volume de disco de 200 GB).

Definir uma política de domínio e registar um nó

Você precisa definir uma política de domínio que use a classe de gerenciamento TSM para os dados salvos do nó de arquivamento e, em seguida, Registrar um nó para usar essa diretiva de domínio.

Os processos do nó de arquivamento podem vazar memória se a senha do cliente para o nó de arquivamento no Tivoli Storage Manager (TSM) expirar. Certifique-se de que o servidor TSM está configurado para que o nome de utilizador/palavra-passe do cliente para o nó de arquivo nunca expire.

Ao Registrar um nó no servidor TSM para o uso do nó de arquivo (ou atualizar um nó existente), você deve especificar o número de pontos de montagem que o nó pode usar para operações de gravação especificando o parâmetro MAXNUMMP para o comando DE NÓ DE REGISTRO. O número de pontos de montagem é normalmente equivalente ao número de cabeças de unidade de fita alocadas ao nó de arquivo. O número especificado para MAXNUMMP no servidor TSM deve ser pelo menos tão grande quanto o valor definido para **ARC** > **Target** > **Configuration** > **Main** > **Maximum Store Sessions** para o Archive Node, que é definido para um valor de 0 ou 1, já que as sessões de armazenamento simultâneas não são suportadas pelo Archive Node.

O valor de MAXSESSIONS definido para o servidor TSM controla o número máximo de sessões que podem ser abertas para o servidor TSM por todos os aplicativos clientes. O valor de MAXSESSIONS especificado no TSM deve ser pelo menos tão grande quanto o valor especificado para **ARC** > **Target** > **Configuration** > **Main** > **Number of Sessions** no Grid Manager para o Archive Node. O nó de arquivo cria simultaneamente, no máximo, uma sessão por ponto de montagem, mais um pequeno número (inferior a 5) de sessões adicionais.

O nó TSM atribuído ao nó de arquivo usa uma política de domínio personalizada `tsm-domain` . A `tsm-domain` política de domínio é uma versão modificada da política de domínio "sandard", configurada para gravar em fita e com o destino do arquivo definido como o pool de armazenamento do sistema StorageGRID (*`SGWSDiskPool`*).

Você deve fazer login no servidor TSM com Privileges administrativo e usar a ferramenta dsmadmc para criar e ativar a diretiva de domínio.

Criando e ativando a política de domínio

Você deve criar uma política de domínio e ativá-la para configurar o servidor TSM para salvar os dados enviados do nó de Arquivo.

Passos

1. Crie uma política de domínio.

   ```
   copy domain standard tsm-domain
   ```

2. Se você não estiver usando uma classe de gerenciamento existente, insira uma das seguintes opções:

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` é a classe de gerenciamento padrão para a implantação.

3. Crie um copygroup para o pool de armazenamento apropriado. Introduza (numa linha):

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

default É a classe de gerenciamento padrão para o nó de arquivo. Os valores de `retinit`, `retmin` e `retver` foram escolhidos para refletir o comportamento de retenção atualmente utilizado pelo nó de arquivo

> Não defina `retinit` para `retinit=create`. A configuração `retinit=create` impede que o nó de arquivo exclua conteúdo, uma vez que os eventos de retenção são usados para remover conteúdo do servidor TSM.

4. Atribua a classe de gerenciamento como padrão.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Defina o novo conjunto de políticas como ativo.

   ```
   activate policyset tsm-domain standard
   ```

   Ignore o aviso "'no backup copy group'" que aparece quando você digita o comando Activate.

6. Registre um nó para usar o novo conjunto de políticas no servidor TSM. No servidor TSM, introduza (numa linha):

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   ARC-user e ARC-password são o mesmo nome de nó de cliente e palavra-passe definidos no nó de arquivo, e o valor de MAXNUMMP é definido para o número de unidades de fita reservadas para sessões de armazenamento de nó de arquivo.

> Por padrão, o Registro de um nó cria uma ID de usuário administrativo com autoridade de proprietário do cliente, com a senha definida para o nó.

Migração de dados para o StorageGRID

É possível migrar grandes quantidades de dados para o sistema StorageGRID e, simultaneamente, usar o sistema StorageGRID para operações diárias.

A seção a seguir é um guia para entender e Planejar uma migração de grandes quantidades de dados para o sistema StorageGRID. Ele não é um guia geral para a migração de dados e não inclui etapas detalhadas para a execução de uma migração. Siga as diretrizes e instruções nesta seção para garantir que os dados sejam migrados com eficiência para o sistema StorageGRID sem interferir nas operações diárias e que os dados migrados sejam tratados adequadamente pelo sistema StorageGRID.

- "Confirmar a capacidade do sistema StorageGRID"
- "Determinando a política de ILM para dados migrados"
- "Impacto da migração nas operações"
- "Agendamento da migração de dados"
- "Monitoramento da migração de dados"
- "Criação de notificações personalizadas para alarmes de migração"

Confirmar a capacidade do sistema StorageGRID

Antes de migrar grandes quantidades de dados para o sistema StorageGRID, confirme se o sistema StorageGRID tem a capacidade de disco para lidar com o volume esperado.

Se o sistema StorageGRID incluir um nó de arquivo e uma cópia de objetos migrados tiver sido salva no armazenamento de dados nearline (como fita), verifique se o armazenamento do nó de arquivamento tem capacidade suficiente para o volume esperado de dados migrados.

Como parte da avaliação de capacidade, observe o perfil de dados dos objetos que você planeja migrar e calcule a quantidade de capacidade de disco necessária. Para obter detalhes sobre como monitorar a capacidade de disco do seu sistema StorageGRID, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Gerenciando nós de storage"

Determinando a política de ILM para dados migrados

A política ILM do sistema StorageGRID determina quantas cópias são feitas, os locais para os quais as cópias são armazenadas e por quanto tempo essas cópias são mantidas. Uma política ILM consiste em um conjunto de regras ILM que descrevem como filtrar objetos e gerenciar dados de objetos ao longo do tempo.

Dependendo de como os dados migrados são usados e de seus requisitos de dados migrados, talvez você queira definir regras exclusivas de ILM para dados migrados que são diferentes das regras de ILM usadas para operações diárias. Por exemplo, se houver requisitos regulatórios diferentes para o gerenciamento diário de dados do que os dados incluídos na migração, talvez você queira um número diferente de cópias dos dados migrados em um nível diferente de storage.

Você pode configurar regras que se aplicam exclusivamente aos dados migrados se for possível distinguir de forma exclusiva entre dados migrados e dados de objetos salvos de operações diárias.

Se você puder distinguir de forma confiável entre os tipos de dados usando um dos critérios de metadados, use esses critérios para definir uma regra de ILM que se aplica apenas aos dados migrados.

Antes de iniciar a migração de dados, certifique-se de que compreende a política de ILM do sistema StorageGRID e de que forma será aplicada aos dados migrados e de que fez e testou quaisquer alterações à política ILM.

Uma política de ILM que foi incorretamente especificada pode causar perda de dados irrecuperável. Revise cuidadosamente todas as alterações feitas em uma política ILM antes de ativá-la para garantir que a política funcionará conforme pretendido.

Informações relacionadas

"Gerenciar objetos com ILM"

Impacto da migração nas operações

O sistema StorageGRID foi desenvolvido para fornecer operações eficientes de storage e recuperação de objetos, além de fornecer excelente proteção contra a perda de dados por meio da criação otimizada de cópias redundantes de dados de objetos e metadados.

No entanto, a migração de dados deve ser cuidadosamente gerenciada de acordo com as instruções deste capítulo para evitar ter impactos nas operações diárias do sistema ou, em casos extremos, colocar os dados em risco de perda em caso de falha no sistema StorageGRID.

A migração de grandes quantidades de dados coloca carga adicional no sistema. Quando o sistema StorageGRID está muito carregado, ele responde mais lentamente às solicitações para armazenar e recuperar objetos. Isso pode interferir com as solicitações de armazenamento e recuperação que são parte integrante das operações diárias. A migração também pode causar outros problemas operacionais. Por exemplo, quando um nó de armazenamento está próximo da capacidade, a carga intermitente pesada devido à ingestão de lote pode fazer com que o nó de armazenamento alterne entre somente leitura e leitura-gravação, gerando notificações.

Se o carregamento pesado persistir, as filas podem se desenvolver para várias operações que o sistema StorageGRID deve executar para garantir a redundância total dos dados e metadados do objeto.

A migração de dados deve ser cuidadosamente gerenciada de acordo com as diretrizes deste documento para garantir o funcionamento seguro e eficiente do sistema StorageGRID durante a migração. Ao migrar dados, ingira objetos em lotes ou controle continuamente a ingestão. Em seguida, monitore continuamente o sistema StorageGRID para garantir que vários valores de atributo não sejam excedidos.

Agendamento da migração de dados

Evite migrar dados durante o horário operacional principal. Limite a migração de dados para noites, fins de semana e outras ocasiões em que o uso do sistema é baixo.

Se possível, não programe a migração de dados durante períodos de alta atividade. No entanto, se não for prático evitar completamente o período de atividade elevada, é seguro prosseguir desde que monitorize de perto os atributos relevantes e tome medidas se excederem os valores aceitáveis.

Informações relacionadas

"Monitoramento da migração de dados"

Monitoramento da migração de dados

A migração de dados deve ser monitorada e ajustada conforme necessário para garantir que os dados sejam colocados de acordo com a política de ILM dentro do prazo exigido.

Esta tabela lista os atributos que você deve monitorar durante a migração de dados e os problemas que eles representam.

Se você usar políticas de classificação de tráfego com limites de taxa para reduzir a ingestão, poderá monitorar a taxa observada em conjunto com as estatísticas descritas na tabela a seguir e reduzir os limites, se necessário.

Monitorar	Descrição
Número de objetos aguardando avaliação ILM	1. Selecione **Support** > **Tools** > **Grid Topology**. 2. Selecione ***deployment*** > **Overview** > **Main**. 3. Na seção ILM Activity, monitore o número de objetos mostrados para os seguintes atributos: ◦ **Aguardando - todos (XQUZ)**: O número total de objetos aguardando avaliação ILM. ◦ **Aguardando - Cliente (XCQZ)**: O número total de objetos aguardando avaliação ILM das operações do cliente (por exemplo, ingest). 4. Se o número de objetos mostrados para qualquer um desses atributos exceder 100.000, diminua a taxa de ingestão de objetos para reduzir a carga no sistema StorageGRID.
Capacidade de armazenamento do sistema de arquivamento direcionado	Se a política de ILM salvar uma cópia dos dados migrados para um sistema de armazenamento de arquivamento de destino (fita ou nuvem), monitore a capacidade do sistema de armazenamento de arquivamento de destino para garantir que haja capacidade suficiente para os dados migrados.
Archive Node > **ARC** > **Store**	Se um alarme para o atributo **Store Failures (ARVF)** for acionado, o sistema de armazenamento de arquivos alvo pode ter atingido a capacidade. Verifique o sistema de armazenamento de arquivos alvo e resolva quaisquer problemas que acionaram um alarme.

Criação de notificações personalizadas para alarmes de migração

Você pode querer que o StorageGRID envie notificações de alerta ou notificações de alarme (sistema legado) para o administrador do sistema responsável pelo monitoramento da migração se certos valores excederem os limites recomendados.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter configurado configurações de e-mail para notificações de alerta (ou alarme).

Passos

1. Crie uma regra de alerta personalizada ou um alarme personalizado global para cada métrica ou atributo StorageGRID do Prometheus que você deseja monitorar durante a migração de dados.

   Os alertas são acionados com base nos valores métricos Prometheus. Os alarmes são acionados com base em valores de atributo. Consulte as instruções para monitoramento e solução de problemas do StorageGRID para obter mais informações.

2. Desative a regra de alerta personalizado ou o alarme personalizado global após a conclusão da migração de dados.

Observe que os alarmes personalizados globais substituem os alarmes padrão.

Informações relacionadas

"Monitorizar Resolução de problemas"

Gerenciar objetos com ILM

Saiba como gerenciar objetos com regras e políticas de ciclo de vida das informações e como usar o bloqueio de objetos do S3 para cumprir com os regulamentos de retenção de objetos.

- "Gerenciamento de objetos com gerenciamento do ciclo de vida das informações"
- "Gerenciando objetos com o S3 Object Lock"
- "Exemplo de regras e políticas ILM"

Gerenciamento de objetos com gerenciamento do ciclo de vida das informações

Você gerencia os objetos em um sistema StorageGRID configurando regras e políticas de gerenciamento do ciclo de vida das informações (ILM). As regras e políticas do ILM instruem o StorageGRID a criar e distribuir cópias de dados de objetos e como gerenciar essas cópias ao longo do tempo.

Projetar e implementar regras de ILM e a política 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.

- "Como o ILM opera ao longo da vida de um objeto"
- "O que é uma política ILM"
- "O que é uma regra ILM"
- "Criação de categorias de storage, pools de storage, perfis de EC e regiões"
- "Criando uma regra ILM"
- "Criando uma política ILM"
- "Trabalhando com regras de ILM e políticas de ILM"

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**: O ingest começa quando um aplicativo cliente S3 ou Swift estabelece uma conexão para salvar um objeto no sistema StorageGRID, e é concluído quando o StorageGRID retorna uma mensagem "ingest successful" ao 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

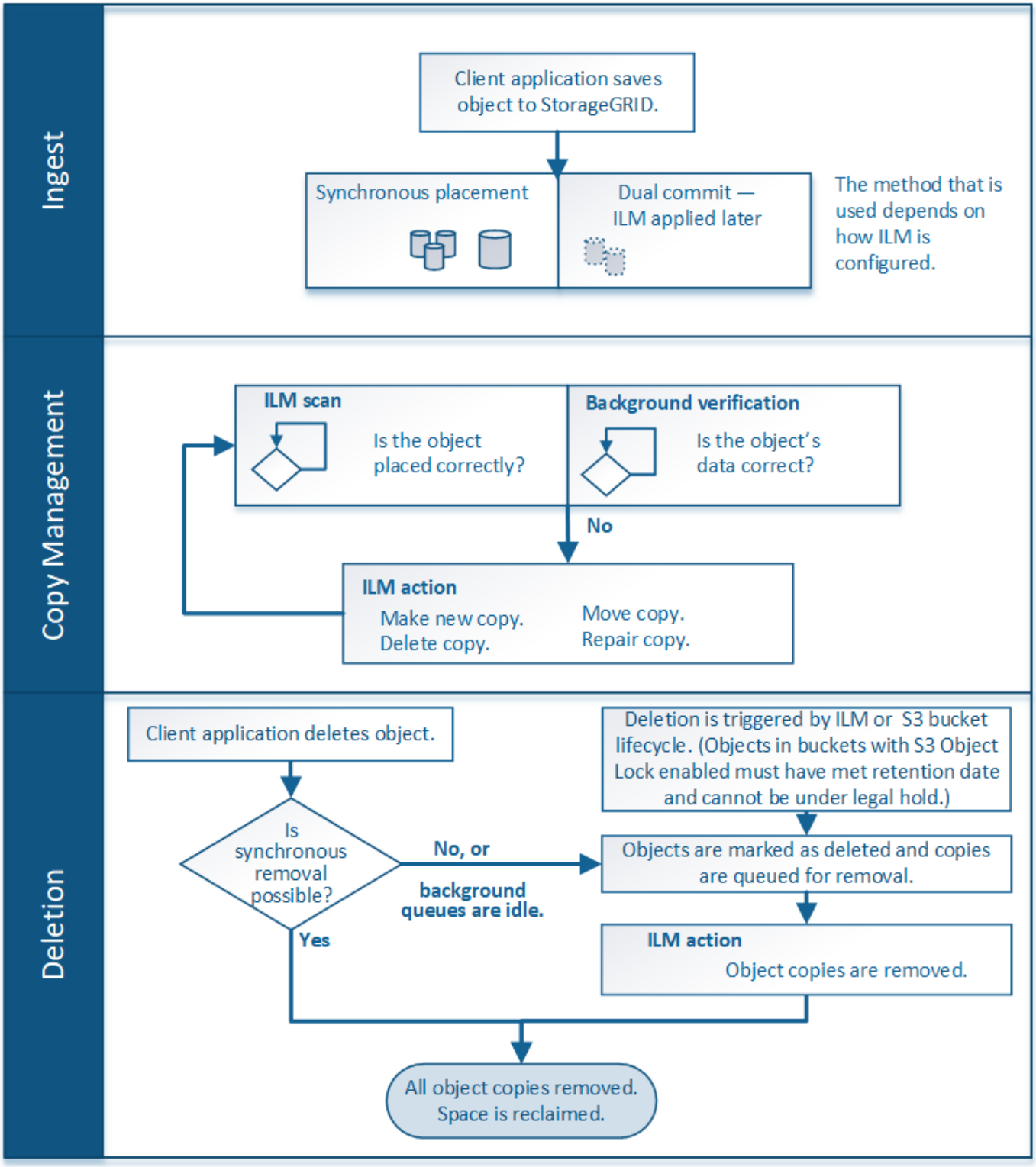
perda.

  - 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. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

- **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.



Informações relacionadas

"Monitorizar Resolução de problemas"

Como os objetos são ingeridos

O StorageGRID protege os objetos durante a ingestão, executando o posicionamento síncrono ou executando commit duplo, conforme especificado na regra ILM que corresponde aos objetos.

Quando um cliente S3 ou Swift armazena um objeto na grade, o StorageGRID ingere o objeto usando um destes dois métodos:

- **Colocação síncrona**: O StorageGRID cria imediatamente todas as cópias de objetos necessárias para atender aos requisitos do ILM. O StorageGRID envia uma mensagem de "ingestão bem-sucedida" ao cliente quando todas as cópias são criadas.

  Se o StorageGRID não puder criar imediatamente todas as cópias de objeto (por exemplo, porque um local necessário está temporariamente indisponível), ele enviará uma mensagem "'ingest failed'" para o cliente, ou se recairá a criar cópias de objeto provisórias e avaliar o ILM mais tarde, dependendo da escolha feita quando você criou a regra ILM.

- * Commit duplo*: O StorageGRID cria imediatamente duas cópias provisórias do objeto, cada uma em um nó de armazenamento diferente, e envia uma mensagem "'ingest successful'" ao cliente. O StorageGRID então coloca o objeto em fila para avaliação do ILM.

  Quando o StorageGRID executa a avaliação ILM, ele primeiro verifica se as cópias provisórias satisfazem as instruções de colocação na regra ILM. Por exemplo, as duas cópias provisórias podem satisfazer as instruções em uma regra ILM de duas cópias, mas elas não satisfazem as instruções em uma regra de codificação de apagamento. Se as cópias provisórias não satisfizerem as instruções do ILM, o StorageGRID criará novas cópias de objeto e excluirá quaisquer cópias provisórias que não sejam necessárias.

  Se o StorageGRID não puder criar duas cópias provisórias (por exemplo, se um problema de rede impedir que a segunda cópia seja feita), o StorageGRID não tentará novamente. A ingestão falha.

> Os clientes S3 ou Swift podem especificar que o StorageGRID crie uma única cópia provisória na ingestão especificando `REDUCED_REDUNDANCY` para a classe de armazenamento. Consulte as instruções para implementar um cliente S3 ou Swift para obter mais informações.

Por padrão, o StorageGRID usa o posicionamento síncrono para proteger objetos durante a ingestão.

Informações relacionadas

"Opções de proteção de dados para ingestão"

"Use S3"

"Use Swift"

Opções de proteção de dados para ingestão

Ao criar uma regra ILM, você especifica uma das três opções para proteger objetos na ingestão: Commit duplo, balanceado ou rigoroso. 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.

Commit duplo

Quando você seleciona a opção de confirmação dupla, o StorageGRID imediatamente faz cópias provisórias de objeto em dois nós de armazenamento diferentes e retorna uma mensagem de ""ingestão bem-sucedida""

para o cliente. O objeto é colocado em fila para avaliação ILM e cópias que atendem às instruções de colocação da regra são feitas posteriormente.

Quando usar a opção de confirmação dupla

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 dual 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.

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.

Quando usar a opção estrita

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 determinado data center.

"Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"

Equilibrado

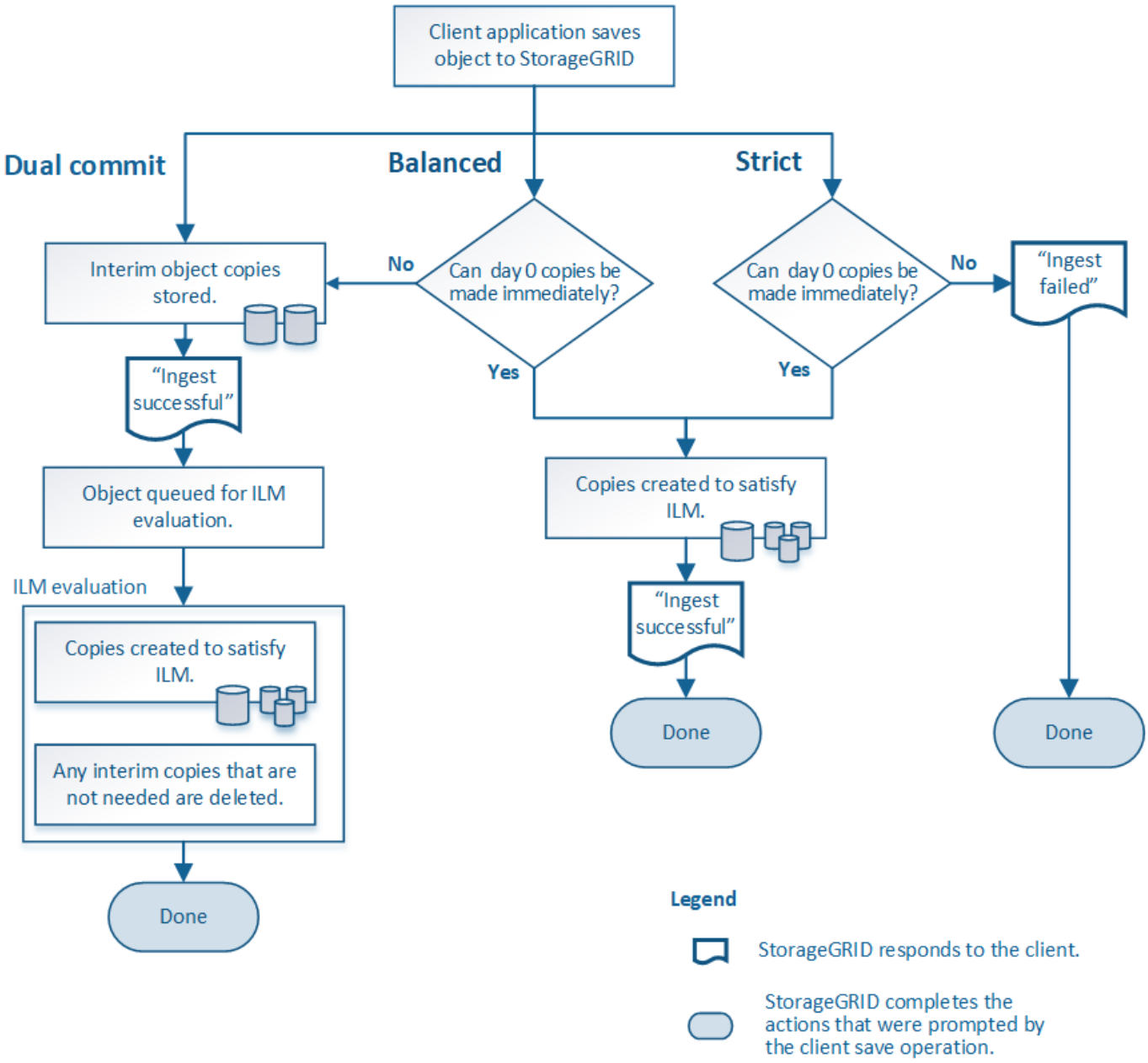
Quando você seleciona a opção equilibrada, o StorageGRID também usa o posicionamento síncrono na ingestão e faz imediatamente todas as cópias especificadas nas instruções de posicionamento da regra. Em contraste com a opção estrita, se o StorageGRID não puder fazer imediatamente todas as cópias, ele usará o Dual Commit.

Quando usar a opção equilibrada

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 de regras ILM.

Fluxograma de três opções de ingestão

O fluxograma mostra o que acontece quando os objetos são combinados por uma regra ILM que usa uma dessas opções de ingestão.



Informações relacionadas

"Como os objetos são ingeridos"

Vantagens, desvantagens e limitações das opções de proteção de dados

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.

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 de uso para 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 e rigorosas, uma mensagem ""ingest successful"" 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 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 não for possível fazer alterações de posicionamento necessárias (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 ou 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.
- Colocação em um nó de arquivo no dia 0.
- Posicionamentos em um pool de armazenamento em nuvem ou em um nó de arquivamento 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 ou um nó de arquivamento, e um tempo de criação definido pelo usuário pode ser resolvido até o momento.

Como as regras do ILM e os controles de consistência interagem para afetar a proteção de dados

Tanto sua regra ILM quanto sua escolha de controle 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 o controle de consistência usado quando um objeto é armazenado afeta o posicionamento inicial dos metadados de objetos. 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 nível de consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

Aqui está um breve resumo dos controles de consistência 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 eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados.
- **Available** (eventual consistência para OPERAÇÕES DE CABEÇA): Comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações DE CABEÇA.

> Antes de selecionar um nível de consistência, leia a descrição completa dessas configurações nas instruções para criar um aplicativo cliente S3 ou Swift. Você deve entender os benefícios e limitações antes de alterar o valor padrão.

Exemplo de como o controle de consistência e a regra ILM podem interagir

Suponha que você tenha uma grade de dois locais com a seguinte regra ILM e a seguinte configuração de nível de consistência:

- **Regra ILM**: Crie duas cópias de objeto, uma no local e outra em um local remoto. O comportamento de ingestão estrita é selecionado.
- **Nível de consistência**: "Trong-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 o nível de consistência "site-trong", o cliente poderá receber uma mensagem de sucesso depois que os dados do objeto forem 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 níveis de consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Informações relacionadas

"O que é replicação"

"O que é codificação de apagamento"

"Quais são os esquemas de codificação de apagamento"

"Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"

"Use S3"

"Use Swift"

Como os objetos são armazenados (replicação ou codificação de apagamento)

O StorageGRID pode proteger objetos contra perda armazenando cópias replicadas ou armazenando cópias codificadas por apagamento. Você especifica o tipo de cópias a serem criadas nas instruções de colocação das regras do ILM.

- "O que é replicação"
- "Por que você não deve usar replicação de cópia única"
- "O que é codificação de apagamento"
- "Quais são os esquemas de codificação de apagamento"
- "Vantagens, desvantagens e requisitos para codificação de apagamento"

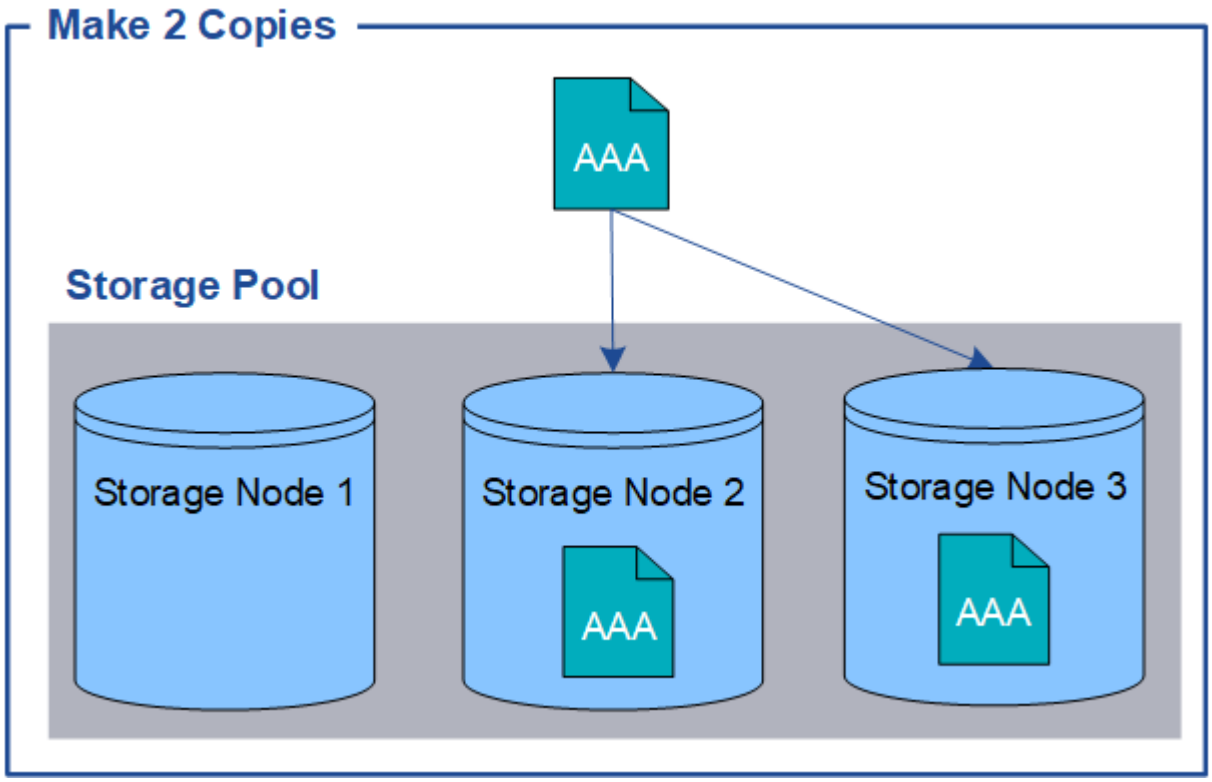
O que é replicação

A replicação é um dos dois métodos usados pelo StorageGRID para armazenar dados de objetos. 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 ou nós de arquivamento.

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 um pool de armazenamento"

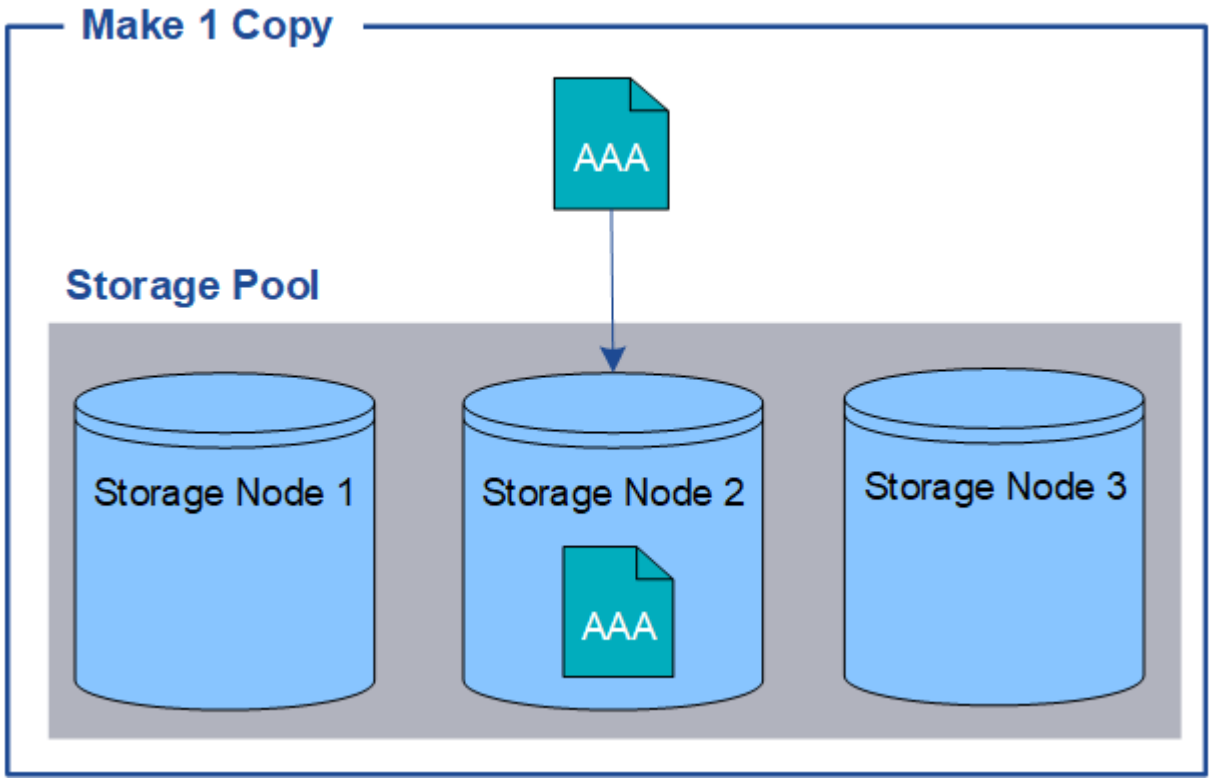
"Uso de vários pools de storage para replicação entre locais"

Por que você não deve usar replicação de cópia única

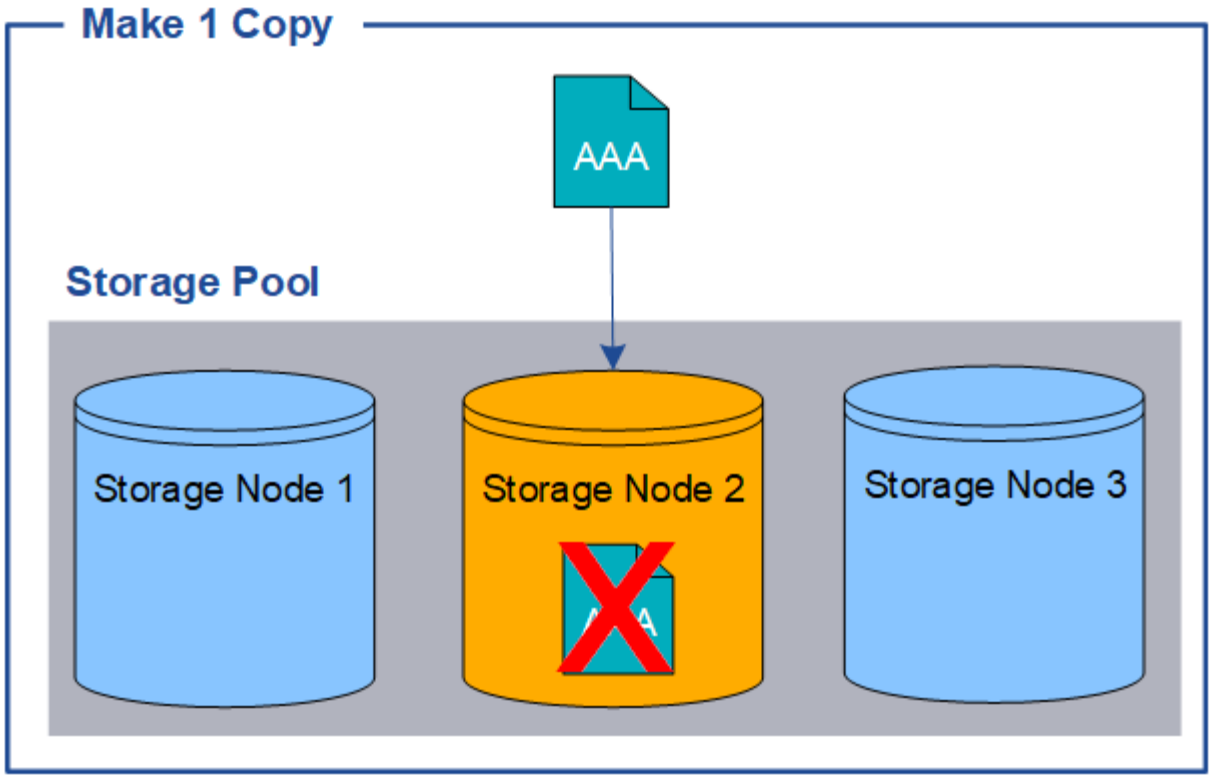
Ao criar uma regra ILM para criar cópias replicadas, você deve sempre especificar pelo menos duas cópias para qualquer período de tempo nas instruções de colocação.

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.

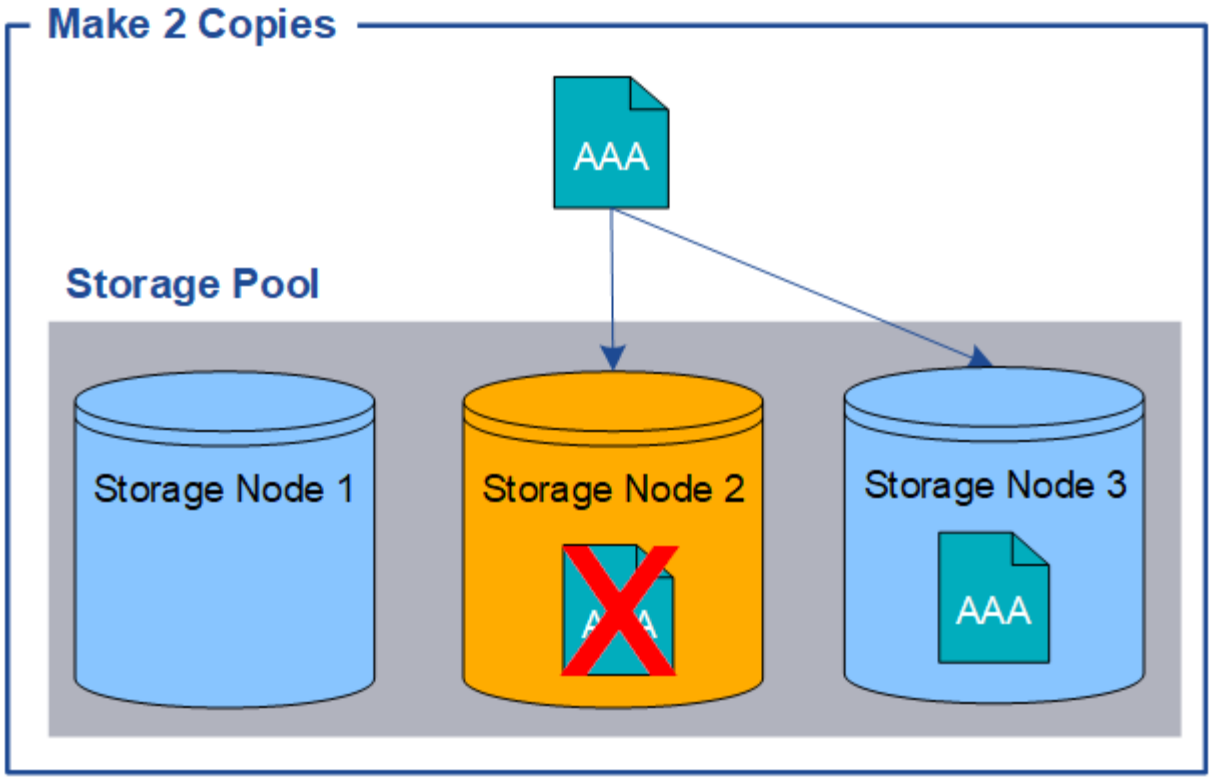
No exemplo a seguir, a regra Make 1 Copy ILM especifica que uma cópia replicada de um objeto seja colocada em um pool de storage que contém três nós de storage. Quando um objeto é ingerido que corresponde a essa regra, o StorageGRID coloca uma única cópia em apenas um nó de storage.



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.



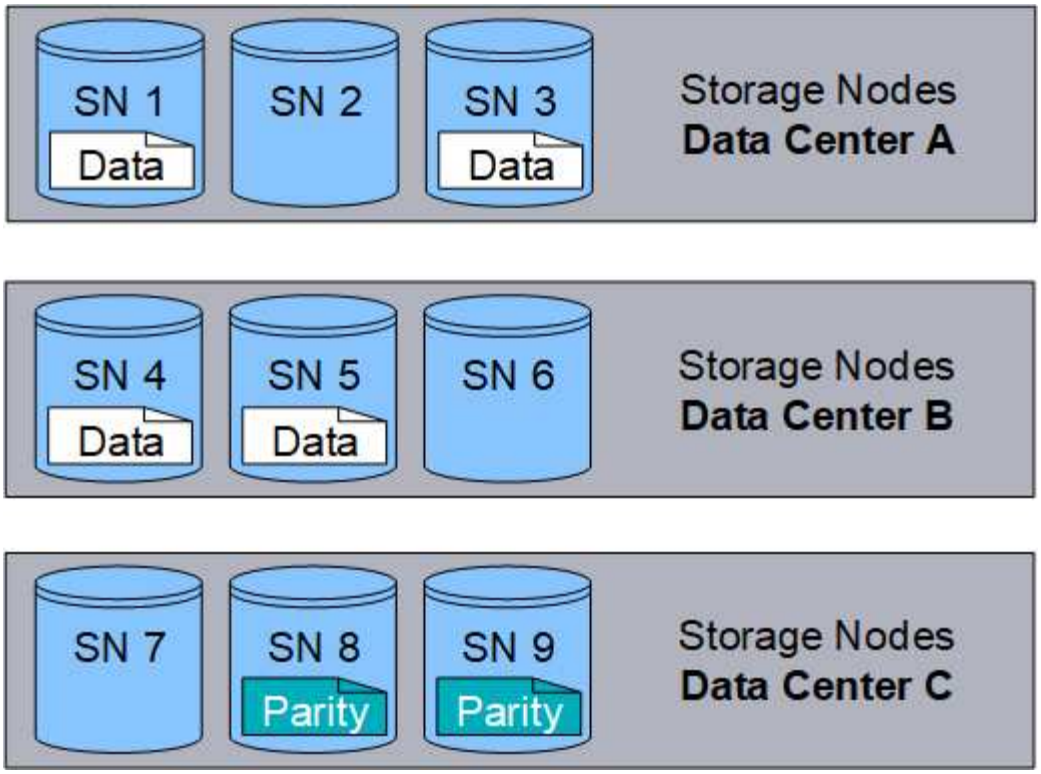
Para evitar a perda de dados de objetos, você sempre deve fazer pelo menos duas cópias de todos os objetos que deseja proteger com a replicação. Se existirem duas ou mais cópias, ainda poderá aceder ao objeto se um nó de armazenamento falhar ou ficar offline.



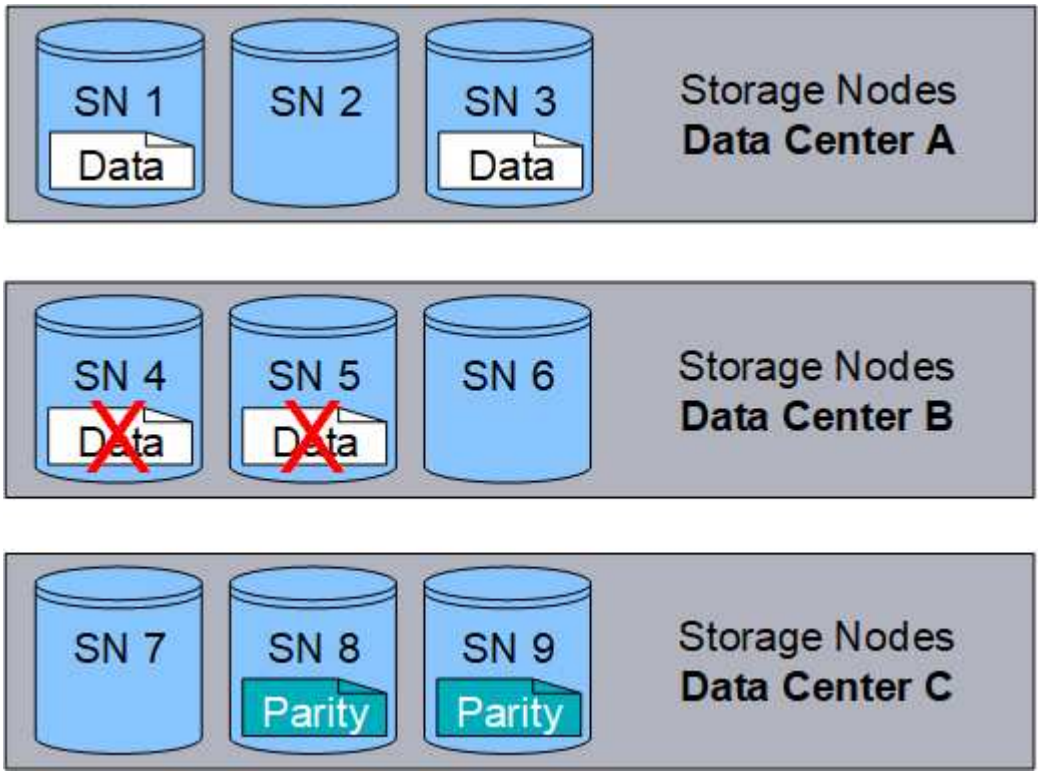
O que é codificação de apagamento

A codificação de apagamento é o segundo método usado pelo StorageGRID para armazenar dados de objetos. 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.

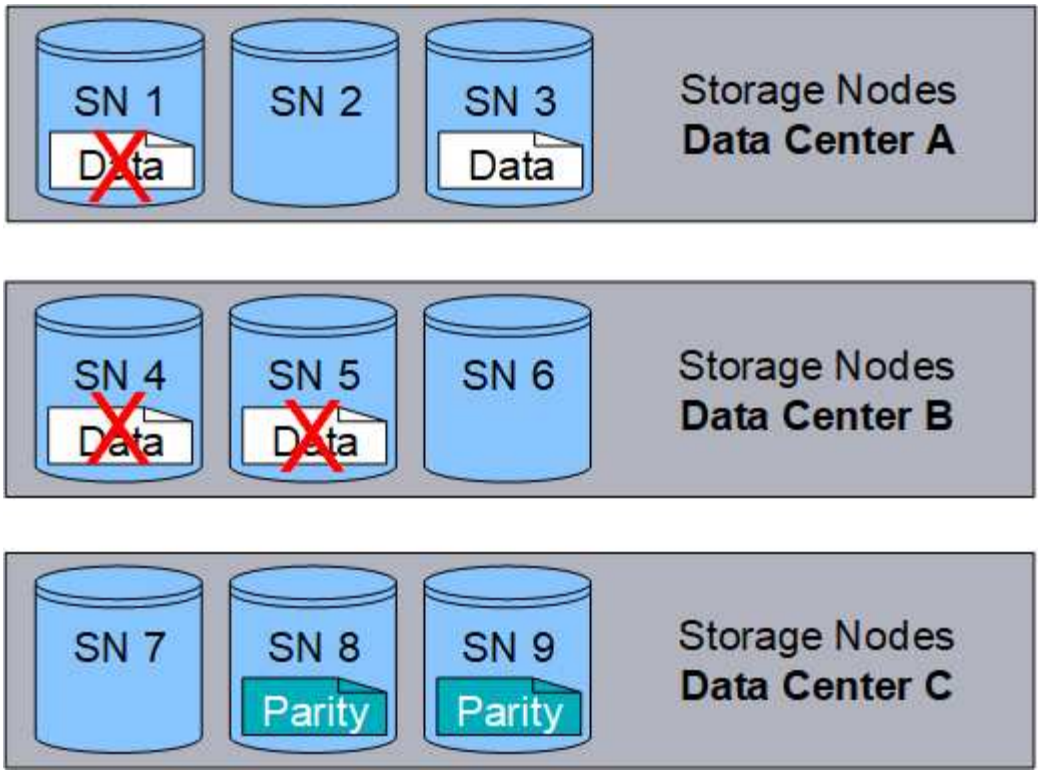
O exemplo a seguir ilustra o uso de um algoritmo de codificação de apagamento nos dados de um objeto. Neste exemplo, a regra ILM usa um esquema de codificação de apagamento 4-2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados 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 mais de 2 requer um mínimo de nove nós de storage, com três nós de storage em cada um dos três locais diferentes. 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 de data center for perdido, o objeto ainda poderá 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 um pool de armazenamento"

"Quais são os esquemas de codificação de apagamento"

"Configurando perfis de codificação de apagamento"

Quais são os esquemas de codificação de apagamento

Ao configurar o perfil de codificação de apagamento para uma regra ILM, você seleciona um esquema de codificação de apagamento disponível com base em quantos nós de storage e sites compõem o pool de storage que você planeja usar. Os esquemas de codificação de apagamento controlam quantos fragmentos de dados e quantos fragmentos de paridade são criados para cada objeto.

O sistema StorageGRID usa o algoritmo de codificação de apagamento de Reed-Solomon. O algoritmo corta um objeto em fragmentos de dados k e calcula fragmentos de paridade m. Os fragmentos k são espalhados pelos nós de storage para fornecer proteção de dados. Um objeto pode sustentar até m fragmentos perdidos ou corrompidos.k fragmentos são necessários para recuperar ou reparar um objeto.

Ao configurar um perfil de codificação de 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 configurar um perfil de 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 o pool de storage padrão, todos os nós de storage ou um pool de storage que inclua o site padrão, todos os sites.
- O pool de storage deve incluir, no mínimo, *k m* 1 nós de storage.

  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.

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 dados (*k*). 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.

Os esquemas de codificação de apagamento com um número menor de fragmentos são geralmente mais eficientes em termos computacionais, pois menos fragmentos são criados e distribuídos (ou recuperados) por objeto, podem mostrar melhor desempenho devido ao tamanho maior do fragmento e podem exigir menos nós sendo adicionados em uma expansão quando mais storage é necessário. (Consulte as instruções para expandir o StorageGRID para obter informações sobre como Planejar uma expansão de armazenamento.)

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 perdas 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 armazenamento 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%

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
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, quando *m* tem um valor maior.)
- **Tráfego de rede**: Ao recuperar de falhas, usar um esquema com mais fragmentos (ou seja, um total mais alto 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 recomendado um pool de storage com nós de storage _k m_1. 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%

Informações relacionadas

"Expanda sua grade"

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 que é codificado de 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:

- É necessário aumentar o número de nós e locais de storage. Por exemplo, se você usar um esquema de codificação de apagamento de 6 a 3, precisará ter pelo menos três nós de storage em três locais diferentes. Em contraste, se você simplesmente replicar dados de objeto, precisará de apenas um nó de storage para cada cópia.
- Aumento do custo e complexidade das expansões de armazenamento. Para expandir uma implantação que usa replicação, basta adicionar capacidade de storage em todos os locais onde as cópias de objetos são feitas. 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, você deve adicionar pelo menos nós de storage *k-m*, mas 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, consulte as instruções para expandir o StorageGRID.
- 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 de apagamento e distribuído entre locais remotos levam mais tempo para serem recuperados por 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.

> Devido à sobrecarga de gerenciamento do número de fragmentos associados a uma cópia codificada por apagamento, não use a codificação de apagamento para objetos de 200 KB ou menos.

- 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.

Informações relacionadas

"Expanda sua grade"

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 têm três maneiras principais de 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, 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 a expiração do ciclo de vida do bucket.

    "Gerenciando objetos com o S3 Object Lock"
- 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.
- Um cliente S3 ou Swift 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 usam instruções de posicionamento ILM para controlar quanto tempo os 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 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, pools de storage de nuvem ou nós de arquivamento).

Como o ciclo de vida do bucket do S3 e o ILM interagem

A ação de expiração em um ciclo de vida do bucket do S3 sempre substitui as configurações do ILM. 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

Armazene 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.

Informações relacionadas

"Gerenciando objetos com o S3 Object Lock"

"Use S3"

"Quais são as instruções de colocação de regras do ILM"

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 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. • Um cliente S3 ou Swift 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 ou Swift 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 ou Swift fazem solicitações de exclusão, o StorageGRID começa adicionando vários 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.

Entendendo o impactos de como o StorageGRID exclui 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 diminuir depois que um certo número de objetos foi 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.

Você deve estar ciente de que o 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 simplesmente cria um marcador de exclusão como a versão atual do objeto, o que torna a versão anterior do objeto "não atual".

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, você deve fazer um dos seguintes procedimentos:

- **Solicitação de cliente S3**: Especifique o número 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.
- **ILM**: Adicione duas regras ILM à sua política ILM. Use **tempo não atual** como tempo de referência na primeira regra para corresponder às versões não atuais do objeto. Use **tempo de ingestão** na segunda regra para corresponder à versão atual. A regra **hora não atual** deve aparecer na política acima da regra **tempo de ingestão**.

Informações relacionadas

"Use S3"

"Exemplo 4: Regras ILM e política para objetos com versão S3"

O que é uma política 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.

Como uma política ILM avalia objetos

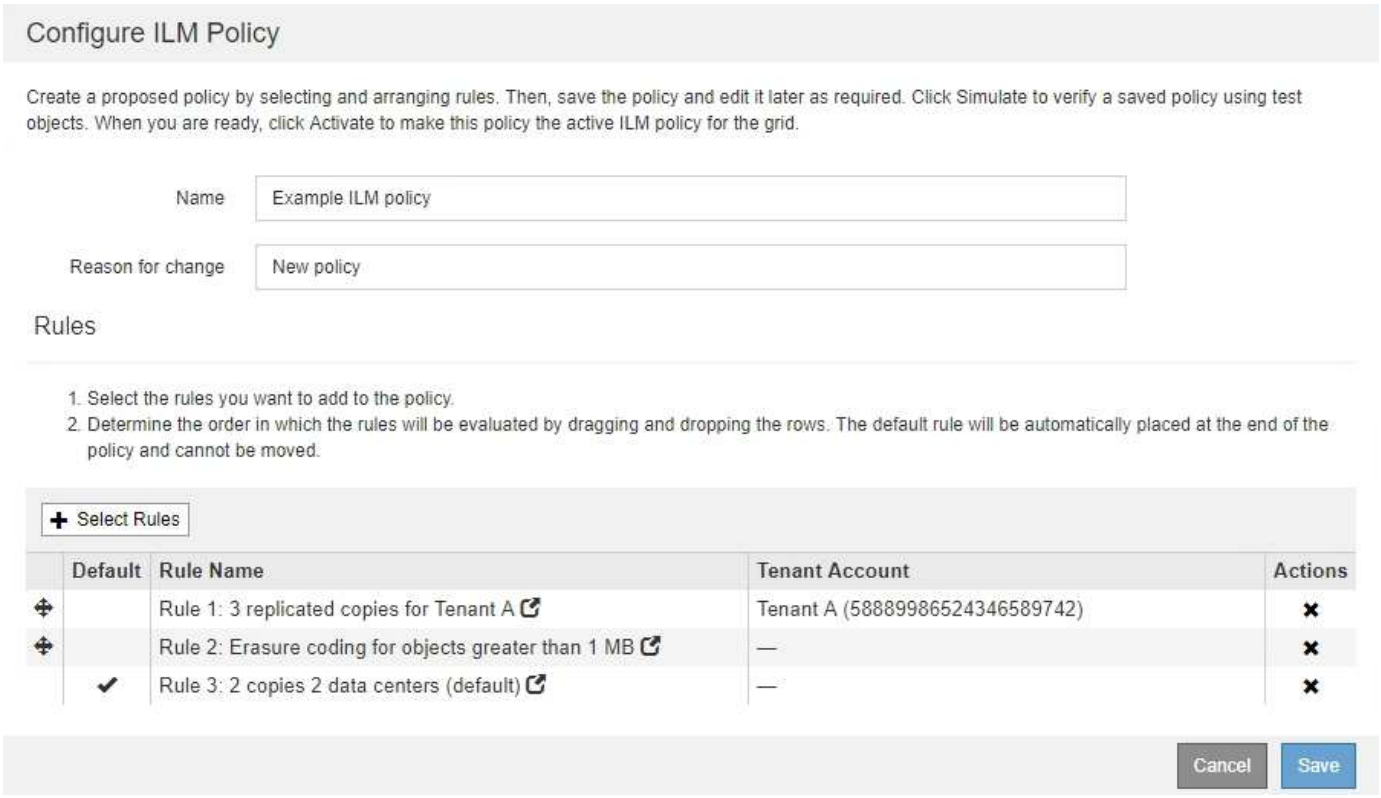
A política de ILM ativa do seu sistema StorageGRID controla o posicionamento, a duração e a proteção de dados de todos os objetos.

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.

Exemplo de política ILM

Este exemplo de política ILM usa três regras ILM.

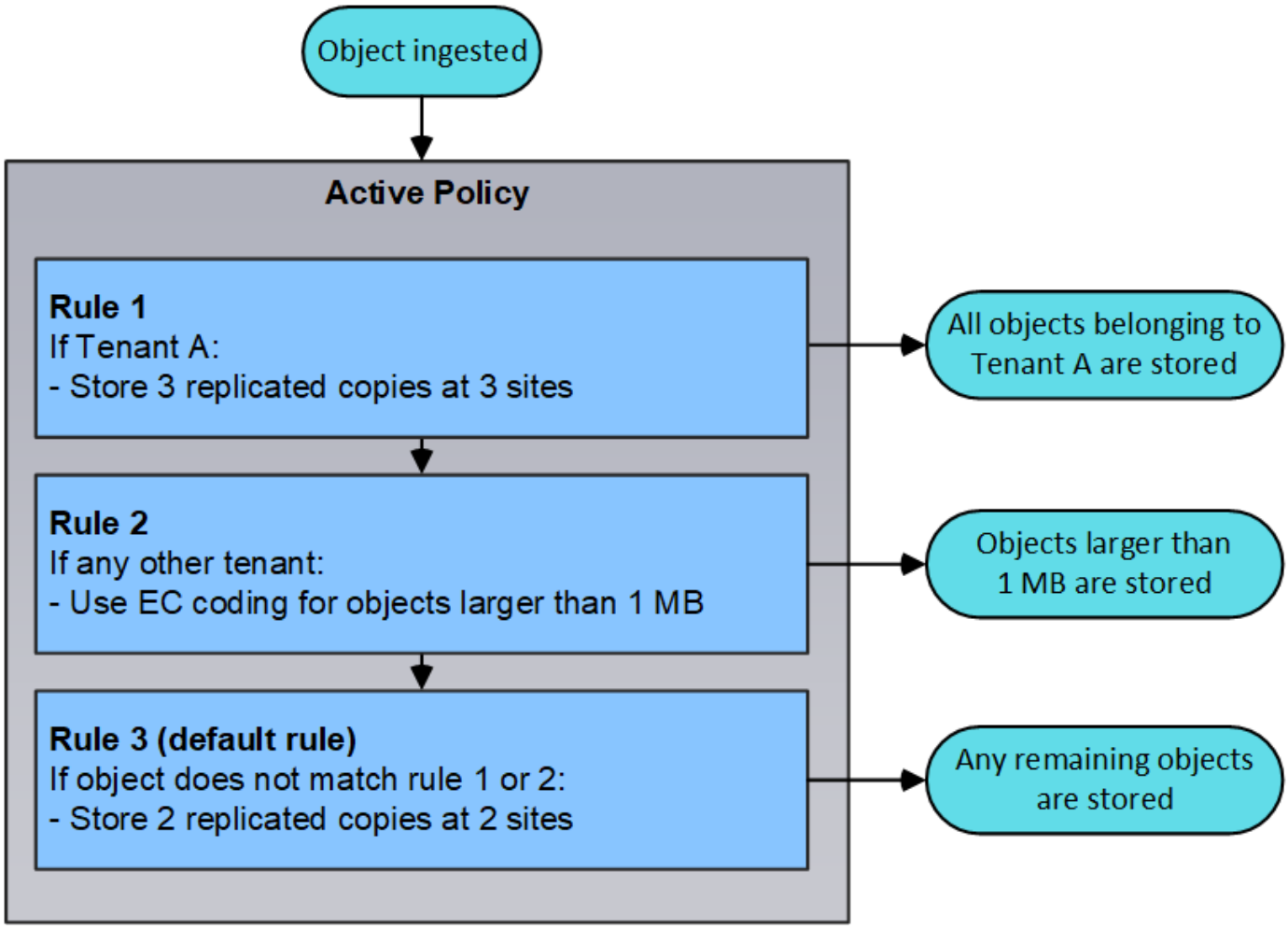


Neste exemplo, a regra 1 corresponde a todos os objetos pertencentes ao locatário A. esses objetos são armazenados como três cópias replicadas em três locais. Os objetos pertencentes a outros inquilinos não são correspondidos pela regra 1, por isso são avaliados em relação à regra 2.

A regra 2 corresponde a 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. A regra 2

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

A regra 3 é a última regra padrão da política e não usa filtros. A regra 3 faz duas cópias replicadas de todos os objetos não correspondidos pela regra 1 ou pela regra 2 (objetos que não pertencem ao locatário A com 1 MB ou menos).



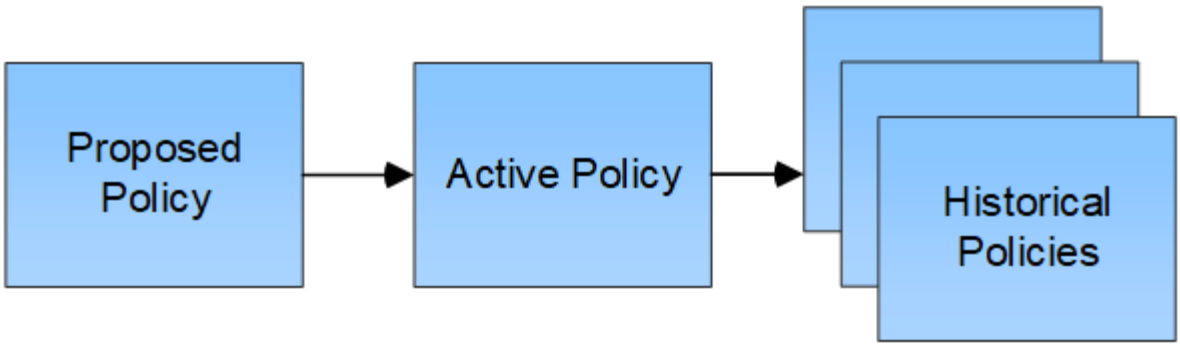
O que as políticas propostas, ativas e históricas são

Cada sistema StorageGRID deve ter uma política ILM ativa. Um sistema StorageGRID também pode ter uma política de ILM proposta e qualquer número de políticas históricas.

Ao criar uma política ILM pela primeira vez, você cria uma política proposta selecionando uma ou mais regras ILM e organizando-as em uma ordem específica. Depois de simular a política proposta para confirmar o seu comportamento, ative-a para criar a política ativa.

Quando você ativa uma nova 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.

Ativar a política proposta faz com que a política anteriormente ativa se torne uma política histórica. As políticas ILM históricas não podem ser eliminadas.



Informações relacionadas

"Criando uma política ILM"

O que é uma regra ILM

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.

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, em pools de storage de nuvem ou em nós de arquivamento.
- 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 de 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. As cópias são distribuídas uniformemente por todos os nós de storage.

Elementos de uma regra ILM

Uma regra ILM tem três elementos:

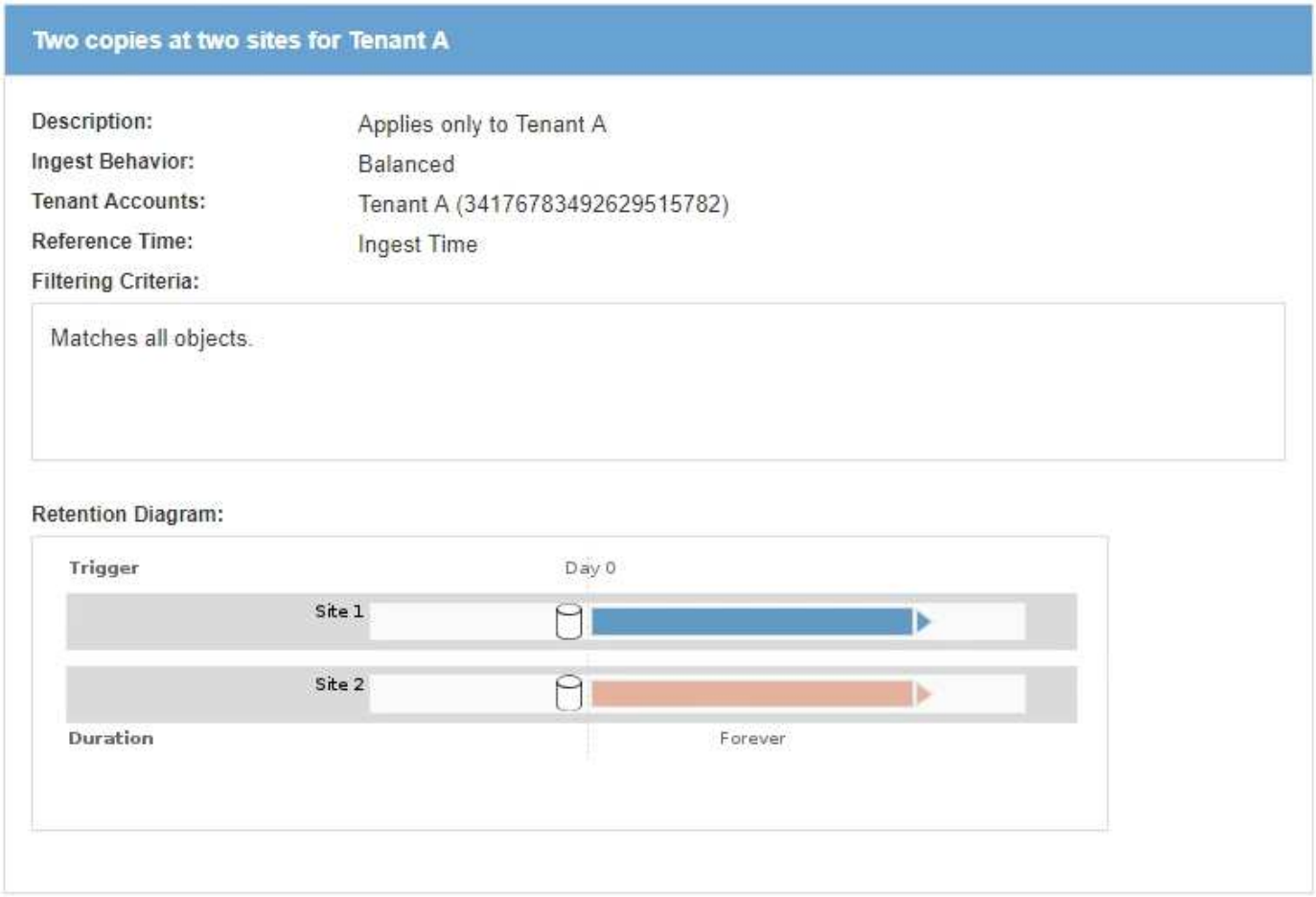
- **Critérios de filtragem**: Os filtros básicos e avançados de uma regra definem a que objetos a regra se aplica. Se um objeto corresponder a todos os filtros, o StorageGRID aplicará a regra e criará as cópias de objeto especificadas nas instruções de colocação da regra.

- **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 define o que acontece quando um cliente S3 ou Swift salva um objeto na grade. 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.

Exemplo de regra ILM

Este exemplo de regra ILM aplica-se aos objetos pertencentes ao locatário A. Ele faz duas cópias replicadas desses objetos e armazena cada cópia em um local diferente. As duas cópias são retidas para sempre, o que significa que o StorageGRID não as apagará 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.

Esta regra usa a opção equilibrada para o 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

"Opções de proteção de dados para ingestão"

"O que é um pool de armazenamento"

"O que é um Cloud Storage Pool"

"Como os objetos são armazenados (replicação ou codificação de apagamento)"

"O que é a filtragem de regras ILM"

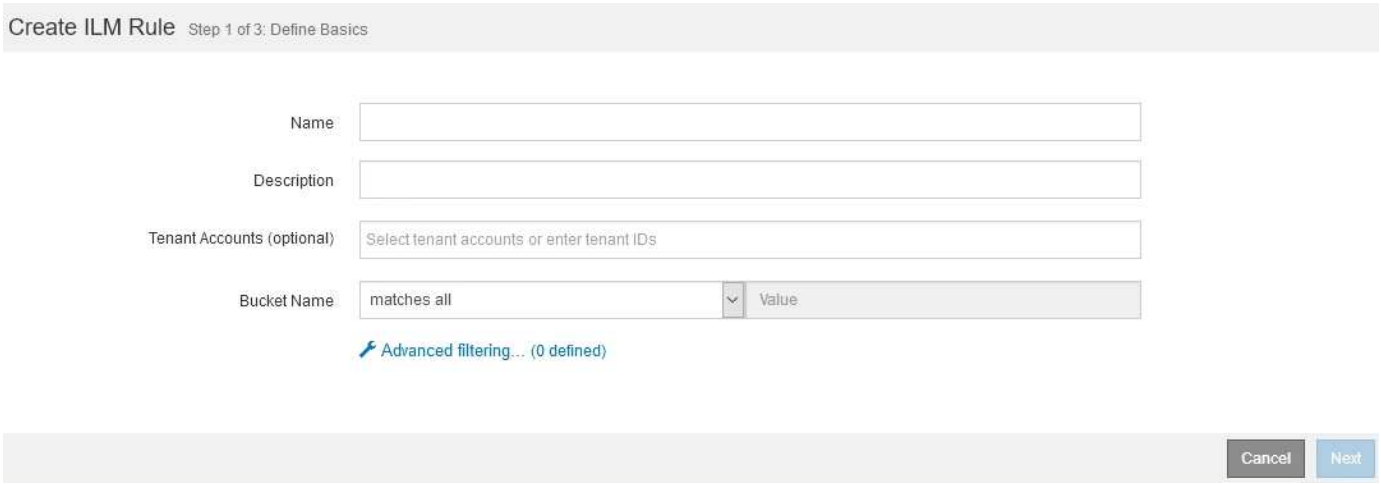
"Quais são as instruções de colocação de regras do ILM"

O que é a 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. Os filtros básicos na página Definir noções básicas do assistente criar regra ILM permitem aplicar uma regra a contas de locatário específicas, buckets específicos do S3 ou contentores Swift, ou ambos.



Esses 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.

A página **Advanced Filtering** do assistente Create ILM Rule fornece 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)
- S3 região do balde (restrição de localização)

- Tamanho do objeto
- Metadados do usuário
- S3 tags de objeto

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 também pode combinar filtros básicos e avançados 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 avançados em cada regra para identificar o tipo específico de objetos aos quais a regra se aplica.

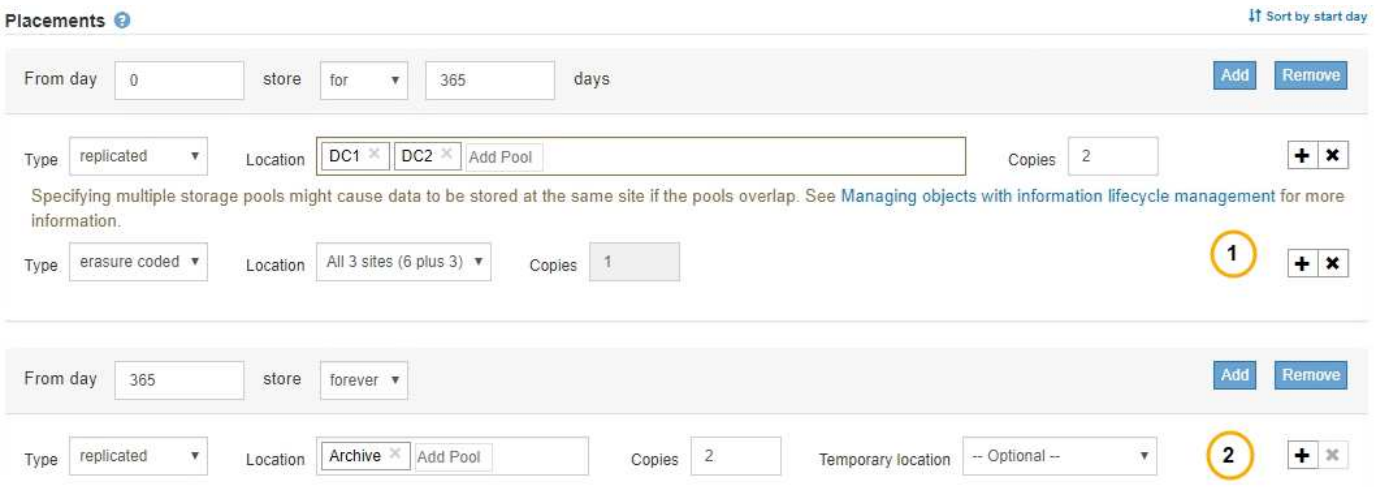
Quais são as instruções de colocação de regras do ILM

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 uma instrução de posicionamento, você especifica quando o posicionamento se aplica (o período de tempo), que tipo de cópias criar (replicadas ou codificadas para apagamento) e onde armazenar as cópias (um ou mais locais de storage). Em uma única regra, você pode especificar vários canais por um período de tempo e instruções de posicionamento por mais de um período de tempo:

- Para especificar mais de um posicionamento de objeto durante um único período de tempo, clique no ícone de sinal de adição ➕para adicionar mais de uma linha para esse período de tempo.
- Para especificar posicionamentos de objetos por mais de um período de tempo, clique no botão **Adicionar** para adicionar o próximo período de tempo. Em seguida, especifique uma ou mais linhas dentro do período de tempo.

O exemplo mostra a página Definir posicionamentos do assistente criar regra ILM.



1	A primeira instrução de colocação tem duas linhas para o primeiro ano: 1. A primeira linha cria duas cópias de objeto replicadas em dois locais de data center. 2. A segunda linha cria uma cópia codificada por apagamento de mais de 6 3 usando três locais de data center.
2	A segunda instrução de colocação cria duas cópias arquivadas 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.

Criação de categorias de storage, pools de storage, perfis de EC e regiões

Antes de criar as regras de ILM para o seu sistema StorageGRID, você deve definir locais de storage de objetos, determinar os tipos de cópias desejadas e, opcionalmente, configurar regiões S3.

- "Criação e atribuição de notas de armazenamento"
- "Configurando pools de armazenamento"
- "Usando Cloud Storage Pools"
- "Configurando perfis de codificação de apagamento"
- "Configurar regiões (opcional e apenas S3)"

Criação e atribuição de notas de armazenamento

Os graus de armazenamento identificam o tipo de armazenamento usado por um nó de

armazenamento. Você pode criar graus de storage se quiser que as regras de ILM coloquem certos objetos em determinados nós de storage, em vez de em todos os nós no local. Por exemplo, você pode querer que certos objetos sejam armazenados em seus nós de storage mais rápidos, como dispositivos de storage all-flash StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Se você usar mais de um tipo de armazenamento, você pode criar opcionalmente um nível de armazenamento para identificar cada tipo. A criação de classes de armazenamento permite selecionar um tipo específico de nó de armazenamento ao configurar pools de armazenamento.

Se o nível de storage não for uma preocupação (por exemplo, todos os nós de storage são idênticos), você poderá ignorar este procedimento e usar o nível de storage padrão de todos os nós de storage ao configurar pools de storage.

Quando você adiciona um novo nó de storage em uma expansão, esse nó é adicionado ao nível de storage padrão de todos os nós de storage. Como resultado:

- Se uma regra de ILM usar um pool de storage com o nível todos os nós de storage, o novo nó poderá ser usado imediatamente após a conclusão da expansão.
- Se uma regra de ILM usar um pool de armazenamento com um grau de armazenamento personalizado, o novo nó não será usado até que você atribua manualmente o grau de armazenamento personalizado ao nó, conforme descrito abaixo.

> ⓘ Ao criar classes de armazenamento, não crie mais classes de armazenamento do que o necessário. Por exemplo, não crie um nível de storage para cada nó de storage. 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. Criar um grau de armazenamento:

   a. Para cada grau de armazenamento que você precisa definir, clique em **Insert** ⊕ para adicionar uma linha e insira um rótulo para o grau de armazenamento.

      O grau de armazenamento predefinido não pode ser modificado. Ele é reservado para novos nós de storage adicionados durante a expansão do sistema StorageGRID.

Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

a. Para editar uma nota de armazenamento existente, clique em **Editar** e modifique a etiqueta conforme necessário.

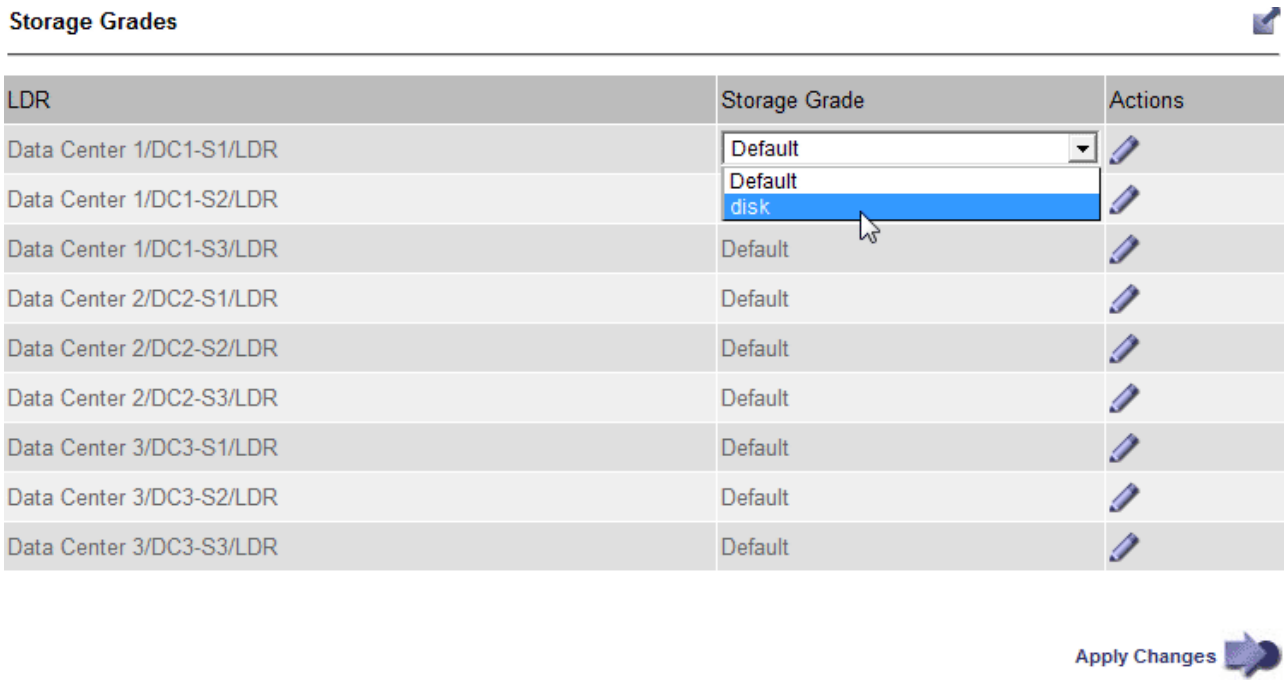
> Não é possível eliminar graus de armazenamento.

b. Clique em **aplicar alterações**.

Esses tipos de storage agora estão disponíveis para atribuição aos nós de storage.

3. Atribuir um nível de storage a um nó de storage:

a. Para cada serviço LDR do nó de armazenamento, clique em **Edit** e selecione uma nota de armazenamento 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. Clique em **aplicar alterações**.

Configurando pools de armazenamento

Ao definir uma regra ILM, você usa pools de armazenamento para especificar onde os objetos são armazenados . Antes de criar um pool de armazenamento, você deve rever as diretrizes do pool de armazenamento.

- "O que é um pool de armazenamento"
- "Diretrizes para a criação de pools de armazenamento"
- "Uso de vários pools de storage para replicação entre locais"
- "Usando um pool de armazenamento como um local temporário (obsoleto)"
- "Criando um pool de armazenamento"
- "Visualização dos detalhes do pool de armazenamento"
- "Editando um pool de armazenamento"
- "Removendo um pool de armazenamento"

O que é um pool de armazenamento

Um pool de storage é um agrupamento lógico de nós de storage ou nós de arquivamento. Você configura pools de storage para determinar onde o sistema StorageGRID armazena dados de objetos e o tipo de storage usado.

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. Ao configurar regras de ILM para replicação, você seleciona um ou mais pools de storage que incluem nós de storage ou nós de arquivamento. Ao criar perfis de codificação de apagamento, você seleciona um pool de storage que inclua nós de storage.

Diretrizes para a criação de pools de armazenamento

Ao configurar e usar pools de armazenamento, siga estas diretrizes.

Diretrizes para todos os pools de armazenamento

- O StorageGRID inclui um pool de storage padrão, todos os nós de storage, que usa o local padrão, todos os locais e o nível de storage padrão, todos os nós de storage. O pool de storage de todos os nós de storage é atualizado automaticamente sempre que você adicionar novos sites de data center.

> ⓘ O uso do pool de storage todos os nós de storage ou do site todos os sites não é recomendado porque esses itens são atualizados automaticamente para incluir novos sites adicionados em uma expansão, o que pode não ser o comportamento desejado. Antes de usar o pool de storage de todos os nós de storage ou o local padrão, revise cuidadosamente as diretrizes para cópias replicadas e codificadas para apagamento.

- 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.

Diretrizes para pools de storage usados para cópias replicadas

- Crie um pool de armazenamento diferente para cada site. Em seguida, especifique um ou mais pools de armazenamento específicos do local nas instruções de posicionamento para cada regra. 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 para o novo site. Em seguida, atualize as regras do ILM para controlar quais objetos são armazenados no novo site.
- Em geral, não use o pool de storage padrão, todos os nós de storage ou qualquer pool de storage que inclua o site padrão, todos os sites.

Diretrizes para pools de storage usados para cópias codificadas por apagamento

- Você não pode usar nós de arquivamento para dados codificados por apagamento.
- O número de nós de storage e sites contidos no pool de storage determina quais esquemas de codificação de apagamento estão disponíveis.

- 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.
- Em geral, não use o pool de storage padrão, todos os nós de storage ou qualquer pool de storage que inclua o site padrão, todos os sites em qualquer perfil de codificação de apagamento.

> Se a grade incluir apenas um local, você será impedido de usar o pool de storage todos os nós de storage ou o site padrão todos os sites em um perfil de codificação de apagamento. Esse comportamento impede que o perfil de codificação de apagamento se torne inválido se um segundo site for adicionado.

- Se você tiver altos requisitos de taxa de transferência, não é recomendável criar um pool de armazenamento que inclua vários locais se a latência de rede entre locais for superior a 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 strict ou balanced 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).
- 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.

Diretrizes para pools de storage usados para cópias arquivadas

- Não é possível criar um pool de storage que inclua nós de storage e nós de arquivamento. As cópias arquivadas exigem um pool de storage que inclui apenas nós de arquivamento.
- Ao usar um pool de storage que inclua nós de arquivamento, você também deve manter pelo menos uma cópia replicada ou codificada de apagamento em um pool de storage que inclua nós de storage.
- Se a configuração global S3 Object Lock estiver ativada e você estiver criando uma regra ILM compatível, não será possível usar um pool de armazenamento que inclua nós de arquivamento. Consulte as instruções para gerenciar objetos com o S3 Object Lock.
- Se o tipo de destino de um nó de arquivamento for Cloud Tiering - Simple Storage Service (S3), o nó de arquivamento deverá estar em seu próprio pool de storage. Consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"O que é replicação"

"O que é codificação de apagamento"

"Quais são os esquemas de codificação de apagamento"

"Uso de vários pools de storage para replicação entre locais"

"Usando um pool de armazenamento como um local temporário (obsoleto)"

"Gerenciando objetos com o S3 Object Lock"

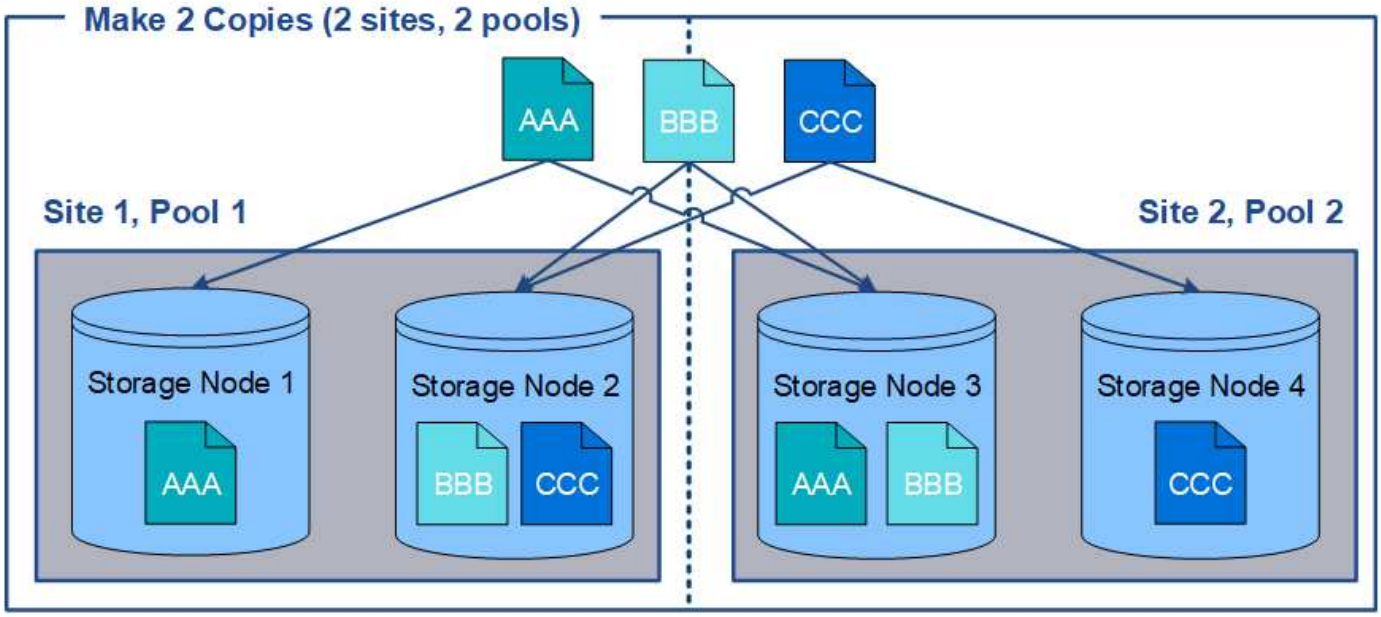
"Administrar o StorageGRID"

Uso de vários pools de storage para replicação entre locais

Se a implantação do StorageGRID incluir mais de um local, você poderá habilitar a proteção contra perda de site criando um pool de armazenamento para cada local e especificando ambos os pools de armazenamento nas instruções de posicionamento da regra. Por exemplo, se você configurar uma regra ILM para fazer duas cópias replicadas e especificar pools de armazenamento em dois locais, uma cópia de cada objeto será colocada em cada local. Se você configurar uma regra para fazer duas cópias e especificar três pools de storage, as cópias serão distribuídas para equilibrar o uso do disco entre os pools de storage, ao mesmo tempo em que garante que as duas cópias sejam armazenadas em locais diferentes.

O exemplo a seguir ilustra o que pode acontecer se uma regra ILM colocar cópias de objetos replicadas em um único pool de storage que contém nós de storage de dois locais. Como o sistema usa todos os nós disponíveis no pool de storage quando ele coloca as cópias replicadas, ele pode colocar todas as cópias de alguns objetos em apenas um dos sites. Neste exemplo, o sistema armazenou duas cópias do objeto AAA em nós de armazenamento no local 1 e duas cópias do objeto CCC em nós de armazenamento no local 2. Somente o objeto BBB é protegido se um dos sites falhar ou se tornar inacessível.

Em contraste, este exemplo ilustra como os objetos são armazenados quando você usa vários pools de armazenamento. No exemplo, a regra ILM especifica que duas cópias replicadas de cada objeto serão criadas e que as cópias serão distribuídas em dois pools de storage. Cada pool de storage contém todos os nós de storage em um local. Como uma cópia de cada objeto é armazenada em cada site, os dados do objeto são protegidos contra falha ou inacessibilidade do site.



Ao usar vários pools de armazenamento, tenha em mente as seguintes regras:

- Se você estiver criando n cópias, será necessário adicionar n ou mais pools de armazenamento. Por exemplo, se uma regra estiver configurada para fazer três cópias, especifique três ou mais pools de storage.

- 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, o sistema distribui as cópias para manter o uso do disco entre os pools balanceado e garantir que duas ou mais cópias não sejam armazenadas no mesmo pool de storage.
- 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.

Usando um pool de armazenamento como um local temporário (obsoleto)

Quando você cria uma regra ILM com um posicionamento de objeto que inclui um único pool de armazenamento, você será solicitado a especificar um segundo pool de armazenamento para usar como um local temporário.

Os locais temporários foram obsoletos e serão removidos em uma versão futura. Você não deve selecionar um pool de armazenamento como um local temporário para uma nova regra ILM.

> ⓘ Se você selecionar o comportamento de ingestão estrita (Etapa 3 do assistente criar regra ILM), o local temporário será ignorado.

Informações relacionadas

"Opções de proteção de dados para ingestão"

Criando 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter revisado 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. Selecione o ícone de mais ➕para adicionar uma entrada para cada site.

Não inclua o local padrão de 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 de 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.

  "Diretrizes para a criação de pools de armazenamento"

Passos

1. Selecione **ILM** > **Storage Pools**.

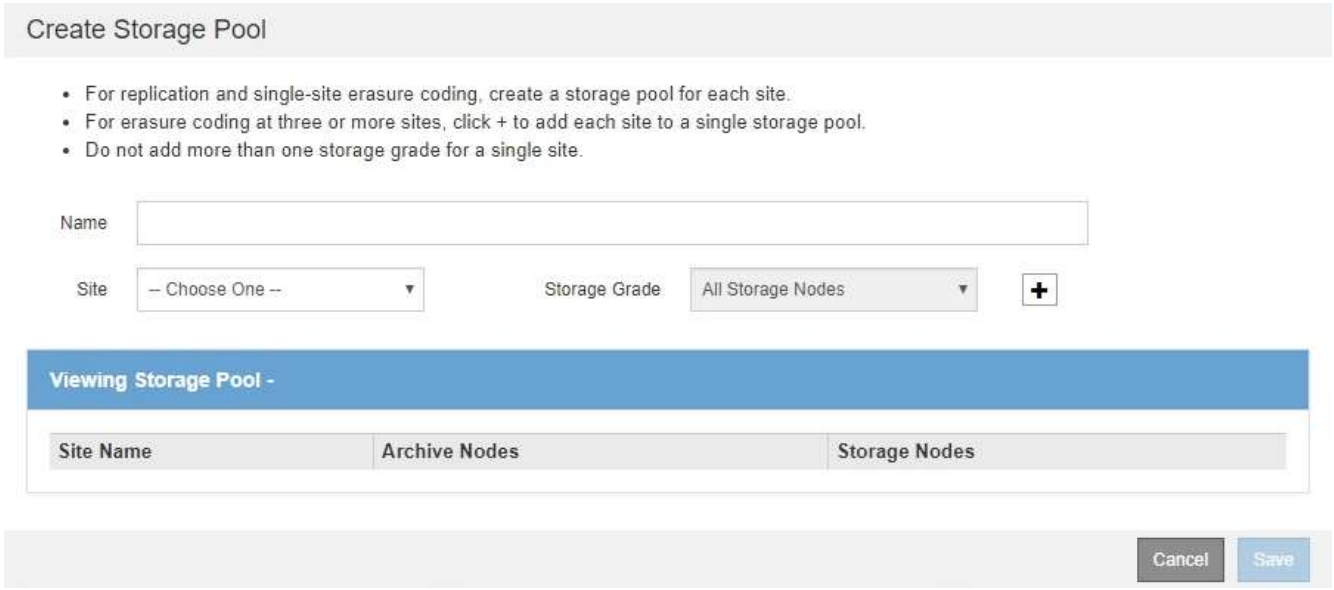
   A página pools de armazenamento é exibida e lista todos os pools de armazenamento definidos.

   A lista inclui o pool de storage padrão do sistema, todos os nós de storage, que usa o site padrão do sistema, todos os sites e a categoria de storage padrão, todos os nós de storage.

   Como o pool de storage de todos os nós de storage é atualizado automaticamente sempre que você adiciona novos locais de data center, o uso desse pool de storage em regras de ILM não é recomendado.

2. Para criar um novo pool de armazenamento, selecione **criar**.

   A caixa de diálogo criar pool de armazenamento é exibida.



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.

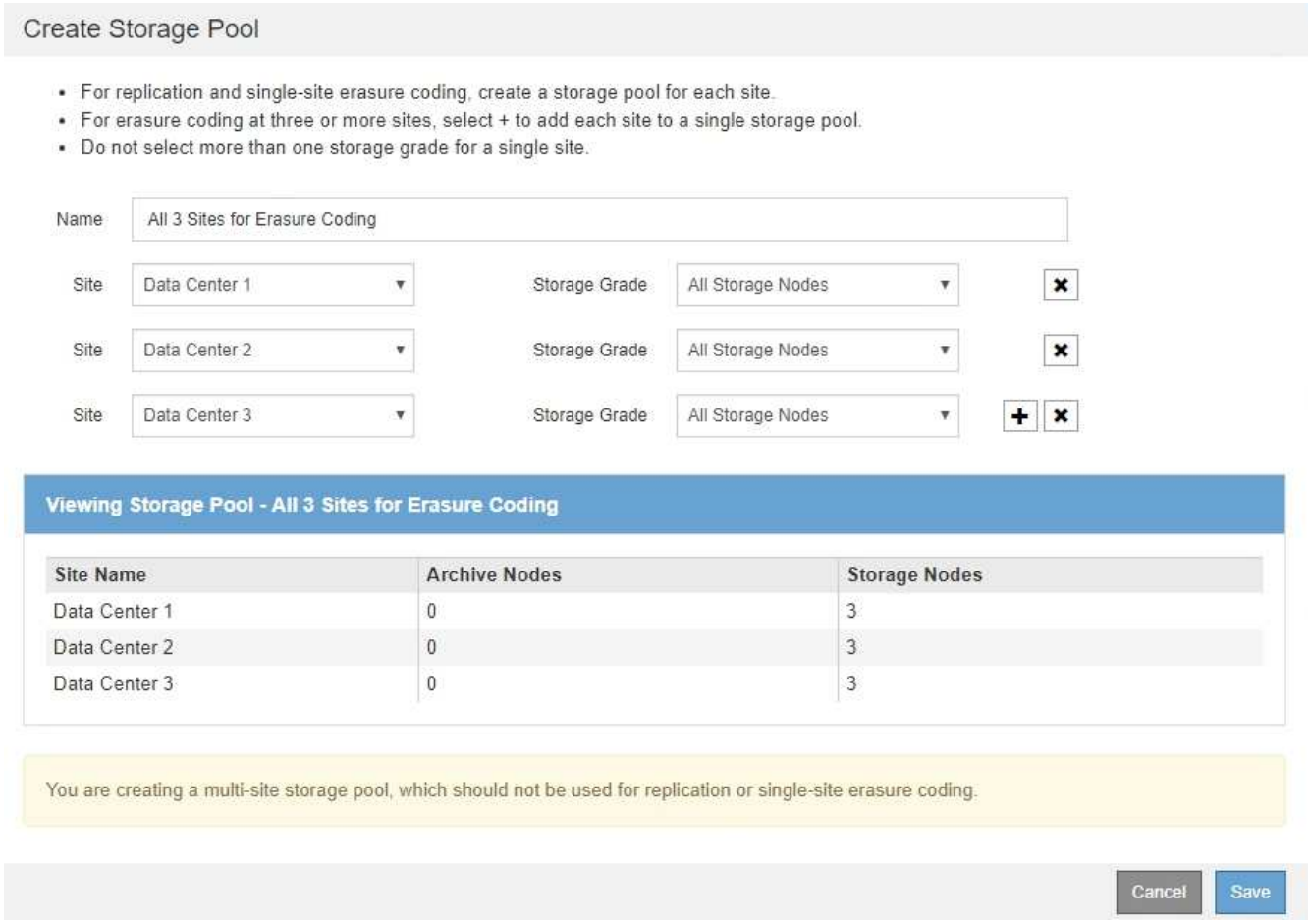
4. Na lista suspensa **Site**, selecione um site para esse pool de armazenamento.

   Quando você seleciona um site, o número de nós de storage e nós de arquivamento na tabela é atualizado automaticamente.

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 padrão de todos os nós de storage inclui todos os nós de storage no local selecionado. O grau de storage padrão dos nós de arquivamento inclui todos os nós de arquivamento 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 para adicionar uma entrada para cada site ao pool de armazenamento.



É impedido de criar entradas duplicadas ou de criar um pool de armazenamento que inclua o grau de armazenamento **Archive Nodes** e qualquer tipo de armazenamento que contenha nós de armazenamento.

Você será avisado se você adicionar mais de uma entrada para um site, mas com diferentes graus de armazenamento.

Para remover uma entrada, selecione .

7. Quando estiver satisfeito com suas seleções, selecione **Salvar**.

   O novo pool de armazenamento é adicionado à lista.

Informações relacionadas

"Diretrizes para a criação de pools de armazenamento"

Visualização dos 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.

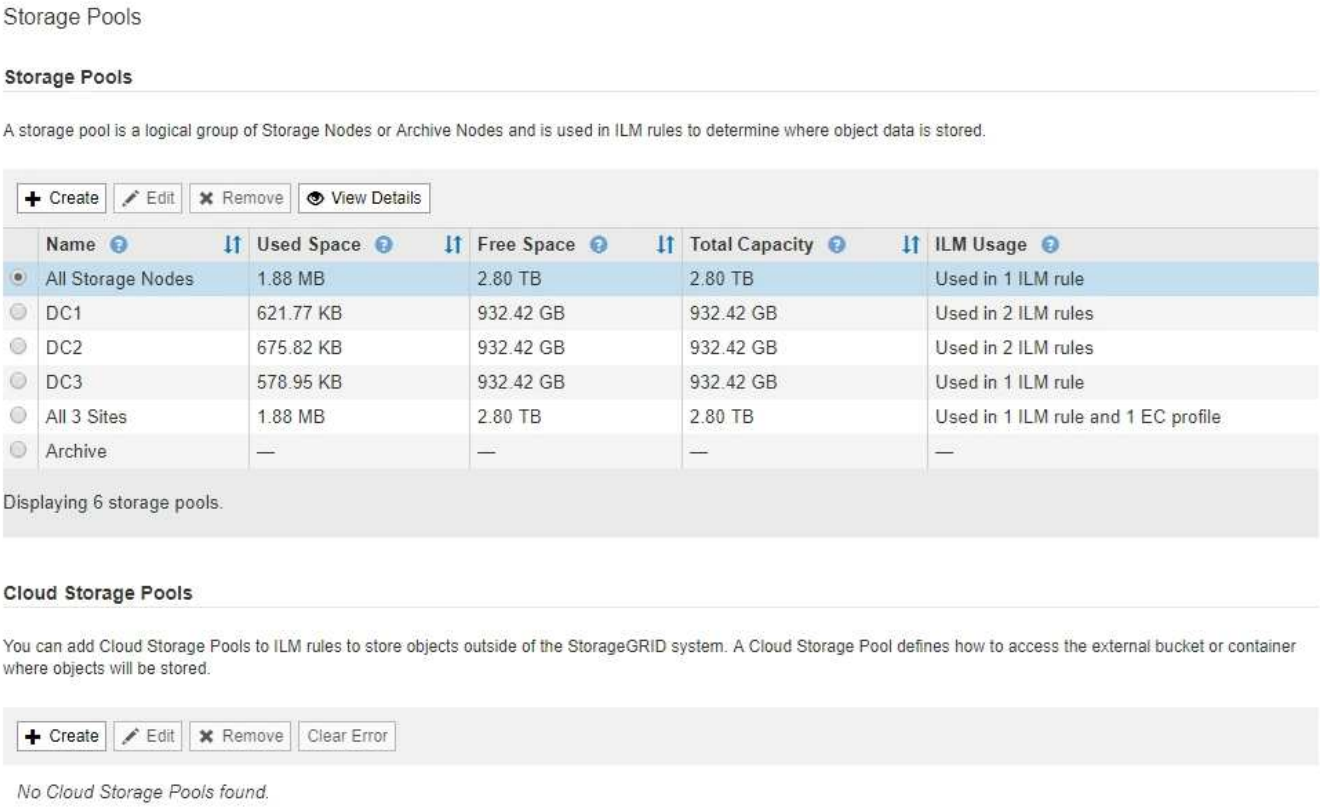
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **ILM** > **Storage Pools**.

   A página conjuntos de armazenamento é exibida. Esta página lista todos os pools de armazenamento definidos.



   A tabela inclui as seguintes informações para cada pool de storage que inclui nós de storage:

   - **Nome**: O nome de exibição exclusivo do pool de armazenamento.
   - **Espaço usado**: A quantidade de espaço que está sendo usada atualmente para armazenar objetos no pool de armazenamento.
   - **Espaço livre**: A quantidade de espaço que permanece disponível para armazenar objetos no pool de armazenamento.
   - **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 do 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.

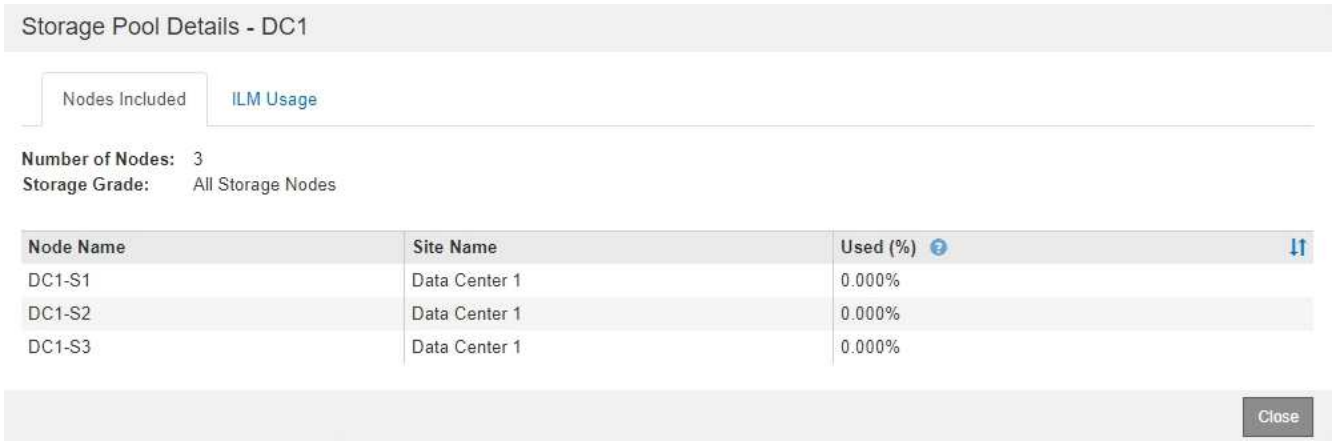
     Você não pode remover um pool de armazenamento se ele estiver sendo usado.

2. Para ver detalhes sobre um pool de armazenamento específico, selecione seu botão de opção e selecione **Exibir detalhes**.

   O modal Detalhes do conjunto de armazenamento é exibido.

3. Exiba a guia **nós incluídos** para saber mais sobre os nós de armazenamento ou nós de arquivamento

incluídos no pool de armazenamento.



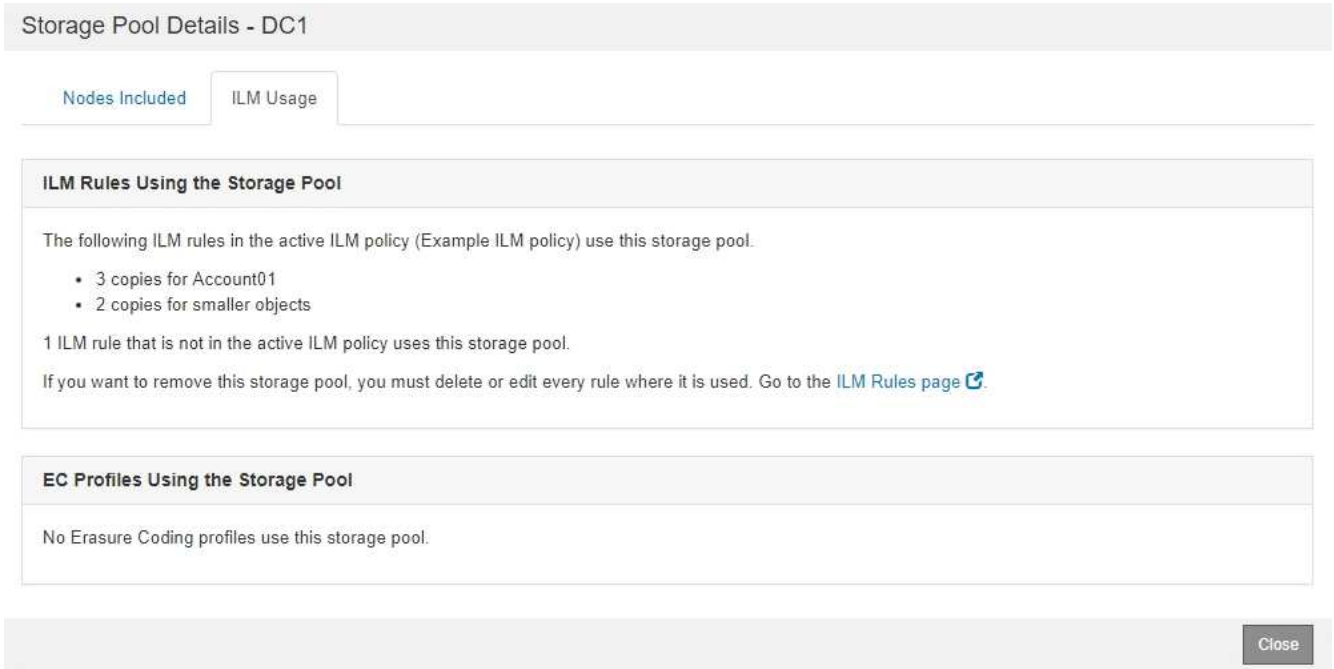
A tabela inclui as seguintes informações para cada nó:

- Nome do nó
- Nome do local
- Usado (%): Para nós de storage, a porcentagem do espaço utilizável total para dados de objetos que foram usados. Esse valor não inclui metadados de objetos.

> O mesmo valor usado (%) também é mostrado no gráfico armazenamento usado - dados de objetos para cada nó de armazenamento (selecione **nós** > ***Storage Node*** > **Storage**).

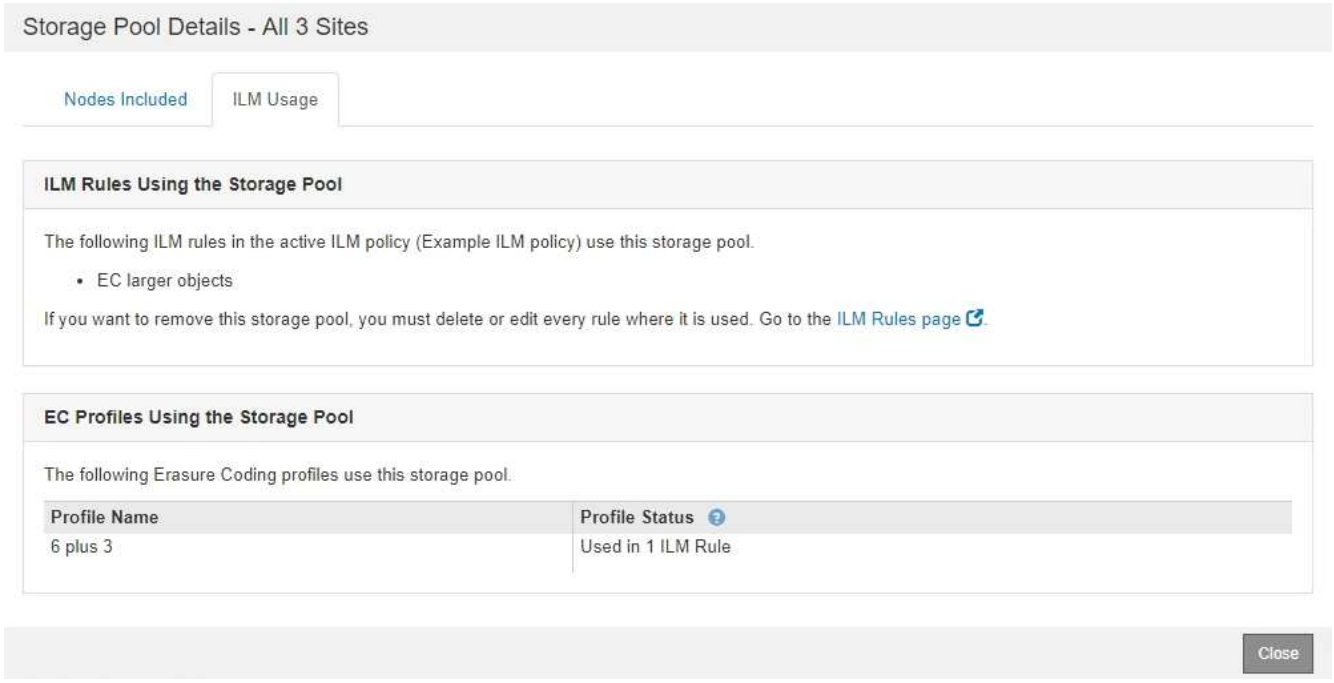
4. Selecione a guia **uso de ILM** para determinar se o pool de armazenamento está sendo usado atualmente em quaisquer regras de ILM ou perfis de codificação de apagamento.

   Neste exemplo, o pool de armazenamento DC1 é usado em três regras ILM: Duas regras que estão na política ILM ativa e uma regra que não está na política ativa.



Você não pode remover um pool de armazenamento se ele for usado em uma regra ILM.

Neste exemplo, o pool de armazenamento de todos os 3 sites é usado em um perfil de codificação de apagamento. Por sua vez, esse perfil de codificação de apagamento é usado por uma regra ILM na política ILM ativa.



Não é possível remover um pool de armazenamento se ele for usado em um perfil 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 as instruções para trabalhar com regras ILM.

6. Quando terminar de visualizar os detalhes do conjunto de armazenamento, selecione **Fechar**.

Informações relacionadas

"Trabalhando com regras de ILM e políticas de ILM"

Editando um pool de armazenamento

Você pode editar um pool de armazenamento para alterar seu nome ou atualizar sites e classes de armazenamento.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter revisado as 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 deve ter considerado como suas alterações afetarão o posicionamento dos dados do objeto.

Sobre esta tarefa

Se você estiver adicionando um novo nível de storage a um pool de storage usado na política de ILM ativa, saiba que os nós de storage no novo nível de storage não serão usados automaticamente. Para forçar o StorageGRID a usar um novo 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**.

   A página conjuntos de armazenamento é exibida.

2. Selecione o botão de opção para o pool de armazenamento que deseja editar.

   Não é possível editar o pool de storage todos os nós de storage.

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, uma vez que a alteração tornaria o esquema de codificação de apagamento inválido.

6. Selecione **Guardar**.

Depois de terminar

Se você adicionou um novo 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 nível de armazenamento. Por exemplo, clone sua política ILM existente e, em seguida, ative o clone.

Removendo um pool de armazenamento

Você pode remover um pool de armazenamento que não está sendo usado.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **ILM** > **Storage Pools**.

   A página conjuntos de armazenamento é exibida.

2. Observe a coluna 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 **Exibir detalhes** > **uso do ILM** para determinar onde um pool de armazenamento é usado.

3. Se o conjunto de armazenamento que pretende remover não estiver a ser utilizado, selecione o botão de opção.
4. Selecione **Remover**.
5. Selecione **OK**.

Usando Cloud Storage Pools

Você pode usar o Cloud Storage Pools para mover objetos do StorageGRID para um local de storage externo, como o S3 Glacier ou o storage Microsoft Azure Blob. Mover objetos para fora da grade permite que você aproveite uma camada de storage de baixo custo para arquivamento de longo prazo.

- "O que é um Cloud Storage Pool"
- "Ciclo de vida de um objeto Cloud Storage Pool"
- "Quando usar Cloud Storage Pools"
- "Considerações para pools de storage em nuvem"
- "Comparação do Cloud Storage Pools e da replicação do CloudMirror"
- "Criando um pool de armazenamento em nuvem"
- "Editando um pool de armazenamento em nuvem"
- "Removendo um pool de armazenamento em nuvem"
- "Solução de problemas de 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, é possível mover objetos acessados com pouca frequência para storage de nuvem de baixo custo, como Amazon S3 Glacier, S3 Glacier Deep Archive ou a camada de acesso de arquivamento no storage Microsoft Azure Blob. 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 ou nós de arquivamento no sistema StorageGRID, um pool de storage de nuvem consiste em um bucket externo (S3) ou contêiner (storage Blob do Azure).

A tabela a seguir 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. Você deve configurar classes de armazenamento antes de criar o pool de armazenamento.	Usando a opção **ILM** > **Storage Pools** no Gerenciador de Grade. Você deve configurar o bucket externo ou o contêiner antes de criar o pool de storage de nuvem.
Quantas piscinas você pode criar?	Ilimitado.	Até 10 TB.
Onde os objetos são armazenados?	Em um ou mais nós de storage ou nós de arquivamento no StorageGRID.	Em um bucket do Amazon S3 ou contêiner de storage Azure Blob 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 storage externo deve oferecer suporte à classe de storage Glacier e à API de restauração PÓS-objeto S3. • 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 do armazenamento de Blobs do Azure para o contêiner usado em um pool de storage de nuvem. As operações de restauração PÓS-objeto em objetos no Cloud Storage Pool podem ser afetadas pelo ciclo de vida configurado.
O que controla o posicionamento do objeto?	Uma regra ILM na política ILM ativa.	Uma regra ILM na política ILM ativa.

	Pool de storage	Cloud Storage Pool
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.
Quais são as vantagens?	Os objetos são rapidamente acessíveis a qualquer momento.	Armazenamento de baixo custo.

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.

Informações relacionadas

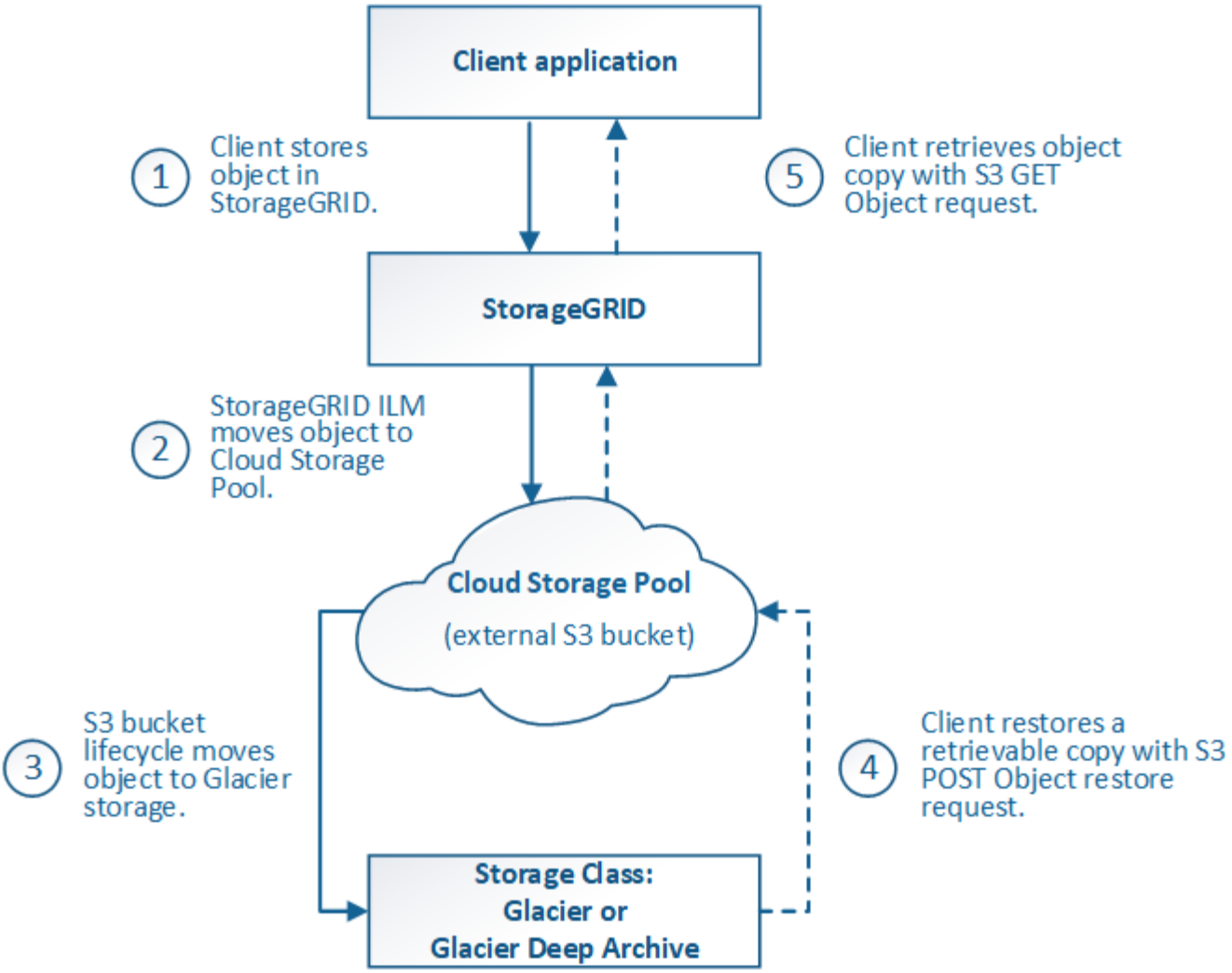
S3: Ciclo de vida de um objeto Cloud Storage Pool

Azure: Ciclo de vida de um objeto Cloud Storage Pool]

S3: Ciclo de vida de um objeto Cloud Storage Pool

A figura mostra os estágios do ciclo de vida de um objeto que é armazenado em um pool de armazenamento em nuvem do S3.

> Na figura e explicações, "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.



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 de objeto S3 GET 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 de restauração PÓS-objetos do S3.

> Não use Cloud Storage Pools para objetos que foram ingeridos por clientes Swift. O Swift não suporta solicitações de restauração PÓS-objeto, portanto, o StorageGRID não poderá recuperar quaisquer objetos Swift que tenham sido transferidos para o armazenamento do Glacier S3. Emitir uma solicitação de objeto Swift GET para recuperar esses objetos falhará (403 Forbidden).

    - Durante a transição, o aplicativo cliente pode usar uma solicitação de objeto S3 HEAD 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 restauração PÓS-objeto S3 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 restauração PÓS-objeto. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma SOLICITAÇÃO GET Object.

5. **Objeto recuperado**

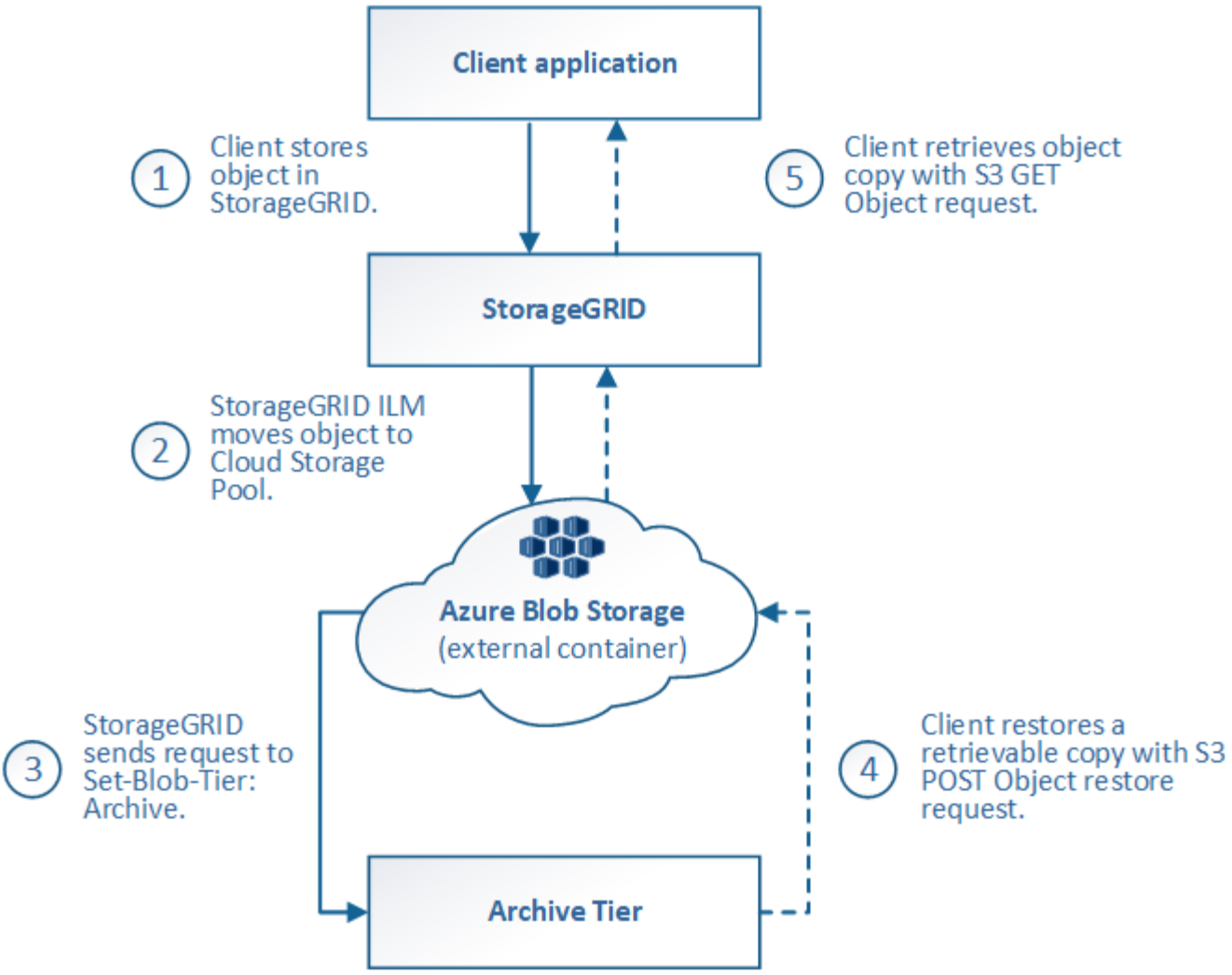
   Uma vez que um objeto foi restaurado, o aplicativo cliente pode emitir uma solicitação GET Object para recuperar o objeto restaurado.

Informações relacionadas

"Use S3"

Azure: Ciclo de vida de um objeto Cloud Storage Pool

A figura mostra 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

   > Não use Cloud Storage Pools para objetos que foram ingeridos por clientes Swift. O Swift não oferece suporte a solicitações de restauração PÓS-objeto, portanto, o StorageGRID não será capaz de recuperar objetos Swift que tenham sido transferidos para a camada de arquivamento de armazenamento de Blobs do Azure. Emitir uma solicitação de objeto Swift GET para recuperar esses objetos falhará (403 Forbidden).

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 a camada de arquivamento, o aplicativo cliente poderá emitir uma solicitação de restauração PÓS-Objeto S3 para restaurar uma cópia recuperável para o pool de armazenamento em nuvem do Azure.

Quando o StorageGRID recebe a Restauração PÓS-Objeto, 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 restauração PÓS-objeto 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 restauração PÓS-objeto. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma SOLICITAÇÃO GET Object.

5. **Objeto recuperado**

   Depois que um objeto for restaurado para o Azure Cloud Storage Pool, o aplicativo cliente poderá emitir uma SOLICITAÇÃO GET Object para recuperar o objeto restaurado.

Quando usar Cloud Storage Pools

Os pools de storage em nuvem podem fornecer benefícios significativos em vários casos de uso.

Fazer backup de dados 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 uma solicitação de restauração PÓS-objeto S3 para acessar a cópia de objeto de backup no Cloud Storage Pool.

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.

Disposição em camadas de dados do StorageGRID para um 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 pools de storage em nuvem 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 armazenamento do Blob do Azure. Ou, talvez você queira mover dados entre o Amazon S3 Glacier e o storage Azure Blob. Ao usar vários pools de armazenamento em nuvem, 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.
- Não use Cloud Storage Pools para objetos que foram ingeridos por clientes Swift. O Swift não oferece suporte a solicitações de restauração PÓS-objeto, portanto, o StorageGRID não poderá recuperar objetos Swift que tenham sido transferidos para o armazenamento do Glacier S3 ou para o nível de arquivamento de armazenamento Blob do Azure. Emitir uma solicitação de objeto Swift GET para recuperar esses objetos falhará (403 Forbidden).
- 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.

Informações necessárias para criar um pool de armazenamento em nuvem

Antes de criar um Cloud Storage Pool, você precisa criar o bucket externo do S3 ou o contêiner de storage externo de Blob do Azure que usará no Cloud Storage Pool. Em seguida, ao criar o pool de armazenamento em nuvem no StorageGRID, você deve especificar as seguintes informações:

- O tipo de provedor: Armazenamento Amazon S3 ou Azure Blob.
- Se você selecionar Amazon S3, se o pool de armazenamento em nuvem é para uso com a região secreta da AWS (**CAP (C2S Access Portal)**).
- O nome exato do balde ou recipiente.
- O endpoint de serviço necessário para acessar o bucket ou o contentor.
- A autenticação necessária para acessar o bucket ou o contentor:
  - **S3**: Opcionalmente, uma ID de chave de acesso e chave de acesso secreta.
  - **C2S**: A URL completa para obter credenciais temporárias do SERVIDOR CAP; um certificado CA de servidor, um certificado de cliente, uma chave privada para o certificado de cliente e, se a chave privada for criptografada, a senha para descriptografá-lo.
  - **Armazenamento Blob do Azure**: Um nome de conta e chave de conta. Essas credenciais devem ter permissão completa para o contentor.
- Opcionalmente, um certificado de CA personalizado para verificar conexões TLS com o bucket ou contentor.

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 para 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. Neste caso, você simplesmente 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

A política de bucket do bucket externo do S3 usada em um pool de armazenamento em nuvem deve 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 pela política de ILM ativa 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 de restauração PÓS-objeto do S3.

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 de ciclo de vida do Azure Blob Storage 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

"Criando um pool de armazenamento em nuvem"

"S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"

"C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"

"Azure: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"

Comparação do Cloud Storage Pools e da 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?	Um pool de storage em nuvem atua como destino de arquivamento. 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 apenas uma cópia no StorageGRID e enviar uma cópia para o pool de storage de nuvem.	O serviço de replicação do CloudMirror 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.
Como é configurado?	Os pools de armazenamento em nuvem são definidos da mesma forma que os pools de armazenamento, usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Um pool de armazenamento em nuvem 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 Tenant ou a API 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
Qual é o destino?	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3) • Camada de arquivamento de Blob do Azure	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3)
O que faz com que os objetos sejam movidos para o destino?	Uma ou mais regras ILM na política ILM ativa. 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.Objects do CloudMirror que existiam no bucket de origem antes que o bucket fosse configurado com o endpoint do CloudMirror não são replicados, a menos que sejam modificados.

	Cloud Storage Pool	Serviço de replicação do CloudMirror
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 no 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.
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.

Informações relacionadas

"Administrar o StorageGRID"

Criando um pool de armazenamento em nuvem

Ao criar um pool de storage de nuvem, especifique o nome e o local do bucket externo ou do contêiner que o StorageGRID usará para armazenar objetos, o tipo de fornecedor de nuvem (Amazon S3 ou armazenamento de Blob do Azure) e as informações que o StorageGRID precisa para acessar o bucket externo ou o contêiner.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter permissões de acesso específicas.
- Você precisa ter revisado as diretrizes para configurar os pools de armazenamento em nuvem.
- O bucket externo ou o contêiner referenciado pelo Cloud Storage Pool deve existir.
- Você deve ter todas as informações de autenticação necessárias para acessar o bucket ou o contentor.

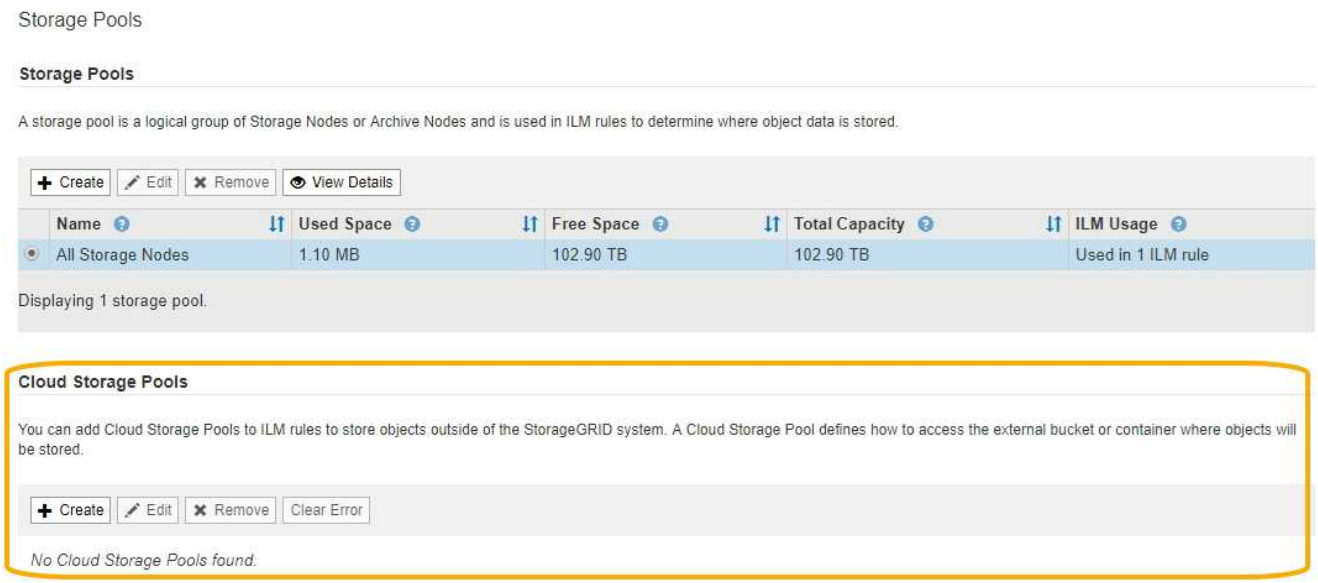
Sobre esta tarefa

Um Cloud Storage Pool especifica um único bucket externo do S3 ou contêiner de storage Azure Blob. 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.

Passos

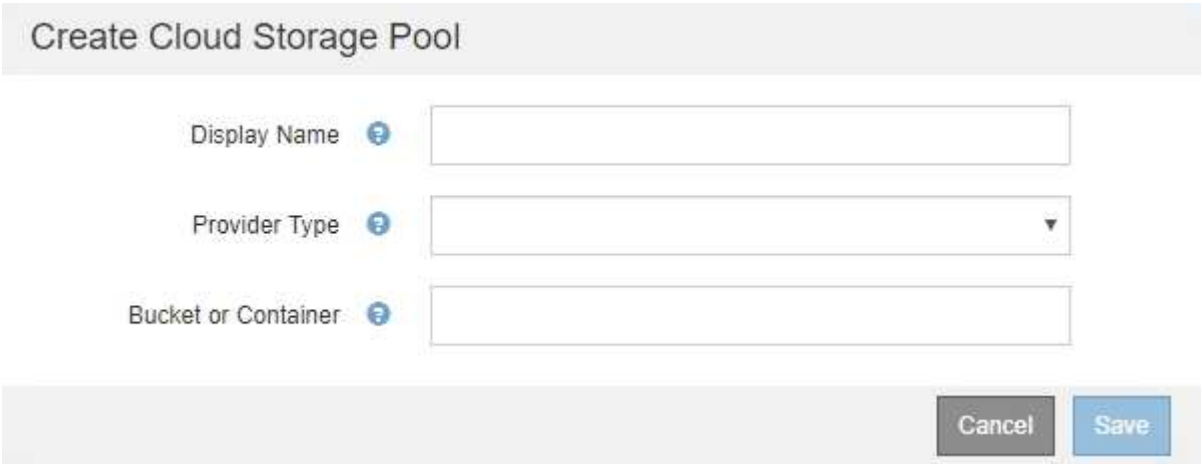
1. Selecione **ILM** > **Storage Pools**.

   A página conjuntos de armazenamento é exibida. Esta página inclui duas seções: Pools de armazenamento e pools de armazenamento em nuvem.



2. Na seção Cloud Storage Pools da página, clique em **criar**.

   A caixa de diálogo criar pool de armazenamento em nuvem é exibida.



3. Introduza as seguintes informações:

Campo	Descrição
Nome de exibição	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 (selecione essa opção para um pool de armazenamento em nuvem S3 ou C2S S3) • Storage Blob do Azure **Observação:** quando você seleciona um tipo de provedor, as seções ponto final do serviço, Autenticação e Verificação do servidor aparecem na parte inferior da página.
Balde ou recipiente	O nome do bucket externo do S3 ou do contêiner do Azure que foi criado para o Cloud Storage Pool. O nome especificado aqui deve corresponder exatamente ao nome do bucket ou do contentor ou a criação do Cloud Storage Pool falhará. Você não pode alterar esse valor depois que o pool de armazenamento em nuvem for salvo.

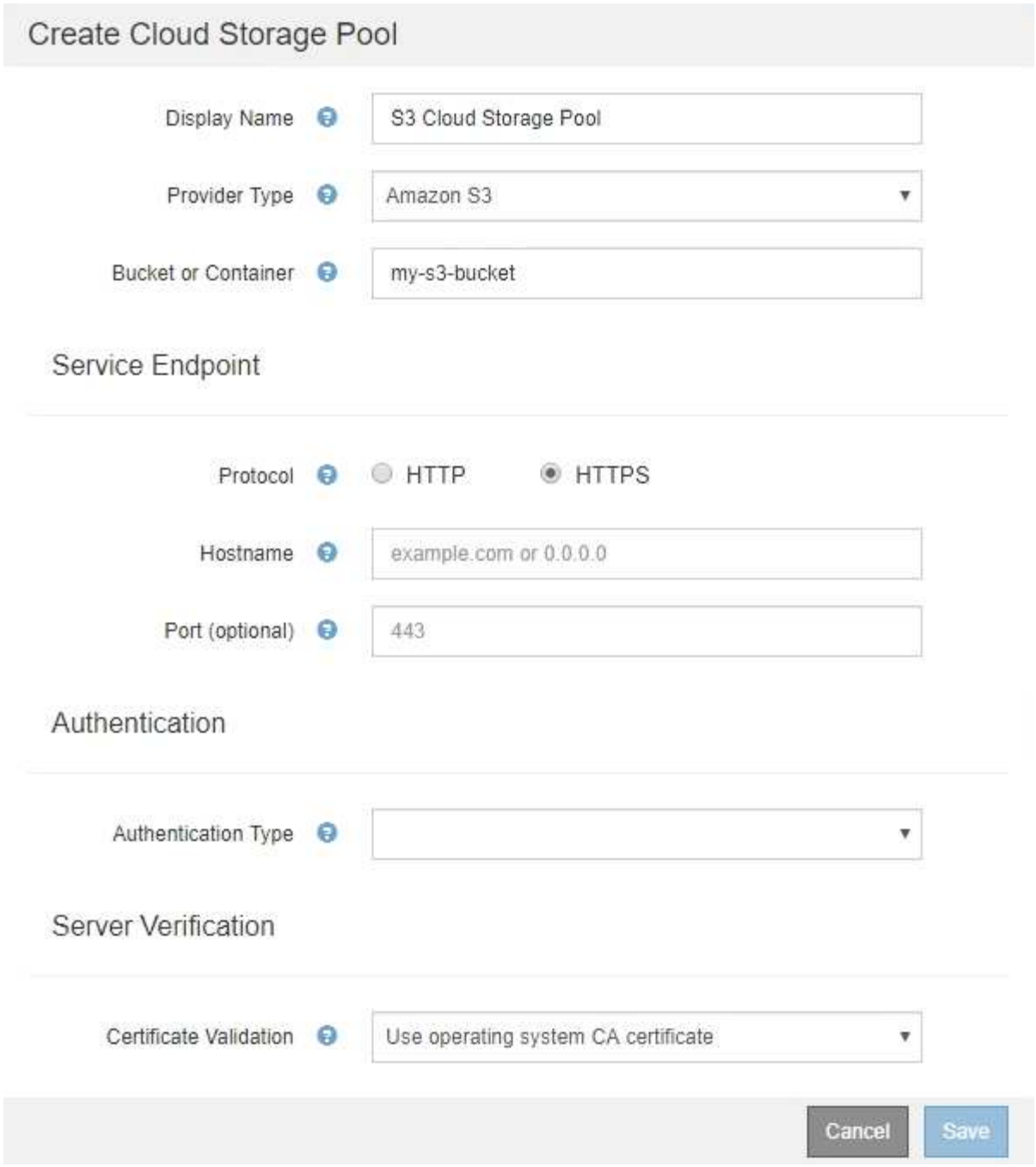
4. Preencha as seções Service Endpoint, Authentication e Server Verification da página, com base no tipo de provedor selecionado.
   - "S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"
   - "C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"
   - "Azure: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"

S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem

Ao criar um pool de armazenamento em nuvem para S3, você deve selecionar o tipo de autenticação necessário para o ponto de extremidade do pool de armazenamento em nuvem. Você pode especificar anônimo ou inserir um ID de chave de acesso e chave de acesso secreta.

O que você vai precisar

- Você deve ter inserido as informações básicas do Cloud Storage Pool e especificado **Amazon S3** como o tipo de provedor.



- Se você estiver usando a autenticação da chave de acesso, você deve saber o ID da chave de acesso e a chave de acesso secreta para o bucket externo do S3.

Passos

1. Na seção **Service Endpoint**, forneça as seguintes informações:

   a. Selecione qual protocolo usar ao se conetar ao pool de armazenamento em nuvem.

      O protocolo padrão é HTTPS.

   b. Insira o nome do host do servidor ou o endereço IP do pool de armazenamento em nuvem.

      Por exemplo:

`s3-aws-region.amazonaws.com`

> Não inclua o nome do intervalo neste campo. Você inclui o nome do bucket no campo **Bucket ou Container**.

a. Opcionalmente, especifique a porta que deve ser usada ao se conetar ao Cloud Storage Pool.

   Deixe este campo em branco para usar a porta padrão: Porta 443 para HTTPS ou porta 80 para HTTP.

2. Na seção **Autenticação**, selecione o tipo de autenticação necessário para o endpoint Cloud Storage Pool.

Opção	Descrição
Chave de acesso	Um ID de chave de acesso e chave de acesso secreta são necessários para acessar o intervalo do pool de armazenamento em nuvem.
Anônimo	Todos têm acesso ao bucket do Cloud Storage Pool. Não é necessário um ID de chave de acesso e uma chave de acesso secreta.
CAP (Portal de Acesso C2S)	Usado apenas para C2S S3. Vá para "C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem".

3. Se tiver selecionado a chave de acesso, introduza as seguintes informações:

Opção	Descrição
ID da chave de acesso	O ID da chave de acesso para a conta que possui o intervalo externo.
Chave de Acesso secreta	A chave de acesso secreto associada.

4. Na seção Verificação do servidor, selecione qual método deve ser usado para validar o certificado para conexões TLS com o pool de armazenamento em nuvem:

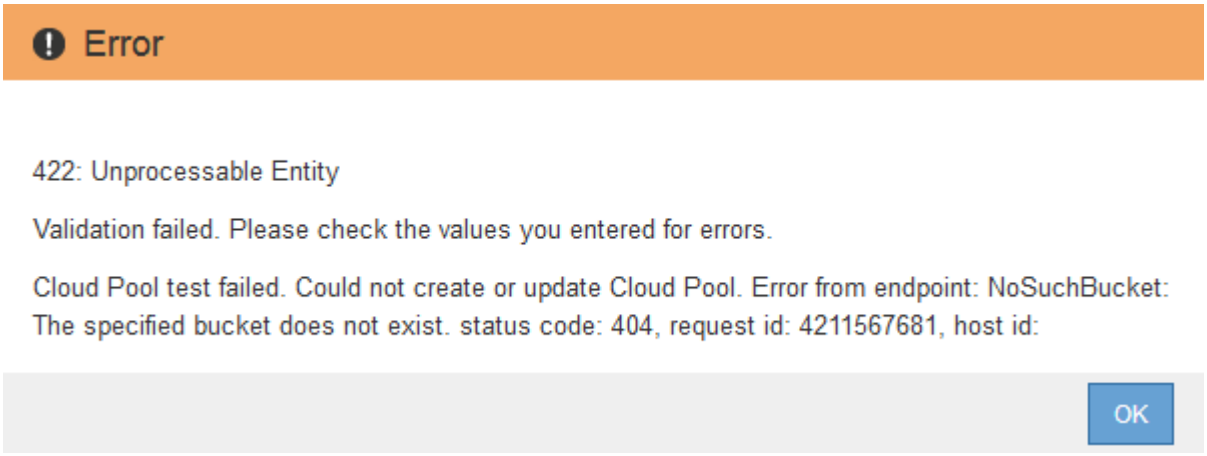
Opção	Descrição
Use o certificado CA do sistema operacional	Use os certificados de CA padrão instalados no sistema operacional para proteger conexões.
Use certificado CA personalizado	Use um certificado de CA personalizado. Clique em **Select New** (Selecionar novo) e carregue o certificado CA codificado em PEM.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado.

5. Clique em **Salvar**.

Quando você salva um pool de storage de nuvem, o StorageGRID faz o seguinte:

- Valida que o intervalo 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 para identificar o bucket como um Cloud Storage Pool. 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 intervalo especificado ainda não existir.



Consulte as instruções para solucionar problemas de pools de armazenamento em nuvem, resolver o problema e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Informações relacionadas

"Solução de problemas de Cloud Storage Pools"

C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem

Para usar o serviço de Serviços comerciais de nuvem (C2S) S3 como um pool de armazenamento em nuvem, você deve configurar o C2S Access Portal (CAP) como o tipo de autenticação, para que a StorageGRID possa solicitar credenciais temporárias para acessar o bucket do S3 na sua conta do C2S.

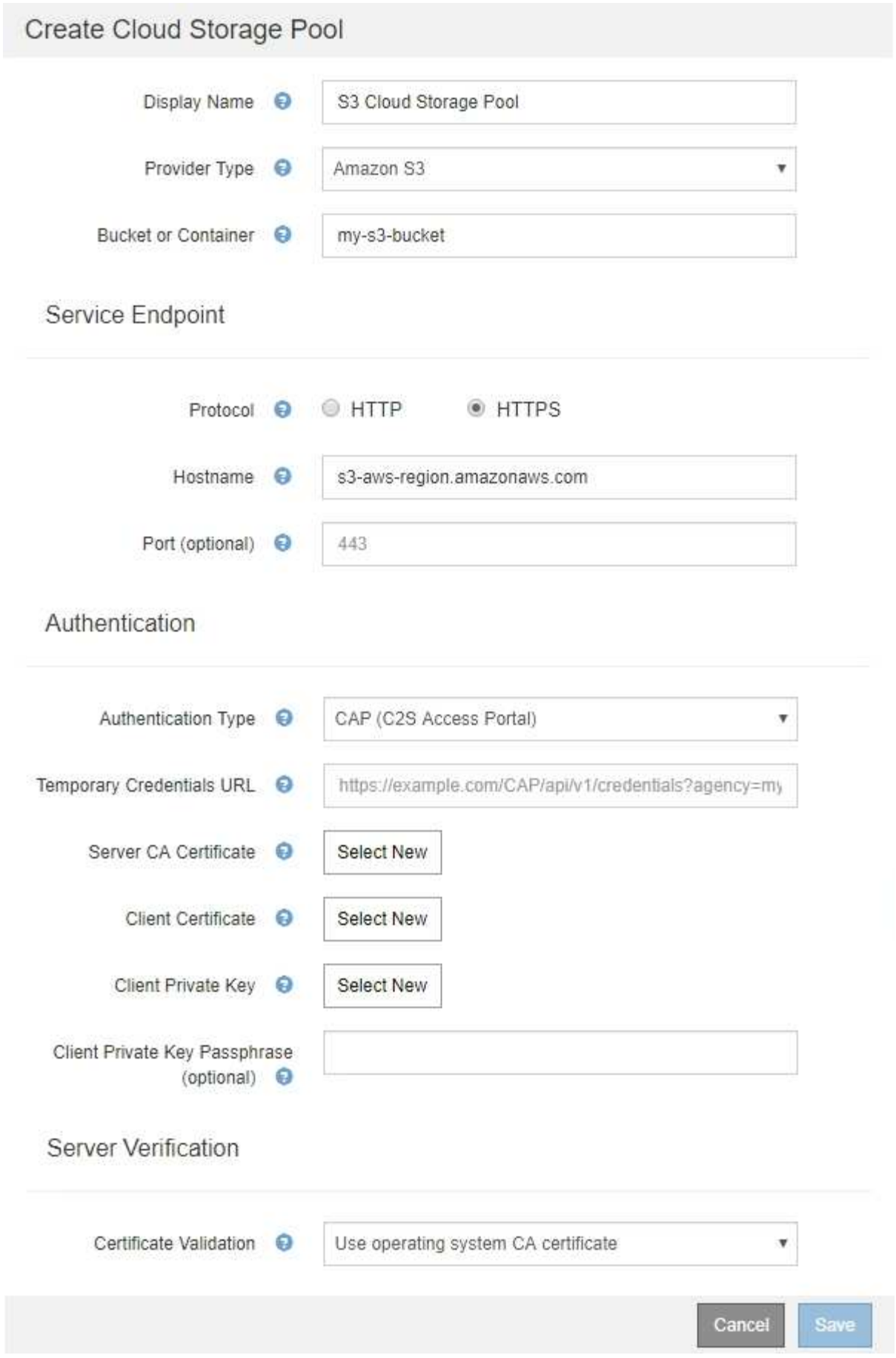
O que você vai precisar

- Você deve ter inserido as informações básicas de um pool de armazenamento em nuvem do Amazon S3, incluindo o endpoint do serviço.
- Você deve saber 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.
- Você deve ter um certificado de CA de servidor emitido por uma autoridade de certificação governamental (CA) apropriada. O StorageGRID usa esse certificado para verificar a identidade do SERVIDOR CAP. O certificado de CA do servidor deve usar a codificação PEM.
- Você deve ter um certificado de cliente emitido por uma autoridade de certificação governamental (CA) apropriada. O StorageGRID usa esse certificado para identificar-se para o servidor CAP. O certificado de cliente deve usar codificação PEM e deve ter acesso à sua conta C2S.
- Você deve ter uma chave privada codificada PEM para o certificado do cliente.
- Se a chave privada do certificado de cliente for encriptada, tem de ter a frase-passe para o desencriptar.

Passos

1. Na seção **Autenticação**, selecione **CAP (C2S Access Portal)** na lista suspensa **Authentication Type**.

   Os campos de autenticação CAP C2S aparecem.


Create Cloud Storage Pool
Display Name
S3 Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-s3-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/credentials?agency=my
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. Forneça as seguintes informações:
   a. Para **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. Para **certificado CA do servidor**, clique em **Selecionar novo** e carregue o certificado CA codificado em PEM que o StorageGRID usará para verificar o servidor CAP.
   c. Para **certificado de cliente**, clique em **Selecionar novo** e carregue o certificado codificado PEM que o StorageGRID usará para se identificar no servidor CAP.
   d. Para **chave privada do cliente**, clique em **Select New** e carregue a chave privada codificada pelo PEM para o certificado do cliente.

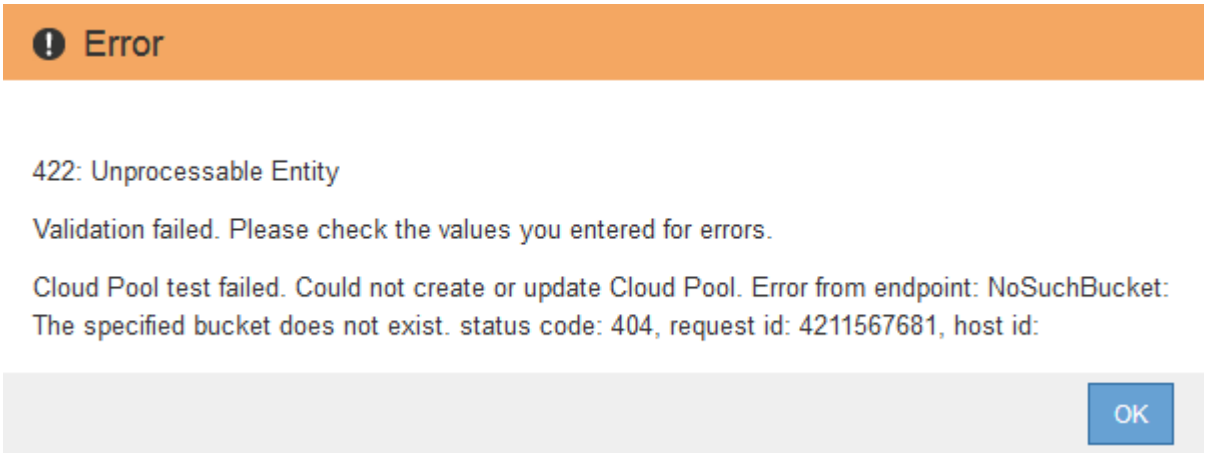
      Se a chave privada for criptografada, o formato tradicional deve ser usado. (O formato criptografado PKCS nº 8 não é suportado.)

   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 **frase-passe de chave privada do cliente** em branco.
3. Na seção Verificação do servidor, forneça as seguintes informações:
   a. Para **Validação de certificado**, selecione **usar certificado CA personalizado**.
   b. Clique em **Select New** (Selecionar novo) e carregue o certificado CA codificado em PEM.
4. Clique em **Salvar**.

Quando você salva um pool de storage de nuvem, o StorageGRID faz o seguinte:

- Valida que o intervalo 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 para identificar o bucket como um Cloud Storage Pool. 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 intervalo especificado ainda não existir.



Consulte as instruções para solucionar problemas de pools de armazenamento em nuvem, resolver o problema e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Informações relacionadas

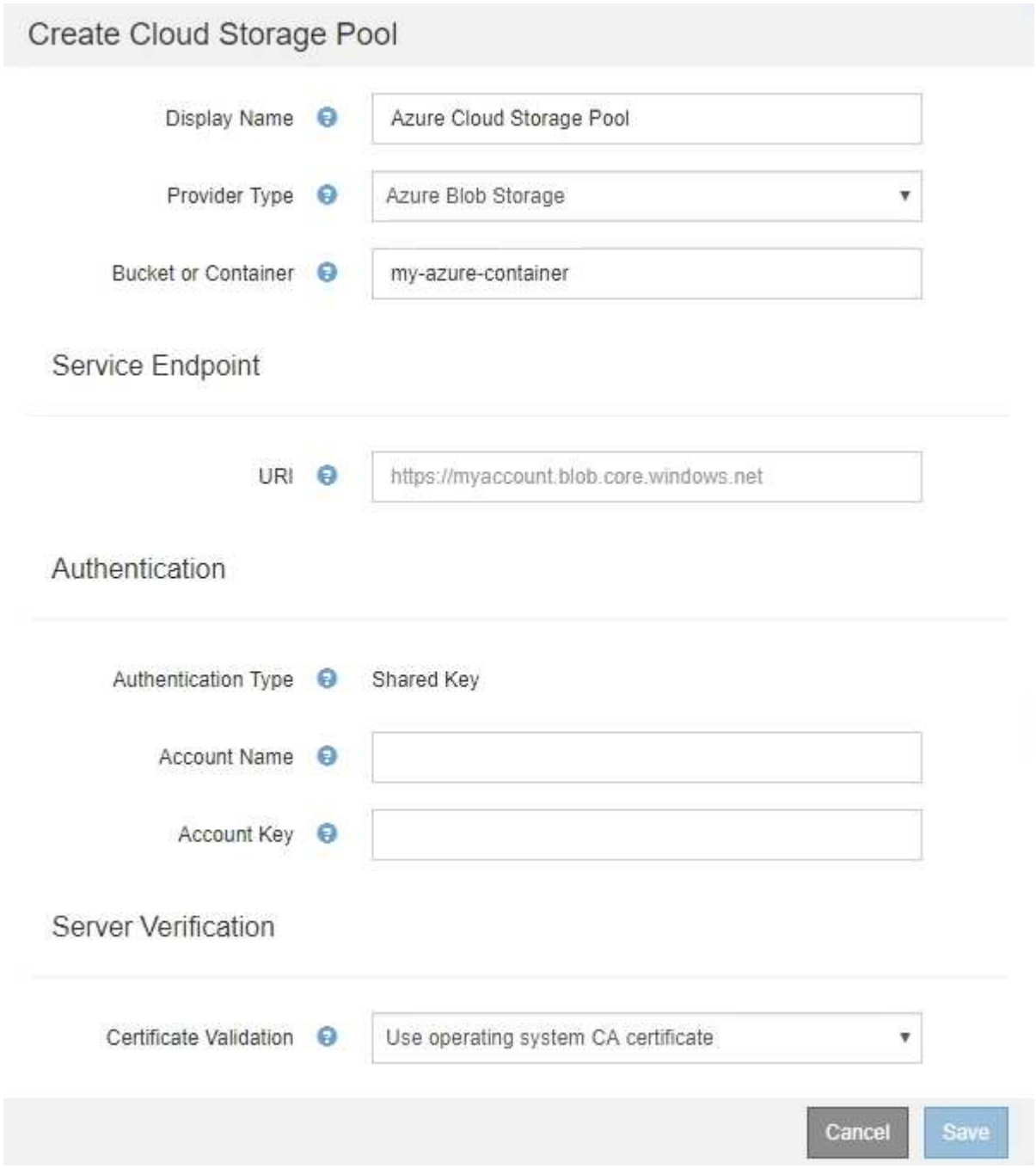
"Solução de problemas de Cloud Storage Pools"

Azure: Especificando detalhes de autenticação para um pool de armazenamento em nuvem

Ao criar um pool de storage de nuvem para storage de Blobs do Azure, você deve especificar um nome de conta e uma chave de conta para o contêiner externo que o StorageGRID usará para armazenar objetos.

O que você vai precisar

- Você precisa ter inserido as informações básicas do Cloud Storage Pool e especificado **armazenamento Blob Azure** como o tipo de provedor. **Chave compartilhada** aparece no campo **tipo de autenticação**.



- Você deve saber o URI (Uniform Resource Identifier) usado para acessar o contentor de armazenamento

de Blob usado para o pool de armazenamento do Cloud Storage.

- Você deve saber o nome da conta de armazenamento e a chave secreta. Você pode usar o portal do Azure para encontrar esses valores.

Passos

1. Na seção **Service Endpoint**, insira o URI (Uniform Resource Identifier) usado para acessar o contentor de armazenamento de Blob usado para o Cloud Storage Pool.

   Especifique o URI em um dos seguintes formatos:

   - `https://host:port`
   - `http://host:port`

   Se você não especificar uma porta, por padrão, a porta 443 será usada para URIs HTTPS e a porta 80 será usada para URIs HTTP. * Exemplo de URI para o contentor de armazenamento Blob do Azure* `https://myaccount.blob.core.windows.net`

2. Na seção **Autenticação**, forneça as seguintes informações:

   a. Para **Nome da conta**, insira o nome da conta de armazenamento Blob que possui o contentor de serviço externo.

   b. Para **chave de conta**, insira a chave secreta da conta de armazenamento Blob.

   Para endpoints do Azure, você deve usar a autenticação chave compartilhada.

3. Na seção **Verificação do servidor**, selecione qual método deve ser usado para validar o certificado para conexões TLS ao pool de armazenamento em nuvem:

Opção	Descrição
Use o certificado CA do sistema operacional	Use os certificados de CA padrão instalados no sistema operacional para proteger conexões.
Use certificado CA personalizado	Use um certificado de CA personalizado. Clique em **Select New** (Selecionar novo) e carregue o certificado codificado PEM.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado.

4. Clique em **Salvar**.

Quando você salva um pool de storage de nuvem, o StorageGRID faz o seguinte:

- Valida que o contentor e o URI existem e que eles podem ser alcançados usando as credenciais que você especificou.
- Grava um arquivo de marcador no contentor para identificá-lo como um Cloud Storage Pool. 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 contentor especificado ainda não existir.

Consulte as instruções para solucionar problemas de pools de armazenamento em nuvem, resolver o problema e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Informações relacionadas

"Solução de problemas de Cloud Storage Pools"

Editando 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.

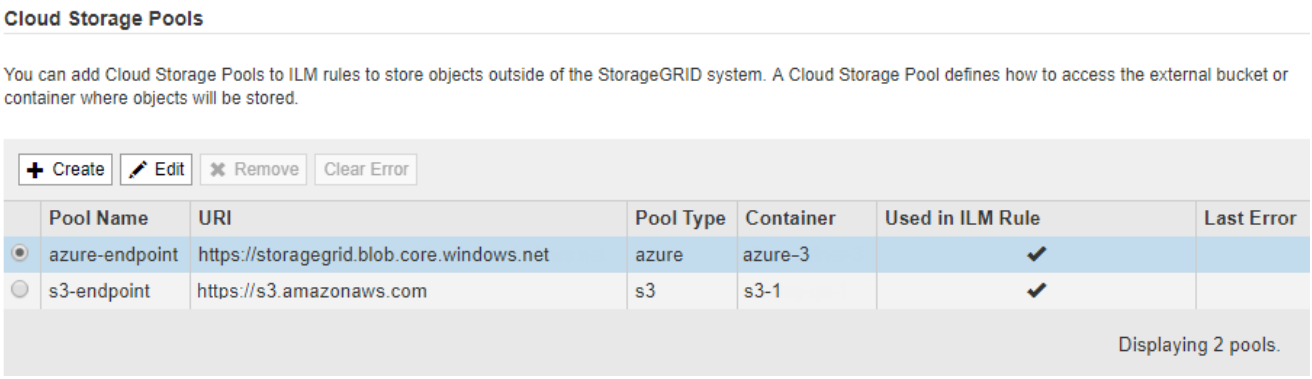
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você precisa ter revisado as diretrizes para configurar os pools de armazenamento em nuvem.

Passos

1. Selecione **ILM** > **Storage Pools**.

   A página conjuntos de armazenamento é exibida. A tabela Cloud Storage Pools lista os pools de armazenamento em nuvem existentes.



2. Selecione o botão de opção do pool de armazenamento em nuvem que você deseja editar.
3. Clique em **Editar**.
4. Conforme necessário, altere o nome de exibição, o ponto de extremidade do serviço, as credenciais de autenticação ou o método de validação do certificado.

   > Você não pode 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, você pode selecionar **Exibir atual** para revisar o certificado que está atualmente em uso.

5. Clique em **Salvar**.

   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 para solucionar problemas de pools de armazenamento em nuvem, resolver o problema e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Informações relacionadas

"Considerações para pools de storage em nuvem"

"Solução de problemas de Cloud Storage Pools"

Removendo um pool de armazenamento em nuvem

Você pode remover um pool de armazenamento em nuvem que não seja usado em uma regra ILM e que não contenha dados de objeto.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- 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. Consulte ""solução de problemas de pools de armazenamento em nuvem"".

> 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 .

- Você já removeu quaisquer regras ILM que possam ter usado o pool.

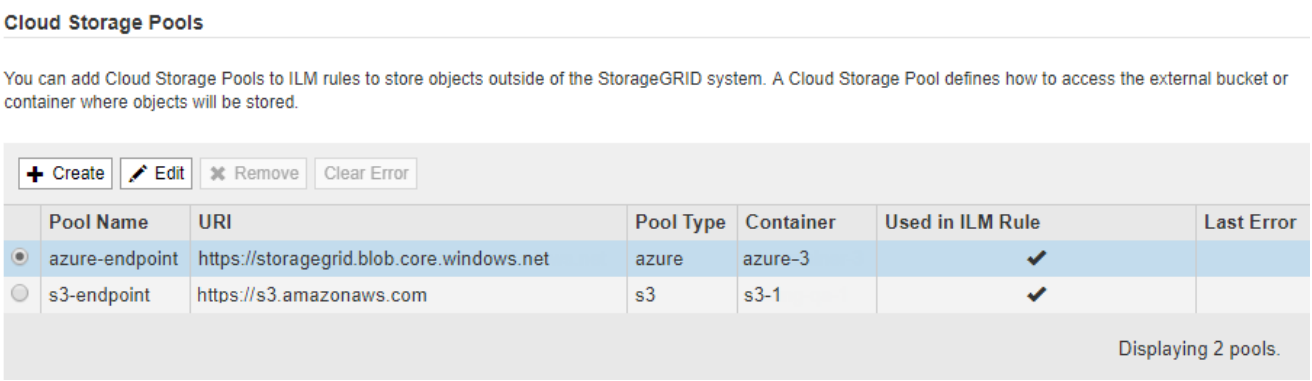
Passos

1. Selecione **ILM** > **Storage Pools**.

   A página conjuntos de armazenamento é exibida.

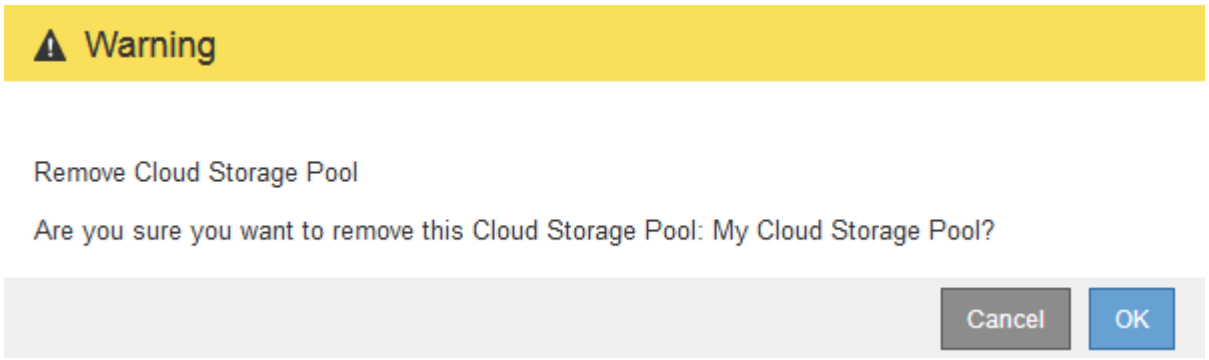
2. Selecione o botão de opção para um pool de armazenamento em nuvem que não é usado atualmente em uma regra ILM.

   Você não pode remover um pool de armazenamento em nuvem se ele for usado em uma regra ILM. O botão **Remove** está desativado.



3. Clique em **Remover**.

   É apresentado um aviso de confirmação.



4. Clique em **OK**.

   O pool de armazenamento em nuvem é removido.

Informações relacionadas

"Solução de problemas de Cloud Storage Pools"

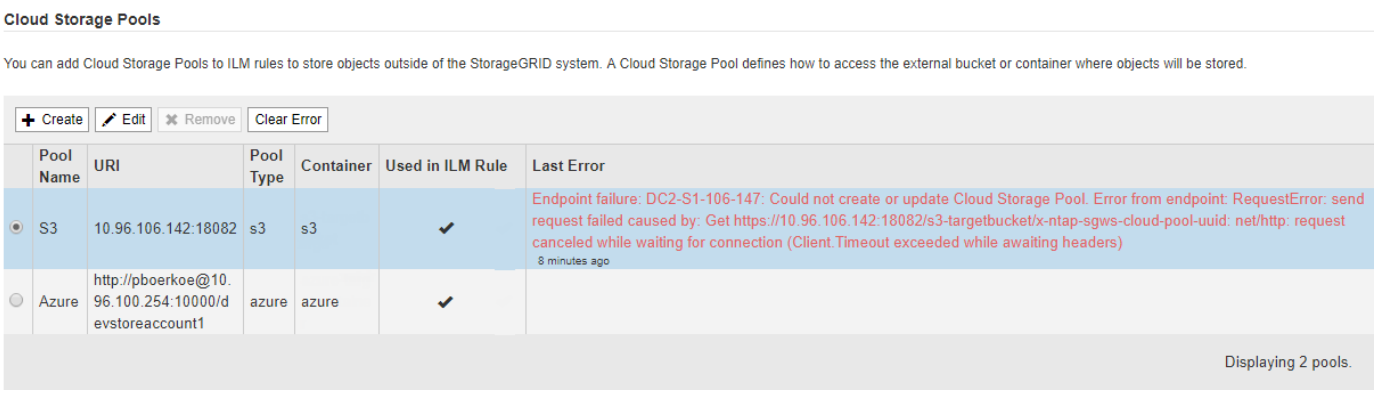
Solução de problemas de Cloud Storage Pools

Se você encontrar erros ao criar, editar ou excluir um pool de armazenamento em nuvem, siga estas etapas de solução de problemas para ajudar a resolver o problema.

Determinar se ocorreu um erro

O StorageGRID executa uma verificação simples de integridade em cada pool de armazenamento em nuvem uma vez por minuto para garantir que o pool de armazenamento em nuvem possa ser acessado e que ele esteja funcionando corretamente. Se a 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.

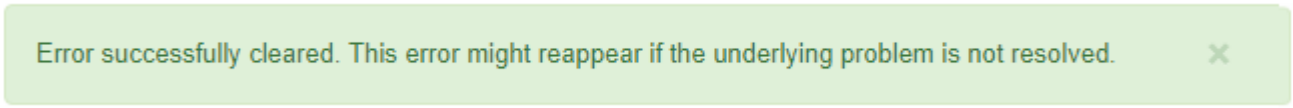


Além disso, um alerta de **erro de conetividade do Cloud Storage Pool** é acionado se a verificação de integridade detetar que um ou mais novos erros do Cloud Storage Pool ocorreram nos últimos 5 minutos. Se você receber uma notificação por e-mail para esse alerta, vá para a página conjunto de armazenamento (selecione **ILM** > **pools de armazenamento**), revise as mensagens de erro na coluna último erro e consulte

as diretrizes de solução de problemas abaixo.

Verificar 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 botão de opção para o endpoint e clique em **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 tiver sido corrigido (ou se for encontrado um erro diferente), a mensagem de erro será mostrada na coluna último erro dentro de alguns minutos.

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. Este erro ocorre se o intervalo ou recipiente incluir o `x-ntap-sgws-cloud-pool-uuid` arquivo marcador, mas esse arquivo não tiver 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 o `x-ntap-sgws-cloud-pool-uuid` arquivo e tente configurar o pool de armazenamento em nuvem novamente.

Erro: Não foi possível criar ou atualizar o Cloud Storage Pool. Erro do endpoint

Você pode encontrar esse erro ao tentar criar ou editar um pool de armazenamento em nuvem. Esse erro indica que algum tipo de 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 o protocolo 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.
- 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 pool de armazenamento em nuvem se ele contiver dados movidos pelo ILM, dados que estavam no bucket antes de configurar o pool de armazenamento em nuvem ou dados que foram colocados no bucket por outra fonte após a criação do pool de armazenamento em nuvem.

Tente um ou mais destes passos para corrigir o problema:

- Siga as instruções para mover objetos de volta para o StorageGRID no "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 pool de armazenamento em nuvem. Esse erro ocorre se o servidor proxy externo não puder alcançar o endpoint 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.

Informações relacionadas

"Ciclo de vida de um objeto Cloud Storage Pool"

Configurando perfis de codificação de apagamento

Você configura os perfis de codificação de apagamento associando um pool de storage a um esquema de codificação de apagamento, como 6-3. Em seguida, ao configurar as instruções de colocação para uma regra ILM, você pode selecionar o perfil de codificação de apagamento. Se um objeto corresponder à regra, os dados e fragmentos de paridade serão criados e distribuídos para os locais de storage no pool de storage de acordo com o esquema de codificação de apagamento.

- "Criando um perfil de codificação de apagamento"
- "Renomeando um perfil de codificação de apagamento"
- "Desativar um perfil de codificação de apagamento"

Criando um perfil de codificação de apagamento

Para criar um perfil de codificação de apagamento, você associa um pool de storage que contém nós de storage a um esquema de codificação de apagamento. Essa associação determina o número de dados e fragmentos de paridade criados e onde o sistema distribui esses fragmentos.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você precisa criar um pool de storage que inclua exatamente um local ou um pool de storage que inclua três ou mais locais. Não há esquemas de codificação de apagamento disponíveis para um pool de storage que tenha apenas dois locais.

Sobre esta tarefa

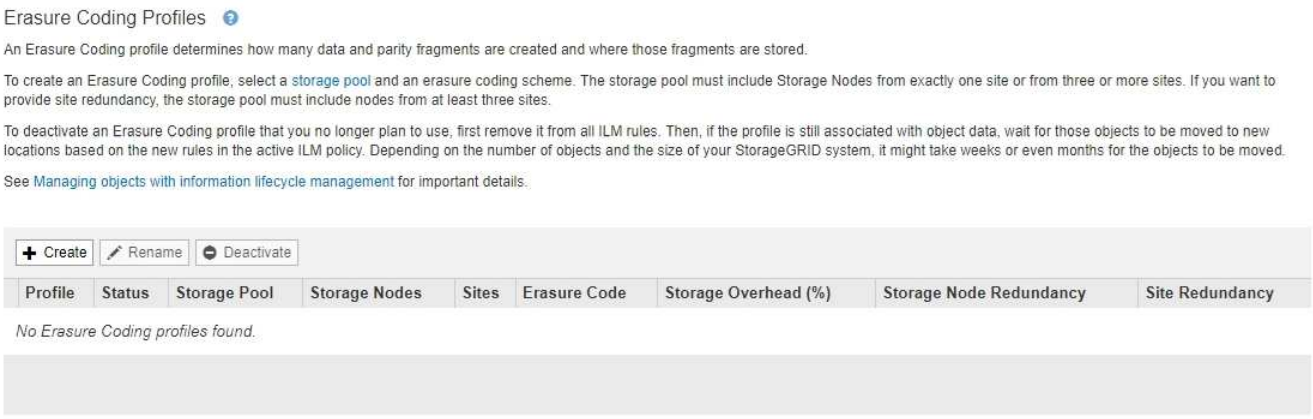
Os pools de storage usados nos perfis de codificação de apagamento devem incluir exatamente um local ou três ou mais locais. Se você quiser fornecer redundância de site, o pool de armazenamento deve ter pelo menos três locais.

> Você deve selecionar um pool de storage que contenha nós de storage. Você não pode usar nós de arquivamento para dados codificados por apagamento.

Passos

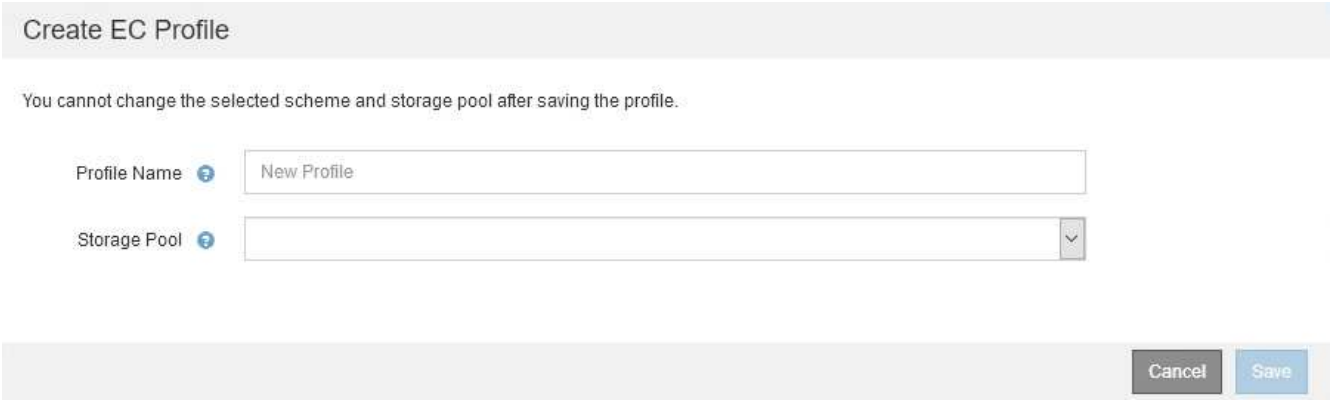
1. Selecione **ILM** > **Codificação de apagamento**.

A página Perfis de codificação de apagamento é exibida.



2. Clique em **criar**.

A caixa de diálogo criar perfil EC é exibida.



3. Introduza um nome exclusivo para o perfil de codificação de apagamento.

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.

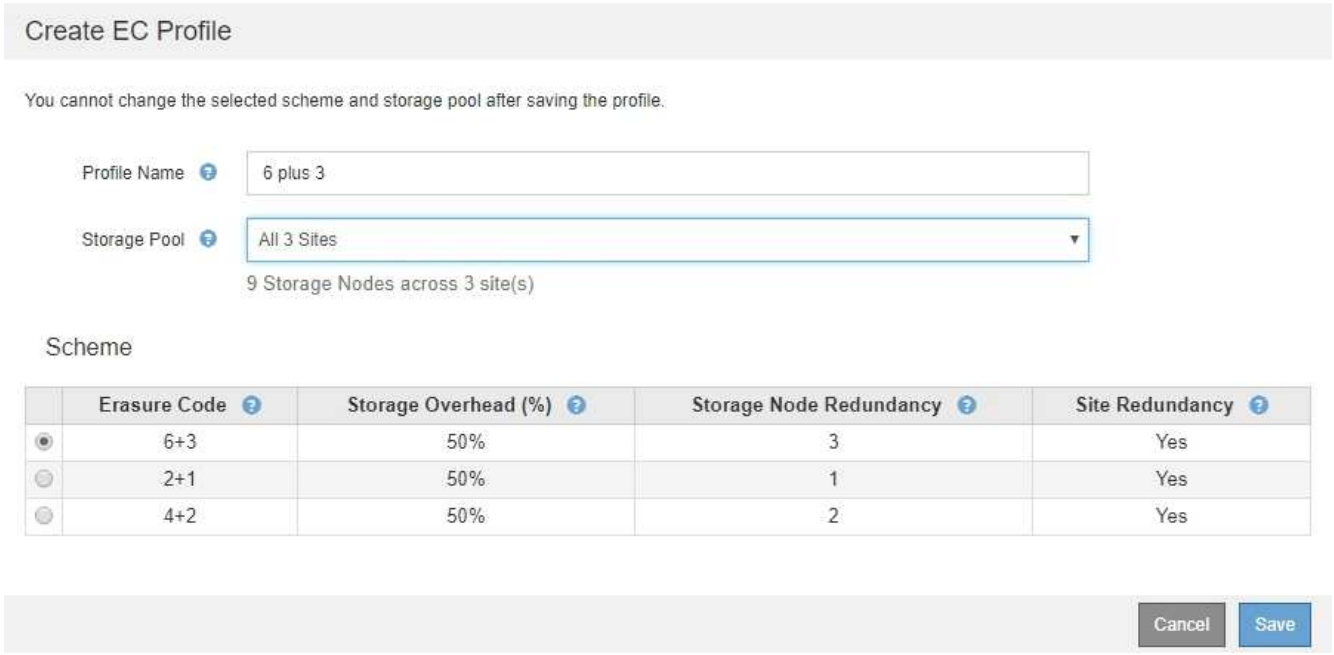
> O nome do perfil de codificação de apagamento é anexado ao nome do pool de armazenamento na instrução de colocação de uma regra ILM.

4. Selecione o pool de armazenamento que você criou para esse perfil de codificação de apagamento.

> Se a grade incluir apenas um local no momento, você será impedido de usar o pool de storage padrão, todos os nós de storage ou qualquer pool de storage que inclua o site padrão, todos os sites. Esse comportamento impede que o perfil de codificação de apagamento se torne inválido se um segundo site for adicionado.

Se um pool de armazenamento incluir exatamente dois locais, 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.

Quando você seleciona um pool de storage, a lista de esquemas de codificação de apagamento disponíveis é exibida, com base no número de nós de storage e sites no pool.



As seguintes informações são listadas para cada esquema de codificação de apagamento disponível:

- **Código de apagamento**: O nome do esquema de codificação de apagamento no seguinte formato: Fragmentos de dados e fragmentos de paridade.
- * Sobrecarga de armazenamento (%)*: O armazenamento adicional necessário para fragmentos de paridade em relação ao tamanho de dados do objeto. Sobrecarga de armazenamento: Número total de fragmentos de paridade / número total de fragmentos de dados.
- **Redundância do nó de storage**: O número de nós de storage que podem ser perdidos, mantendo a capacidade de recuperar dados de objeto.
- **Redundância do site**: Se o código de apagamento selecionado permite que os dados do objeto sejam recuperados se um site for perdido.

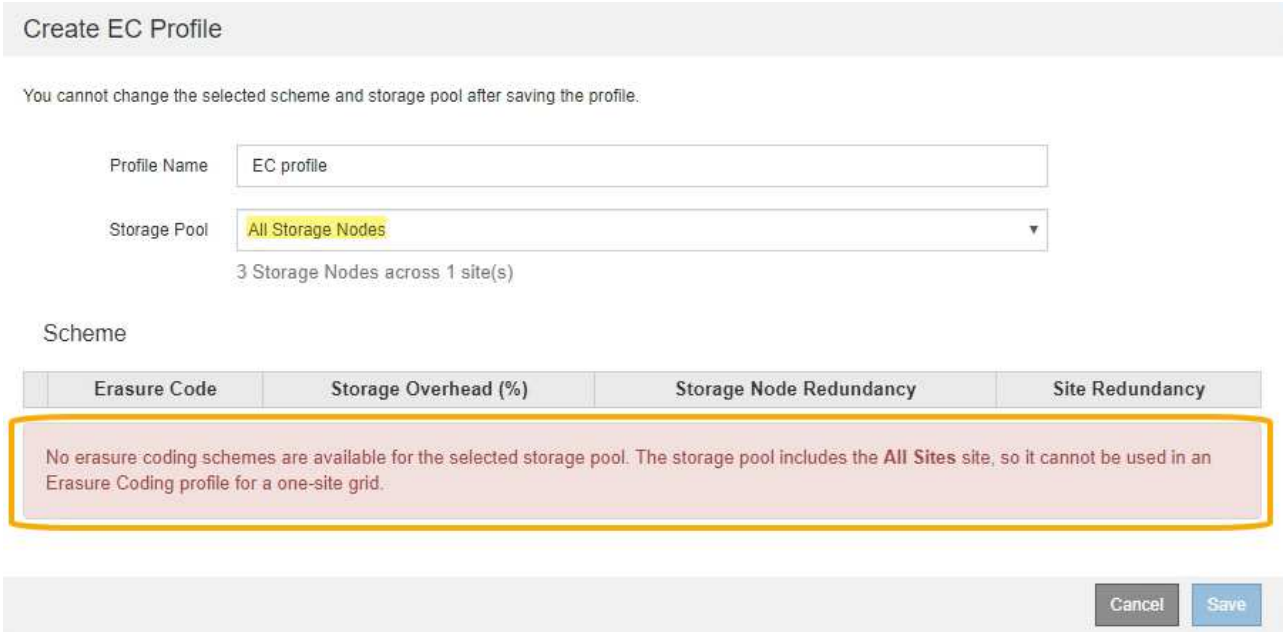
  Para dar suporte à redundância de sites, o pool de storage selecionado deve incluir vários locais, cada um com nós de storage suficientes para permitir que qualquer site seja perdido. Por exemplo, para oferecer suporte à redundância de sites usando um 6 esquema de codificação de apagamento de mais de 3 horas por dia, o pool de storage selecionado deve incluir pelo menos três locais com pelo menos três nós de storage em cada local.

  As mensagens são exibidas nestes casos:

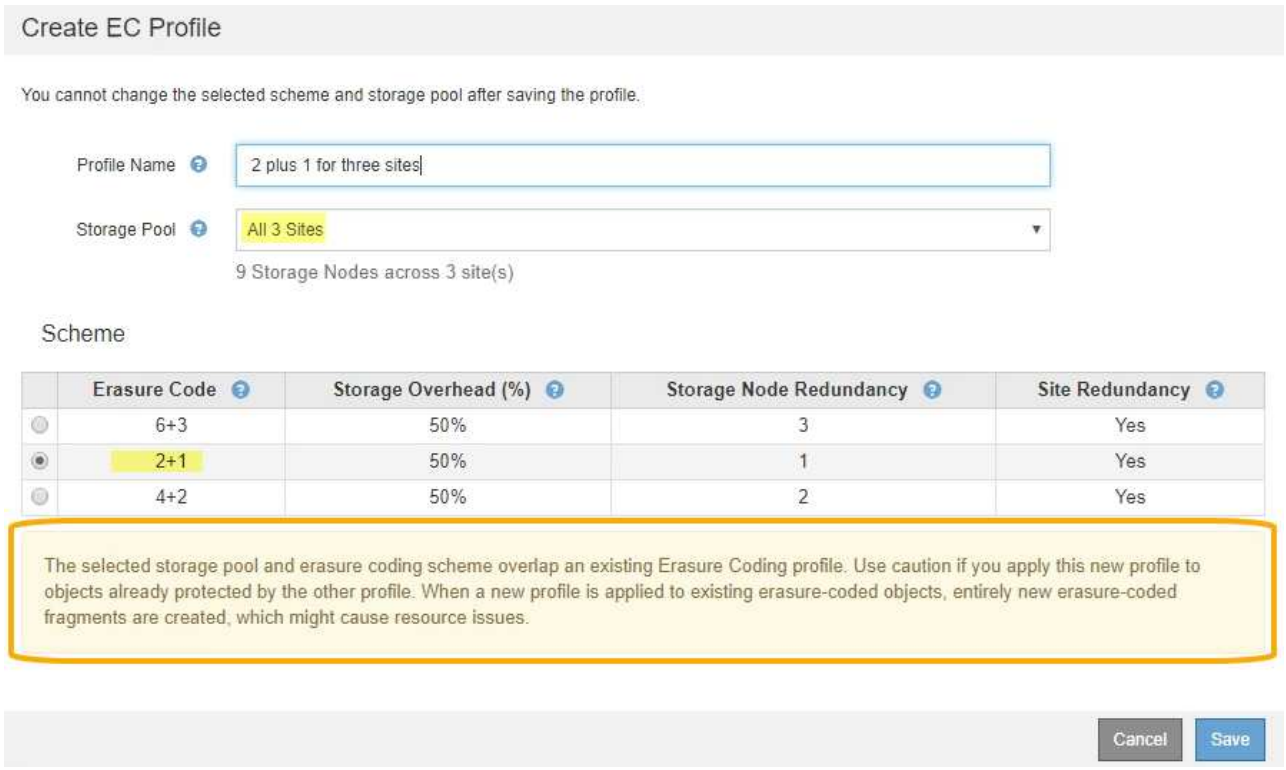
- O pool de armazenamento selecionado não fornece redundância de site. A mensagem a seguir é esperada quando o pool de armazenamento selecionado inclui apenas um local. Você pode usar esse perfil de codificação de apagamento nas regras do ILM para proteger contra falhas de nós.

- O pool de storage selecionado não atende aos requisitos de qualquer esquema de codificação de apagamento. Por exemplo, a seguinte mensagem é esperada quando o pool de armazenamento selecionado inclui exatamente dois locais. Para usar a codificação de apagamento para proteger os dados de objetos, selecione um pool de storage com exatamente um local ou um pool de storage com três ou mais locais.

- Sua grade inclui apenas um local e você selecionou o pool de storage padrão, todos os nós de storage ou qualquer pool de storage que inclua o local padrão, todos os sites.



- O esquema de codificação de apagamento e o pool de storage selecionado se sobrepõem a outro perfil de codificação de apagamento.



Neste exemplo, uma mensagem de aviso aparece porque outro perfil de codificação de apagamento está usando o esquema 2-1 e o conjunto de armazenamento para o outro perfil também usa um dos sites no conjunto de armazenamento de todos os 3 sites.

Embora você não seja impedido de criar este novo perfil, você deve ter muito cuidado ao começar a usá-lo na política ILM. Se esse novo perfil for aplicado a objetos codificados de apagamento já protegidos pelo outro perfil, o StorageGRID criará um conjunto totalmente novo de fragmentos de objeto. Ele não reutilizará os 2 fragmentos existentes. 1. Problemas de recursos podem ocorrer quando você migra de um perfil de codificação de apagamento para o outro, mesmo que os esquemas de codificação de apagamento sejam os mesmos.

5. Se mais de um esquema de codificação de apagamento estiver listado, selecione o que deseja usar.

   Ao decidir qual esquema de codificação de apagamento usar, você deve equilibrar a tolerância a falhas (alcançada por ter mais segmentos de paridade) com os requisitos de tráfego de rede para reparos (mais fragmentos equivale a mais tráfego de rede). Por exemplo, ao decidir entre um esquema 4-2 e um esquema 6-3, selecione o esquema 6-3 se forem necessárias paridade adicional e tolerância a falhas. Selecione o esquema 4 mais 2 se os recursos de rede forem restritos para reduzir o uso da rede durante reparos de nó.

6. Clique em **Salvar**.

Renomeando 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.

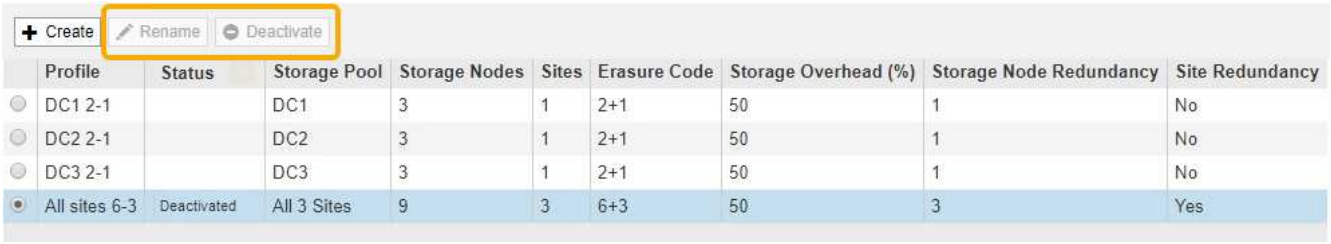
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **ILM** > **Codificação de apagamento**.

   A página Perfis de codificação de apagamento é exibida. Os botões **Renomear** e **Desativar** estão desativados.



	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
○	DC1 2-1		DC1	3	1	2+1	50	1	No
○	DC2 2-1		DC2	3	1	2+1	50	1	No
○	DC3 2-1		DC3	3	1	2+1	50	1	No
◉	All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

2. Selecione o perfil que deseja renomear.

   Os botões **Renomear** e **Desativar** ficam ativados.

3. Clique em **Renomear**.

   A caixa de diálogo Renomear perfil EC é exibida.

4. Introduza 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. Clique em **Salvar**.

Desativar um perfil de codificação de apagamento

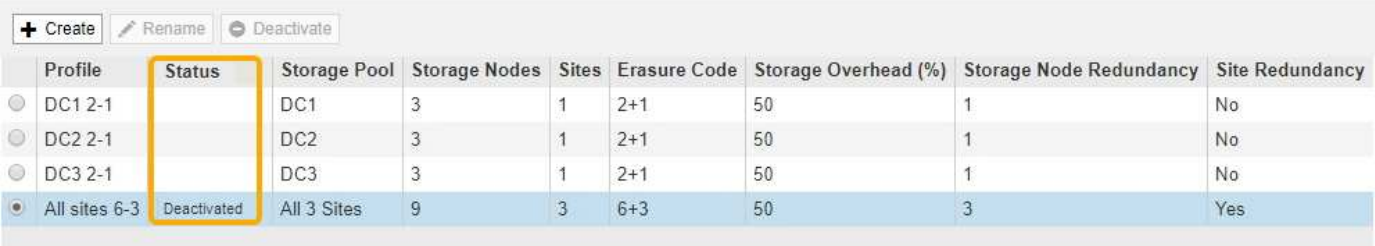
Você pode desativar um perfil de codificação de apagamento se você não planeja mais usá-lo e se o perfil não for usado atualmente em nenhuma regra de ILM.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter confirmado que nenhuma operação de reparo de dados codificados de apagamento ou procedimentos de desativação estão em andamento. Uma mensagem de erro é retornada se você tentar desativar um perfil de codificação de apagamento enquanto qualquer uma dessas operações estiver em andamento.

Sobre esta tarefa

Quando você desativa um perfil de codificação de apagamento, o perfil ainda aparece na página Perfis de codificação de apagamento, mas seu status é **desativado**.



Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

Já não pode utilizar um perfil de codificação de apagamento que tenha sido desativado. Um perfil desativado não é exibido quando você cria as instruções de colocação para uma regra ILM. Não é possível reativar um perfil desativado.

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 objeto e fragmentos de paridade para o perfil ainda existem.

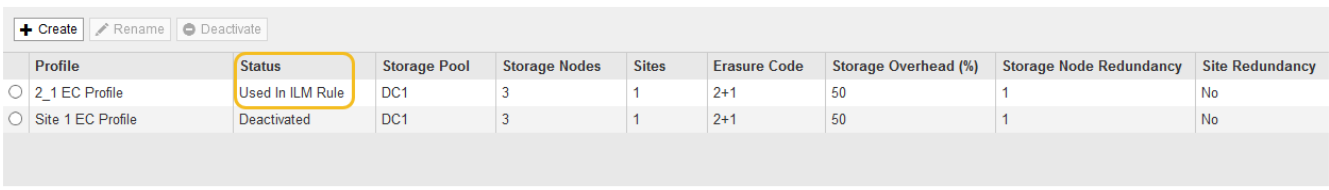
Passos

1. Selecione **ILM** > **Codificação de apagamento**.

   A página Perfis de codificação de apagamento é exibida. Os botões **Renomear** e **Desativar** estão desativados.

2. 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 **2_1 EC Profile** é usado em pelo menos uma regra ILM.



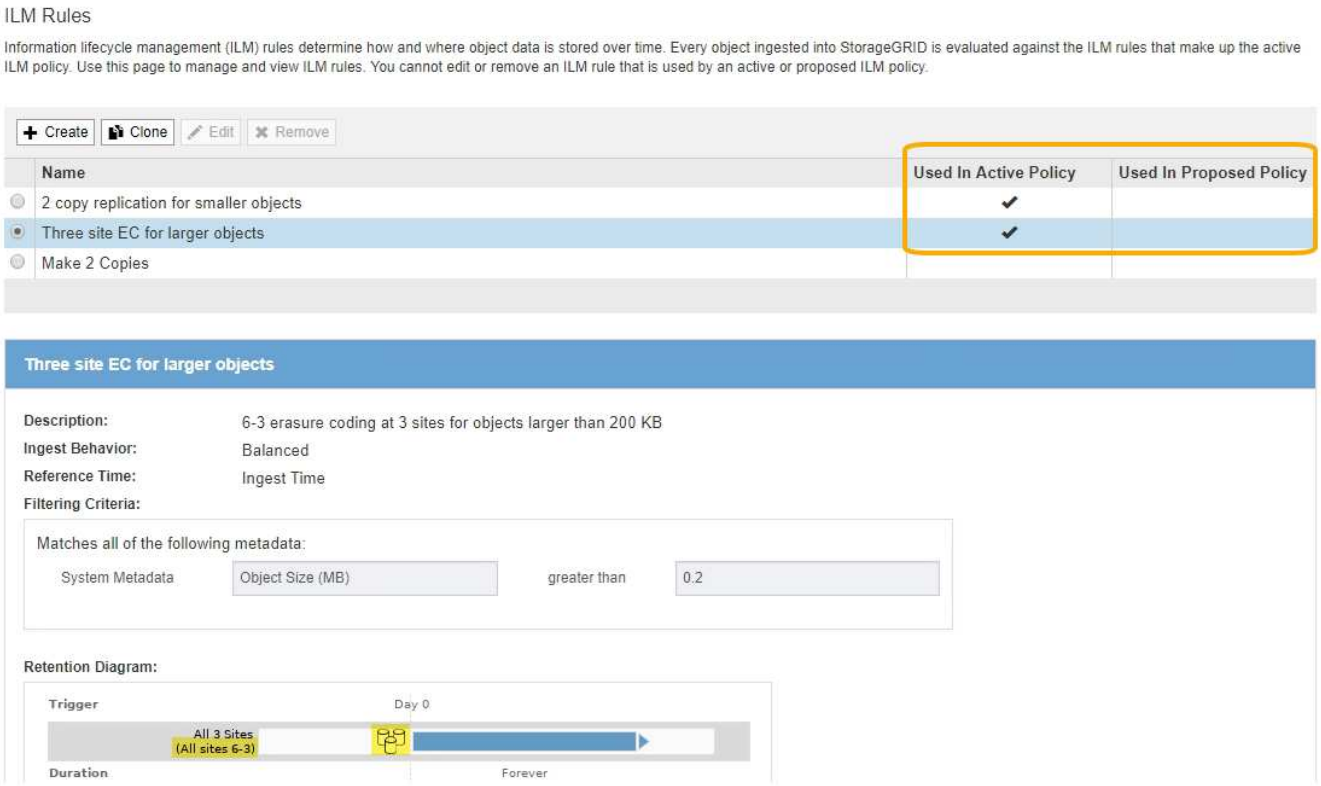
Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No
Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No

3. Se o perfil for usado em uma regra ILM, siga estas etapas:

   a. Selecione **ILM** > **regras**.

b. Para cada regra listada, selecione o botão de opção e revise o diagrama de retenção para determinar se a regra usa o perfil de codificação de apagamento que você deseja desativar.

   No exemplo, a regra **Three site EC para objetos maiores** usa um pool de armazenamento chamado **All 3 Sites** e o perfil **All Sites 6-3** Erasure Coding. Os perfis de codificação de apagamento são representados por este ícone:



a. Se a regra ILM usar o perfil de codificação de apagamento que você deseja desativar, determine se a regra é usada na política ILM ativa ou em uma política proposta.

   No exemplo, a regra **Three site EC para objetos maiores** é usada na política ILM ativa.

b. 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.	*none*
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.	"Trabalhando com regras de ILM e políticas de 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 na política ILM ativa	i. Clonar a política ativa. 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 com segurança um perfil de codificação de apagamento 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.	• "Criando uma política ILM" • "Trabalhando com regras de ILM e políticas de ILM"
Em uma regra ILM que está atualmente em uma política de ILM proposta	i. Edite a política proposta. 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 proposta. 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.	• "Criando uma política ILM" • "Trabalhando com regras de ILM e políticas de 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 em uma política ILM histórica	i. Edite ou exclua a regra. Se você editar a regra, remova todos os canais que usam o perfil de codificação de apagamento. (A regra agora aparecerá como uma regra histórica na política histórica.) ii. Continue com este procedimento.	• "Trabalhando com regras de ILM e políticas de ILM"

c. 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 EC é exibida.

5. Se tiver a certeza de que pretende desativar o perfil, selecione **Desativar**.
   - 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.
   - 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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 projetar uma regra que se aplica apenas a objetos em buckets do S3 criados na região US-West-2. 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 baldes são considerados como pertencentes à região US-East-1.
- 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 e devem conter pelo menos 2 e não mais de 32 carateres. Os carateres válidos são números, letras e hífens.

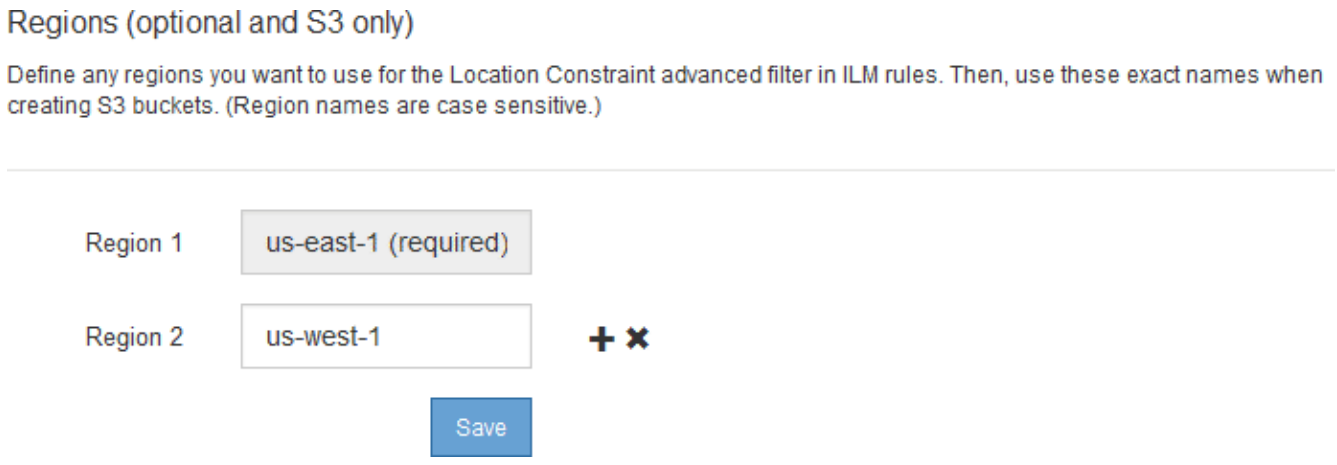
> ⓘ A UE não é considerada um apelido para a ue-oeste-1. Se você quiser usar a região da UE ou da ue-oeste-1, você deve usar o nome exato.

- Não é possível excluir ou modificar uma região se ela for usada atualmente na política ILM ativa ou na política ILM proposta.
- Se a região usada como filtro avançado em uma regra ILM for inválida, ainda será possível adicionar essa regra à política proposta. No entanto, um erro ocorre se você tentar salvar ou ativar a política proposta. (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.

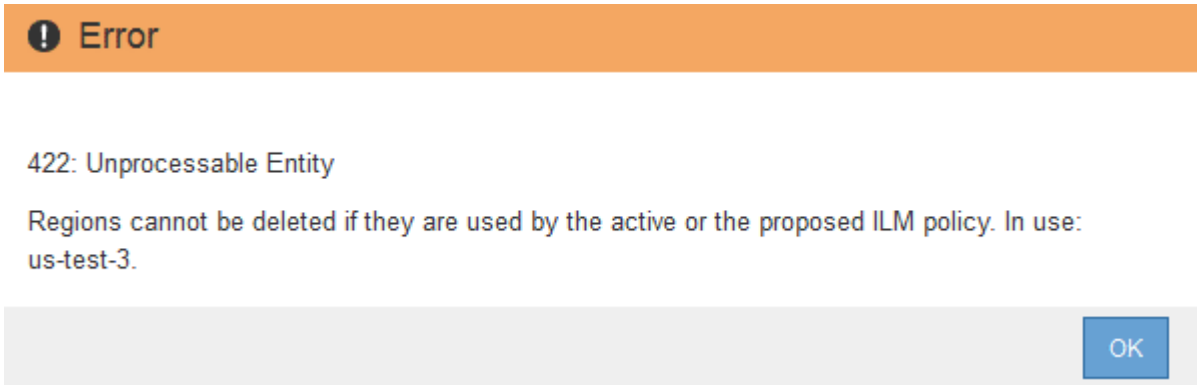


2. Para adicionar uma região:
   a. Clique no ícone de inserção ➕à direita da última entrada.
   b. Insira o nome de uma região que você deseja usar ao criar buckets do S3.

      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, clique no ícone de exclusão ✖.

   Uma mensagem de erro será exibida se você tentar remover uma região atualmente usada na política ativa ou na política proposta.



4. Quando terminar de fazer alterações, clique em **Salvar**.

   Agora você pode selecionar essas regiões na lista **restrição de localização** na página filtragem avançada do assistente criar regra ILM.

Informações relacionadas

"Usando filtros avançados em regras ILM"

Criando 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 regra ILM.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Se você quiser especificar a que contas de inquilino esta regra se aplica, você deve ter a permissão Contas de locatário ou você deve saber o ID da conta para 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 por bucket para S3 ou por container para Swift.
- Se você estiver criando cópias replicadas, terá que ter configurado todos os pools de storage ou pools de storage em nuvem que você planeja usar.
- Se estiver criando cópias codificadas para apagamento, você deverá ter configurado um perfil de codificação de apagamento.
- Você deve estar familiarizado com o "opções de proteção de dados para ingestão".

- Se você precisar criar uma regra compatível para usar com o bloqueio de objetos S3, você deve estar familiarizado com o "Requisitos para o bloqueio de objetos S3".

> Para criar a regra ILM padrão para uma política, use este procedimento em vez disso: "Criando uma regra ILM padrão".

Sobre esta tarefa

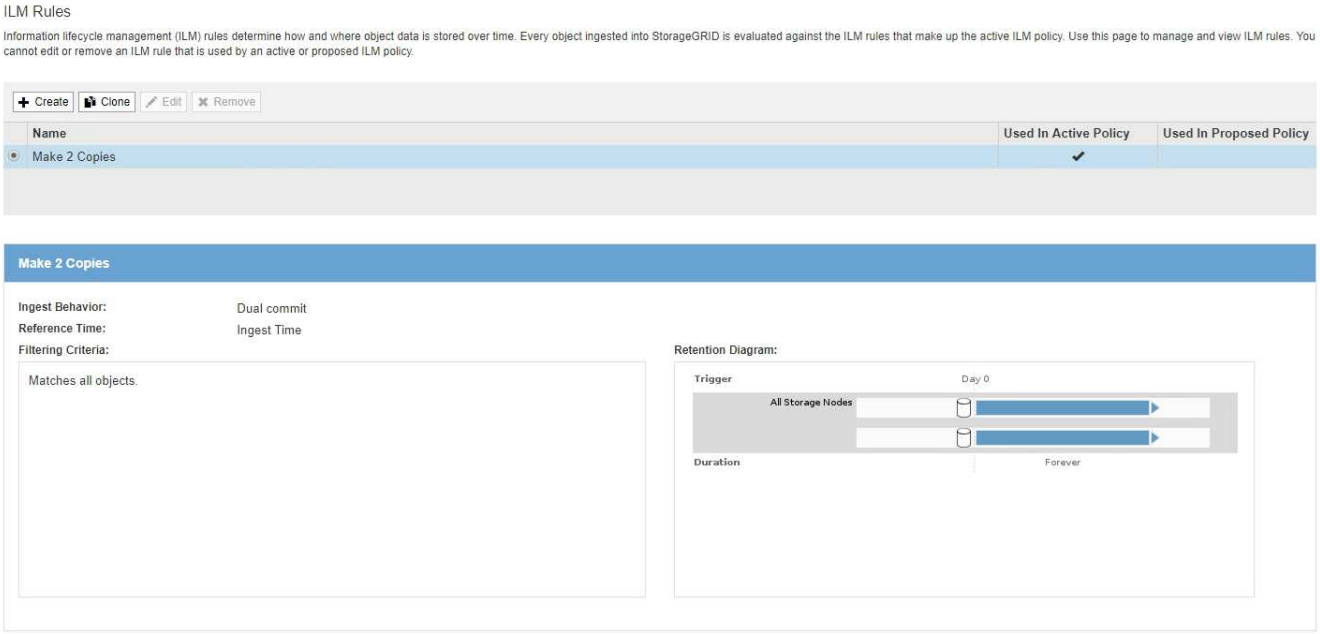
Ao criar regras ILM:

- 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 usar para a opção de proteção de dados na ingestão (Balanced, strict ou Dual Commit)

Passos

1. Selecione **ILM** > **regras**.

   A página ILM Rules (regras do ILM) é exibida, com a regra de estoque, faça 2 cópias, selecionadas.



> A página regras do ILM parece um pouco diferente se a configuração global de bloqueio de objetos do S3 tiver sido ativada para o sistema StorageGRID. A tabela de resumo inclui uma coluna **compliant** e os detalhes da regra selecionada incluem um campo **compliant**.

2. Selecione **criar**.

   A etapa 1 (Definir noções básicas) do assistente criar regra ILM é exibida. Você usa a página Definir noções básicas para definir quais objetos a regra se aplica.

Informações relacionadas

"Use S3"

"Use Swift"

"Configurando perfis de codificação de apagamento"

"Configurando pools de armazenamento"

"Usando Cloud Storage Pools"

"Opções de proteção de dados para ingestão"

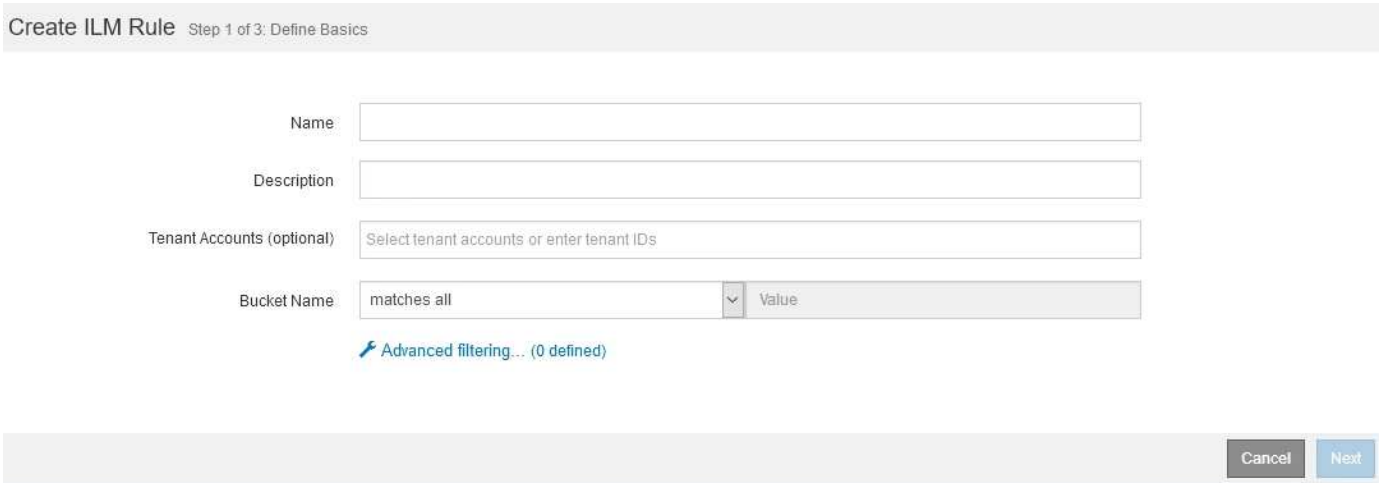
"Gerenciando objetos com o S3 Object Lock"

Passo 1 de 3: Defina o básico

A etapa 1 (Definir noções básicas) do assistente criar regra ILM permite definir os filtros básicos e avançados da regra.

Sobre esta tarefa

Ao avaliar um objeto em relação a uma 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.



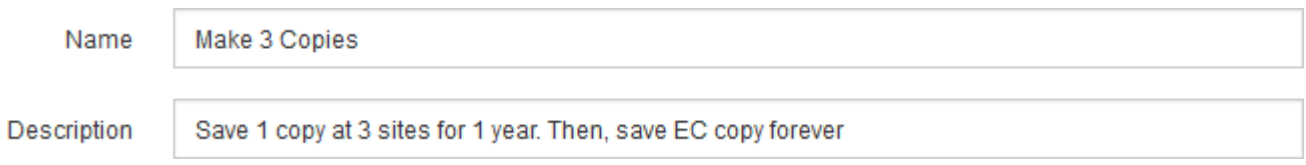
Passos

1. Digite um nome exclusivo para a regra no campo **Nome**.

   Tem de introduzir entre 1 e 64 carateres.

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 ou Swift 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 poderá 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 S3 ou os contentores Swift aos quais esta regra se aplica.

   Se **Matches All** estiver selecionado (padrão), a regra se aplica a todos os buckets do S3 ou contentores Swift.

5. Opcionalmente, selecione **filtragem avançada** para especificar filtros adicionais.

   Se você não configurar a filtragem avançada, a regra se aplica a todos os objetos que correspondem aos filtros básicos.

   > Se esta regra criar cópias codificadas por apagamento, selecione **filtragem avançada**. Em seguida, adicione o filtro avançado **Object Size (MB)** e defina-o como **maior que 0,2**. O filtro de tamanho garante que os objetos com 2 MB ou menos não serão codificados para apagamento.

6. Selecione **seguinte**.

   É apresentado o passo 2 (Definir posicionamentos).

Informações relacionadas

"O que é a filtragem de regras ILM"

"Usando filtros avançados em regras ILM"

"Passo 2 de 3: Definir posicionamentos"

Usando filtros avançados em regras 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.

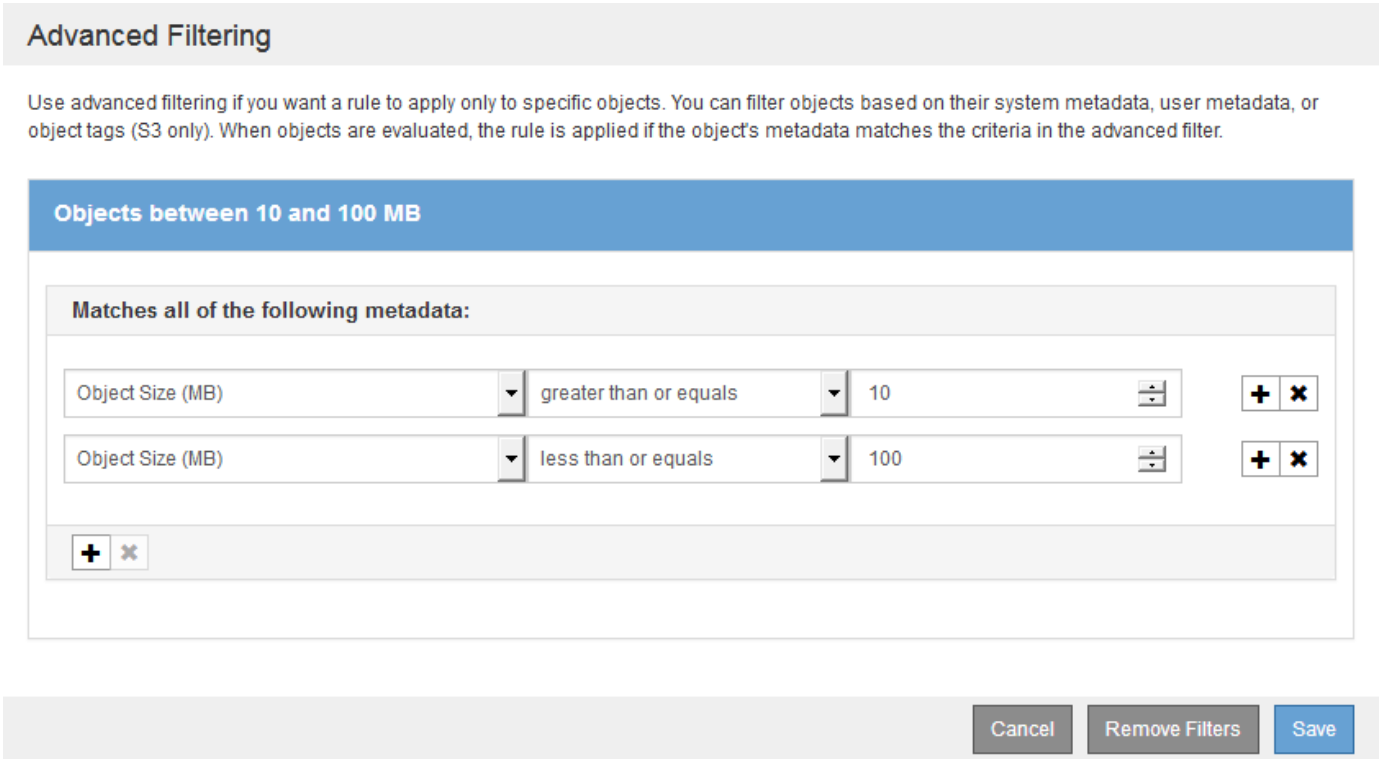
Tipo de metadados	Operadores suportados	Valor dos metadados
Tempo de ingestão (microssegundos)	• igual a • não é igual • menos de • menor que ou igual • superior a. • maior que ou igual	Hora e data em que o objeto foi ingerido. **Observação:** para evitar problemas de recursos ao ativar uma nova política 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 ou Swift única. Por exemplo, você pode querer combinar objetos que terminam com `.txt` ou começam `test-object/` com .
Último tempo de acesso (microssegundos)	• igual a • não é igual • menos de • menor que ou igual • superior a. • maior que ou igual • existe • não existe	Hora e data em que o objeto foi recuperado pela última vez (lido ou visualizado). **Observação:** se você planeja usar o último tempo de acesso como um filtro avançado, as atualizações do último tempo de acesso devem estar ativadas para o bucket do S3 ou o contentor Swift. "Usando o último tempo de acesso nas regras do ILM"
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)"

Tipo de metadados	Operadores suportados	Valor dos metadados
Tamanho do objeto (MB)	• igual a • não é igual • menos de • menor que ou igual • superior a. • maior que ou igual	O tamanho do objeto em MB. Para filtrar em tamanhos de objetos menores que 1 MB, digite um valor decimal. Por exemplo, defina o filtro avançado **Object Size (MB)** para **maior que 0,2** para qualquer regra que faça cópias codificadas por apagamento. Essa configuração garante que a codificação de apagamento não seja usada para objetos 200 KB ou menores. **Observação:** o tipo de navegador e as configurações de localidade controlam se você precisa usar um ponto ou uma vírgula como separador decimal.
Metadados do utilizador	• contém • termina com • igual a • existe • não contém • não termina com • não é igual • não existe • não começa com • começa com	Par chave-valor, onde **Nome de metadados do usuário** é a chave e **valor de metadados do usuário** é o valor. Por exemplo, para filtrar objetos que têm metadados de usuário do `color=blue`, especifique `color` para **Nome de metadados do usuário**, `equals` para o operador e `blue` para **valor de metadados do usuário**. **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 • não contém • não termina com • não é igual • não existe • não começa com • começa com	Par chave-valor, onde **Nome da etiqueta do objeto** é a chave e **valor da etiqueta do objeto** é o valor. Por exemplo, para filtrar objetos que têm uma tag de objeto de `Image=True`, especifique `Image` para **Nome da Etiqueta de objeto**, `equals` para o operador e `True` para **valor da Etiqueta 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.

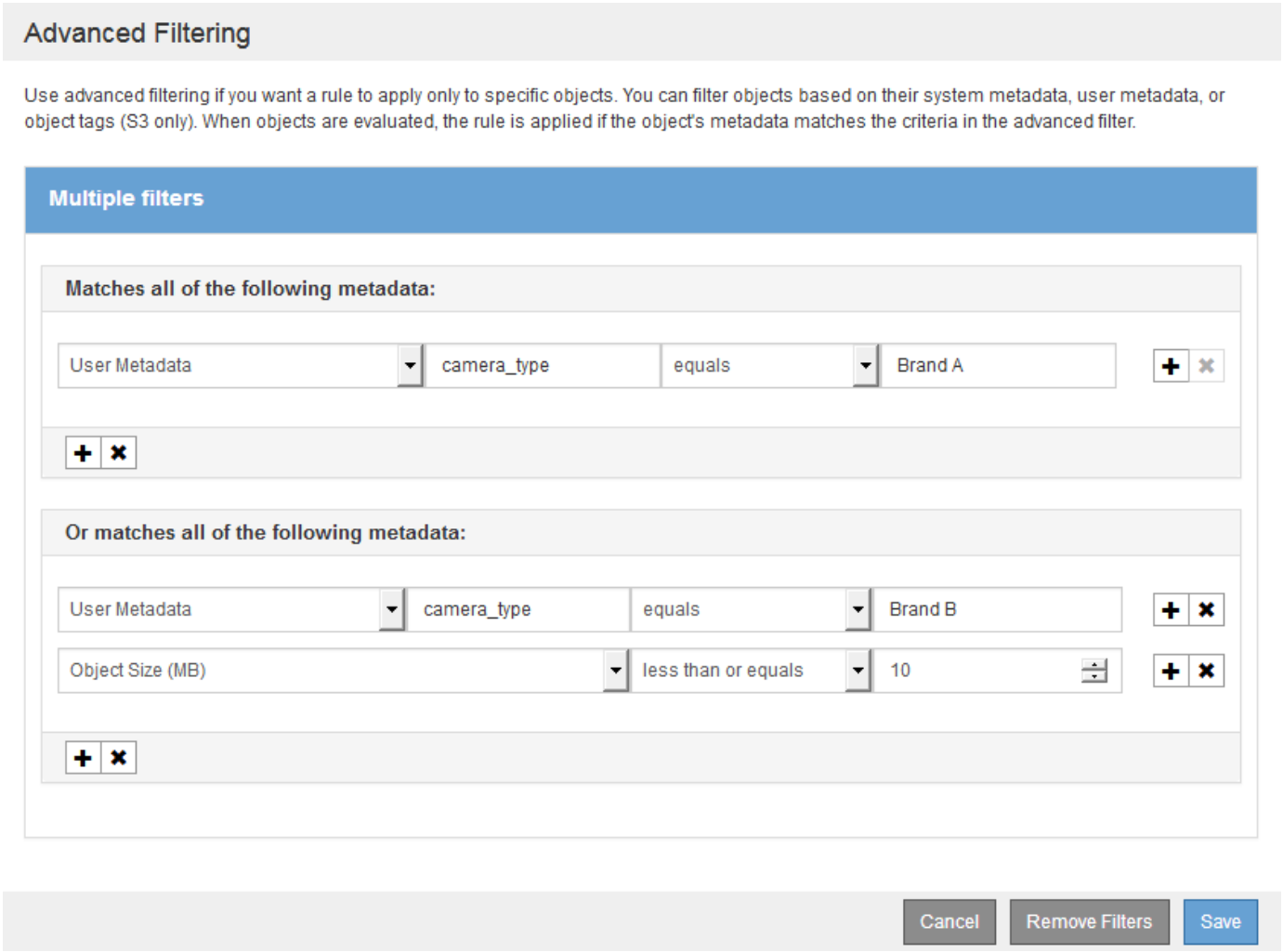
Especificando vários tipos e valores de metadados

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 uma 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.



Informações relacionadas

"Usando o último tempo de acesso nas regras do ILM"

"Configurar regiões (opcional e apenas S3)"

Passo 2 de 3: Definir posicionamentos

A etapa 2 (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 de apagamento), o local de armazenamento e o número de cópias.

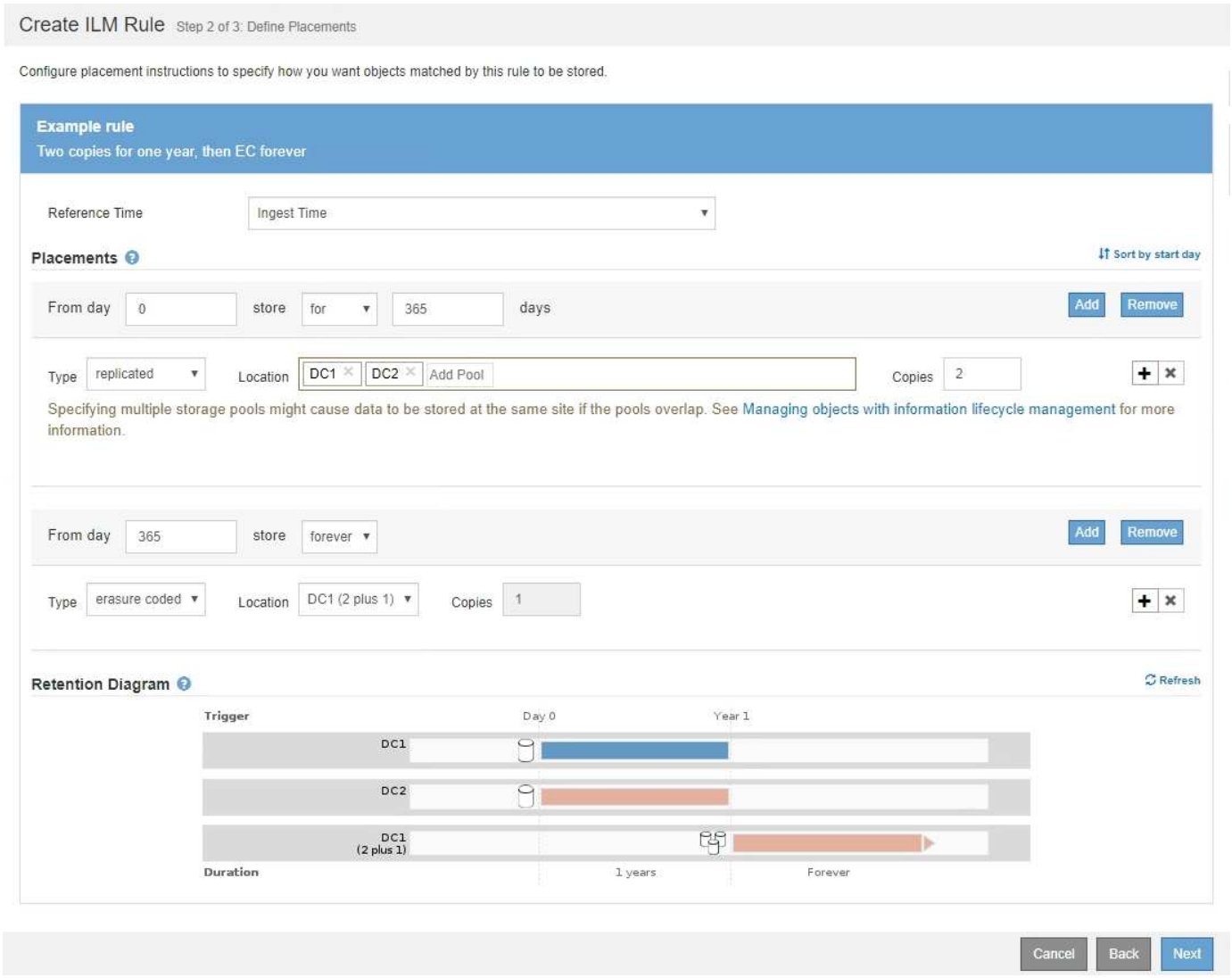
Sobre esta tarefa

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.

Este exemplo de regra ILM cria duas cópias replicadas para o primeiro ano. Cada cópia é salva em um pool de armazenamento em um local diferente. 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). **Observação:** para usar essa opção, as atualizações do último tempo de acesso devem estar ativadas para o bucket S3 ou o contentor Swift. "Usando o último tempo de acesso nas regras do ILM"

Opção	Descrição
Hora não atual	O tempo em que uma versão de objeto se tornou não atual porque uma nova versão foi ingerida e substituída como a versão atual. **Nota:** o tempo não atual aplica-se apenas a objetos S3D em buckets habilitados para versionamento. Você pode usar essa opção para reduzir o impactos de armazenamento de objetos com controle de versão filtrando versões de objetos não atuais. Veja "'exemplo 4: Regras e política do ILM para objetos com versão S3.'"
Tempo de criação definido pelo utilizador	Um tempo especificado nos metadados definidos pelo usuário.

Se você quiser criar uma regra compatível, selecione **tempo de ingestão**.

2. Na seção **colocações**, selecione 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 ("dia 0 para 365 dias"). Pelo menos uma instrução deve começar no dia 0.

3. Se você quiser criar cópias replicadas:
   a. Na lista suspensa **tipo**, selecione **replicado**.
   b. No campo **localização**, selecione **Adicionar pool** para cada pool de armazenamento que você deseja adicionar.

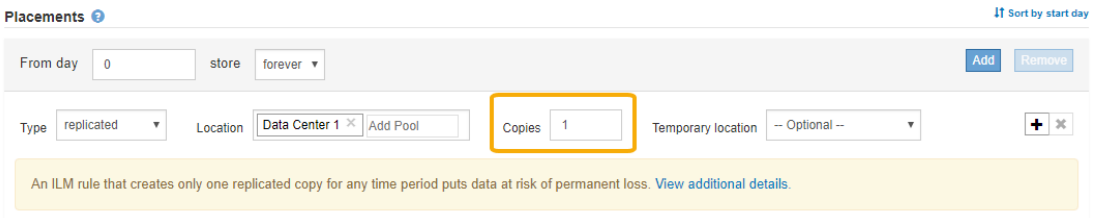
      Se você especificar apenas um pool de armazenamento, esteja ciente de que o StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer nó de armazenamento. Se sua grade incluir três nós de storage e você selecionar 4 como o número de cópias, apenas três cópias serão feitas - uma cópia para cada nó de storage.

      O alerta **ILM Placement Unachievable** é acionado para indicar que a regra ILM não pôde ser completamente aplicada.

      Se você especificar mais de um pool de armazenamento, tenha em mente estas regras:

      - O número de cópias não pode ser maior 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 do que o número de pools de storage, o sistema distribui as cópias para manter o uso do disco entre os pools balanceado e garantir 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 padrão de todos os nós de storage e outro pool de storage.

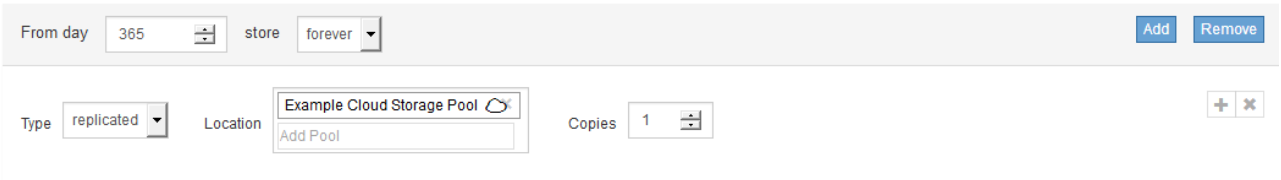
c. Selecione o número de cópias que deseja fazer.

> 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. Se existir apenas uma cópia replicada de um objeto durante um período de tempo, 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.
>
> 
>
>
> Para evitar esses riscos, faça um ou mais dos seguintes procedimentos:
>
> - Aumente o número de cópias para o período de tempo.
> - Clique no ícone de sinal de adição + para criar cópias adicionais durante o período de tempo. Em seguida, selecione um pool de armazenamento diferente ou um pool de armazenamento em nuvem.
> - Selecione **codificar para apagamento** para tipo, em vez de **replicado**. Você pode ignorar esse aviso com segurança se essa regra já criar várias cópias para todos os períodos de tempo.

d. Se você especificou apenas um pool de armazenamento, ignore o campo **local temporário**.

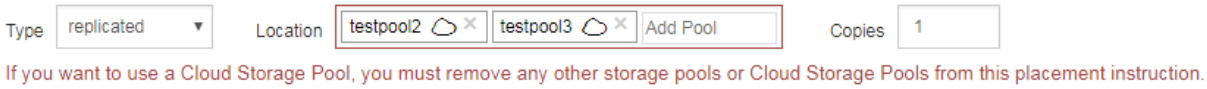
> Os locais temporários são obsoletos e serão removidos em uma versão futura.

4. Se você quiser armazenar objetos em um pool de armazenamento em nuvem:
   a. Na lista suspensa **tipo**, selecione **replicado**.
   b. No campo **localização**, selecione **Adicionar Piscina**. Em seguida, selecione um pool de armazenamento em nuvem.

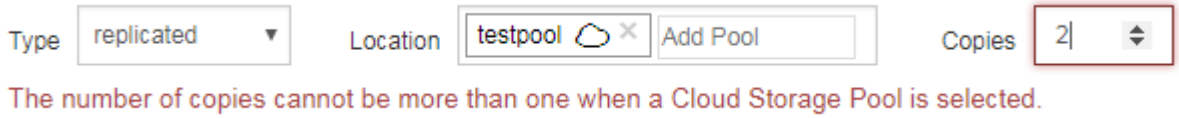


Ao usar Cloud Storage Pools, tenha em mente estas regras:

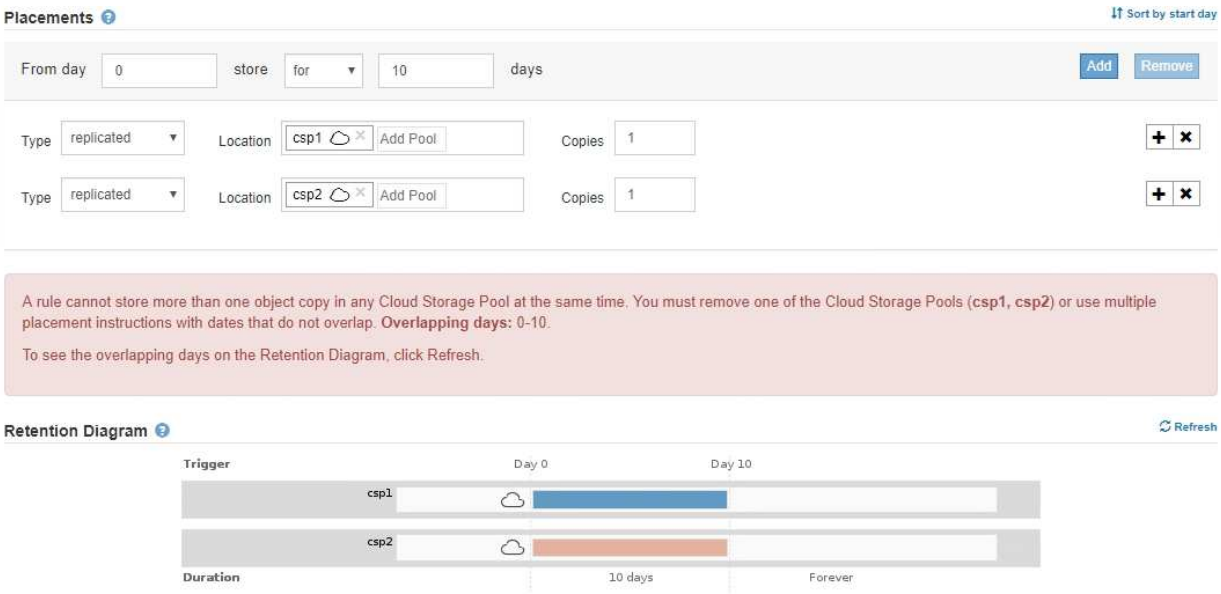
- Você não pode selecionar mais de um pool de armazenamento em nuvem em uma única instrução de colocação. Da mesma forma, você não pode selecionar um pool de armazenamento em nuvem e um pool de armazenamento na mesma instrução de colocação.



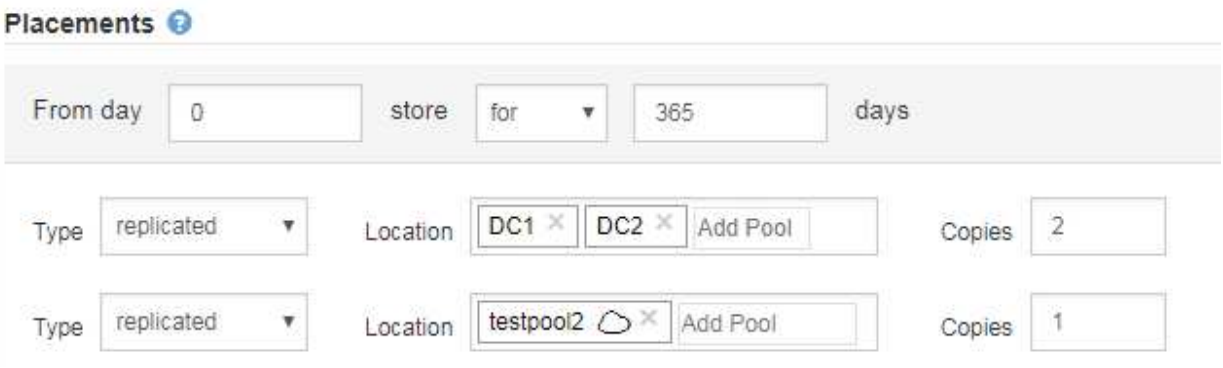
- Você pode armazenar apenas uma cópia de um objeto em qualquer pool de armazenamento em nuvem. Uma mensagem de erro será exibida se você definir **Copies** como 2 ou mais.



- 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 de apagamento no StorageGRID. No entanto, como este exemplo mostra, 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.



5. Se você quiser criar uma cópia codificada por apagamento:

   a. Na lista suspensa **Type**, selecione **Erasure Coded**.

      O número de cópias muda para 1. Um aviso será exibido se a regra não tiver um filtro avançado para ignorar objetos com 200 KB ou menos.

      > 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 o aviso de tamanho do objeto aparecer, siga estas etapas para limpá-lo:

      i. Selecione **voltar** para voltar ao passo 1.

      ii. Selecione **filtragem avançada**.

      iii. Defina o filtro tamanho do objeto (MB) como "'maior que 0,2"".

   c. Selecione o local de armazenamento.

      O local de storage para uma cópia codificada por apagamento inclui o nome do pool de storage, seguido do nome do perfil de codificação de apagamento.

6. Opcionalmente, adicione períodos de tempo diferentes ou crie cópias adicionais em locais diferentes:
   - Clique no ícone de mais para criar cópias adicionais em um local diferente durante o mesmo período de tempo.
   - Clique em **Add** para adicionar um período de tempo diferente às instruções de colocação.

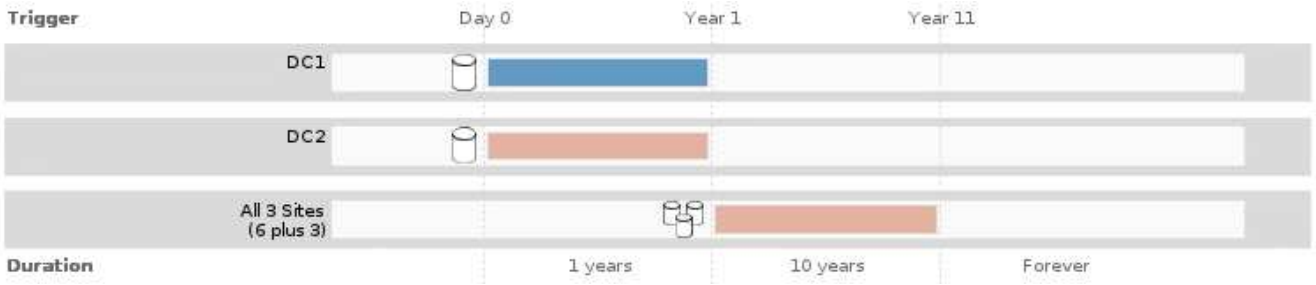
   > Os objetos são automaticamente excluídos no final do período de tempo final, a menos que o período de tempo final termine com **Forever**.

7. Clique em **Refresh** para atualizar o Diagrama de retenção e confirmar as instruções de colocação.

Cada linha no diagrama mostra onde e quando cópias de objetos serão colocadas. O tipo de cópia é representado por um dos seguintes ícones:

	Cópia replicada
	Com codificação de apagamento
	Cópia do Cloud Storage Pool

Neste exemplo, duas cópias replicadas serão salvas em dois pools de armazenamento (DC1 e DC2) por um ano. Em seguida, uma cópia codificada por apagamento será salva por mais 10 anos, usando um esquema de codificação de apagamento de mais de 6 3 em três locais. Após 11 anos, os objetos serão excluídos do StorageGRID.



8. Clique em **seguinte**.

   A etapa 3 (Definir comportamento de ingestão) é exibida.

Informações relacionadas

"Quais são as instruções de colocação de regras do ILM"

"Exemplo 4: Regras ILM e política para objetos com versão S3"

"Por que você não deve usar replicação de cópia única"

"Gerenciando objetos com o S3 Object Lock"

"Usando um pool de armazenamento como um local temporário (obsoleto)"

"Etapa 3 de 3: Definir o comportamento de ingestão"

Usando 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. Você pode usar o Gerenciador do Locatário ou a API de Gerenciamento do Locatário.

> As atualizações do último tempo de acesso são sempre ativadas para contentores Swift, mas 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

Informações relacionadas

"Use S3"

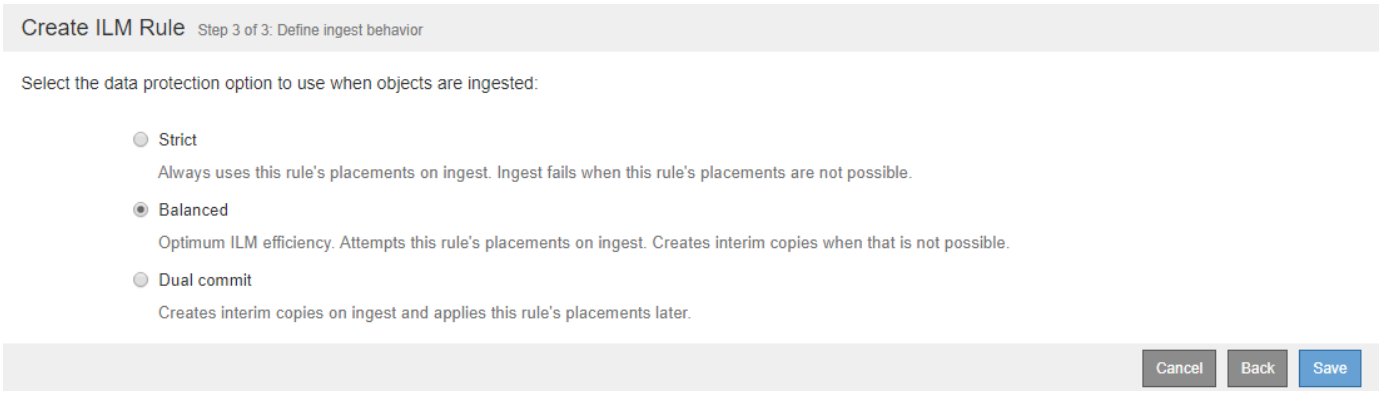
"Use uma conta de locatário"

Etapa 3 de 3: Definir o comportamento de ingestão

A etapa 3 (Definir comportamento de ingestão) do assistente criar regra ILM permite que você escolha 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 opção de proteção de dados a ser usada quando os objetos são ingeridos:

Opção	Descrição
Rigoroso	Sempre usa os posicionamentos desta regra na ingestão. A ingestão falha quando os posicionamentos desta regra não são possíveis.
Equilibrado	Eficiência ideal de ILM. Tenta os posicionamentos desta regra na ingestão. Cria cópias provisórias quando isso não é possível.
Commit duplo	Cria cópias provisórias na ingestão e aplica os posicionamentos desta regra mais tarde.

O Balanced oferece uma combinação adequada de segurança e eficiência dos dados na maioria dos casos. Strict ou Dual Commit são geralmente usados para atender a requisitos específicos.

Consulte "quais são as opções de proteção de dados para ingestão" e "vantagens e desvantagens de cada opção de proteção de dados" para obter mais informações.

Uma mensagem de erro será exibida se você selecionar a opção estrita ou equilibrada e a regra usar um desses posicionamentos:

- Um pool de armazenamento em nuvem no dia 0
- Um nó de arquivo no dia 0
- Um pool de armazenamento em nuvem ou um nó de arquivo quando a regra usa um tempo de criação definido pelo usuário como um tempo de referência

2. Clique em **Salvar**.

   A regra ILM é salva. A regra não se torna ativa até que seja adicionada a uma política ILM e essa política seja ativada.

Informações relacionadas

"Opções de proteção de dados para ingestão"

"Vantagens, desvantagens e limitações das opções de proteção de dados"

"Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"

"Criando uma política ILM"

Criando uma regra ILM padrão

Cada política de ILM deve ter uma regra padrão que não filtra objetos. Antes de criar uma política ILM, você deve criar pelo menos uma regra ILM que possa ser usada como regra padrão para a política.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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.

Nesta política de exemplo, a primeira regra aplica-se apenas a objetos pertencentes ao locatário A. 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 é automaticamente colocada como a última regra na política.
- A regra padrão não pode usar nenhum filtro básico ou avançado.
- 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 para apagamento.

- Em geral, a regra padrão deve manter objetos para sempre.
- Se você estiver usando (ou pretende ativar) a configuração global S3 Object Lock, a regra padrão para a

política ativa ou proposta deve ser compatível.

Passos

1. Selecione **ILM** > **regras**.

   A página regras do ILM é exibida.

2. Selecione **criar**.

   A etapa 1 (Definir noções básicas) do assistente criar regra ILM é exibida.

3. Digite um nome exclusivo para a regra no campo **Nome**.
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 o campo **Bucket Name** em branco.

   A regra padrão deve ser aplicada a todos os buckets do S3 e contentores Swift.

7. Não selecione **filtragem avançada**

   A regra padrão não pode especificar nenhum filtro.

8. Selecione **seguinte**.

   É apresentado o passo 2 (Definir posicionamentos).

9. 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 0,2** para evitar que objetos menores sejam codificados para 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 objeto não podem ser salvas em um pool de storage de nuvem.
     - As cópias de objeto não podem ser guardadas nos nós de arquivo.
     - 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".

10. Clique em **Refresh** para atualizar o Diagrama de retenção e confirmar as instruções de colocação.
11. Clique em **seguinte**.

    A etapa 3 (Definir comportamento de ingestão) é exibida.

12. Selecione a opção de proteção de dados a ser usada quando os objetos são ingeridos e selecione **Salvar**.

Criando uma política ILM

Quando você cria uma política ILM, você começa selecionando e organizando as regras ILM. Em seguida, você verifica o comportamento de sua política proposta simulando-a contra objetos previamente ingeridos. Quando estiver satisfeito de que a política proposta está a funcionar conforme pretendido, pode ativá-la para criar a política ativa.

> 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.

Considerações para criar uma política ILM

- Utilize a política incorporada do sistema, a Política de cópias da linha de base 2, apenas em sistemas de teste. A regra fazer cópias 2 nesta política usa o pool de storage 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.
- 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, essa regra não será avaliada 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.

Informações relacionadas

"O que é uma política ILM"

"Exemplo 6: Alterando uma política ILM"

Você pode criar uma política de ILM proposta do zero ou clonar a política ativa atual se quiser começar com o mesmo conjunto de regras.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter criado as regras ILM que deseja adicionar à política proposta. Conforme necessário, você pode salvar uma política proposta, criar regras adicionais e editar a política proposta para adicionar as novas regras.
- Você deve ter criado uma regra ILM padrão para a política que não contém nenhum filtro.

  "Criando uma regra ILM padrão"

Sobre esta tarefa

As razões típicas para criar uma política de ILM proposta incluem:

- Você adicionou um novo site e precisa usar novas regras ILM para colocar objetos nesse site.
- Você está desativando um site e você precisa remover todas as regras que se referem ao site.
- Você adicionou um novo locatário com requisitos especiais de proteção de dados.
- Você começou a usar um Cloud Storage Pool.

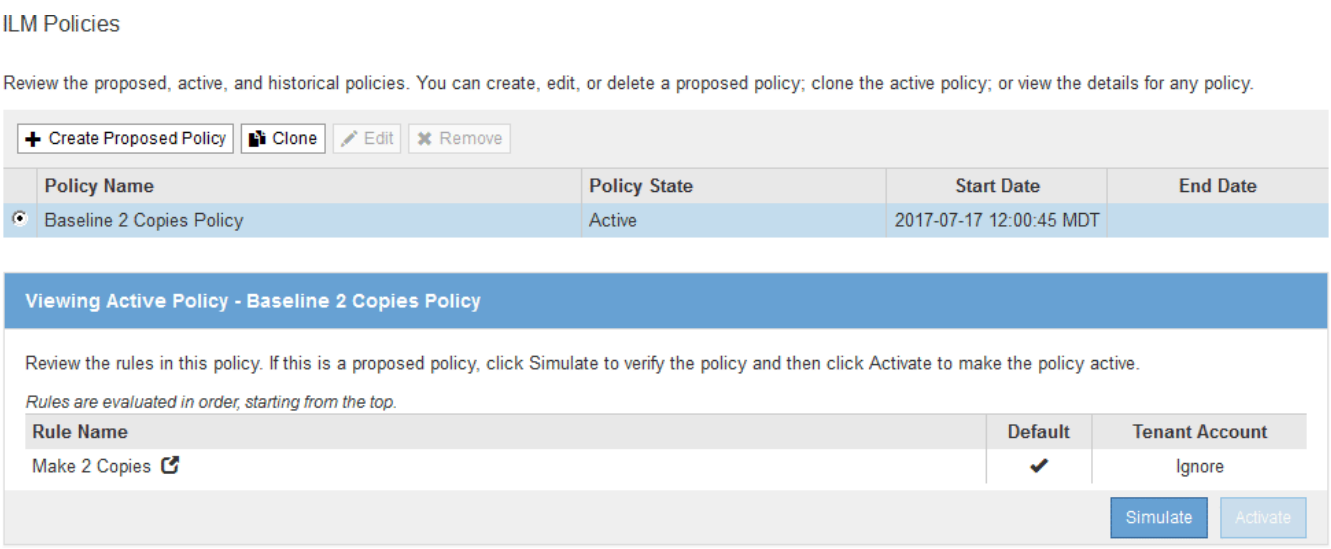
> Utilize a política incorporada do sistema, a Política de cópias da linha de base 2, apenas em sistemas de teste. A regra fazer cópias 2 nesta política usa o pool de storage todos os nós de storage, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.

> Se a configuração global S3 Object Lock tiver sido ativada, as etapas para criar uma política serão ligeiramente diferentes. Você deve garantir que a política ILM esteja em conformidade com os requisitos de buckets que têm o bloqueio de objeto S3 ativado.
>
> "Criar uma política ILM depois que o bloqueio de objetos S3 estiver ativado"

Passos

1. Selecione **ILM** > **políticas**.

   É apresentada a página ILM Policies (políticas ILM). Nesta página, você pode revisar a lista de políticas propostas, ativas e históricas; criar, editar ou remover uma política proposta; clonar a política ativa; ou exibir os detalhes de qualquer política.

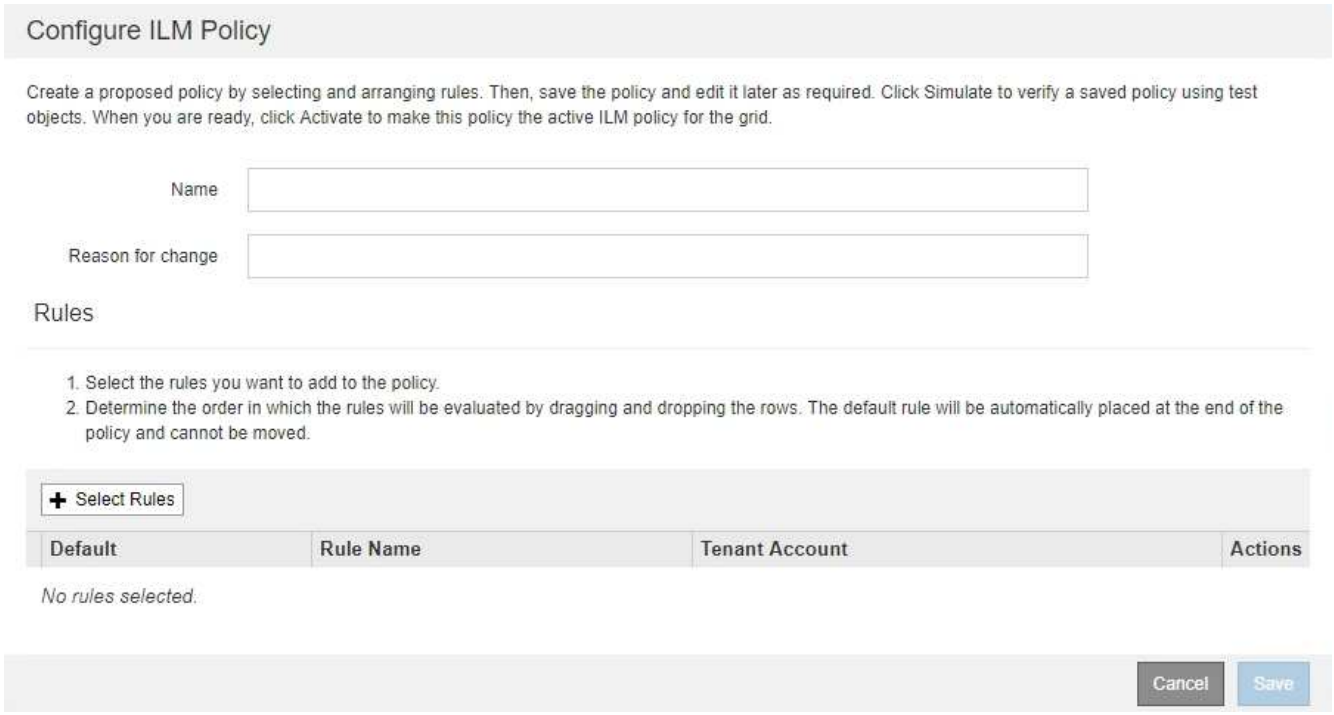


2. Determine como você deseja criar a política de ILM proposta.

Opção	Passos
Crie uma nova política proposta que não tenha regras já selecionadas	a. Se uma política de ILM proposta existir atualmente, selecione essa política e clique em **Remover**. Não é possível criar uma nova política proposta se uma política proposta já existir. b. Clique em **criar política proposta**.
Criar uma política proposta com base na política ativa	a. Se uma política de ILM proposta existir atualmente, selecione essa política e clique em **Remover**. Você não pode clonar a política ativa se uma política proposta já existir. b. Selecione a política ativa na tabela. c. Clique em **Clone**.
Edite a política proposta existente	a. Selecione a política proposta na tabela. b. Clique em **Editar**.

A caixa de diálogo Configurar política ILM é exibida.

Se você estiver criando uma nova política proposta, todos os campos estarão em branco e nenhuma regra será selecionada.



Se você estiver clonando a política ativa, o campo **Name** mostra o nome da política ativa, anexado por um número de versão ("'v2'" no exemplo). As regras usadas na política ativa são selecionadas e mostradas em sua ordem atual.

3. Digite um nome exclusivo para a política proposta no campo **Nome**.

   Você deve inserir pelo menos 1 e não mais de 64 carateres. Se você estiver clonando a política ativa, poderá usar o nome atual com o número de versão anexado ou inserir um novo nome.

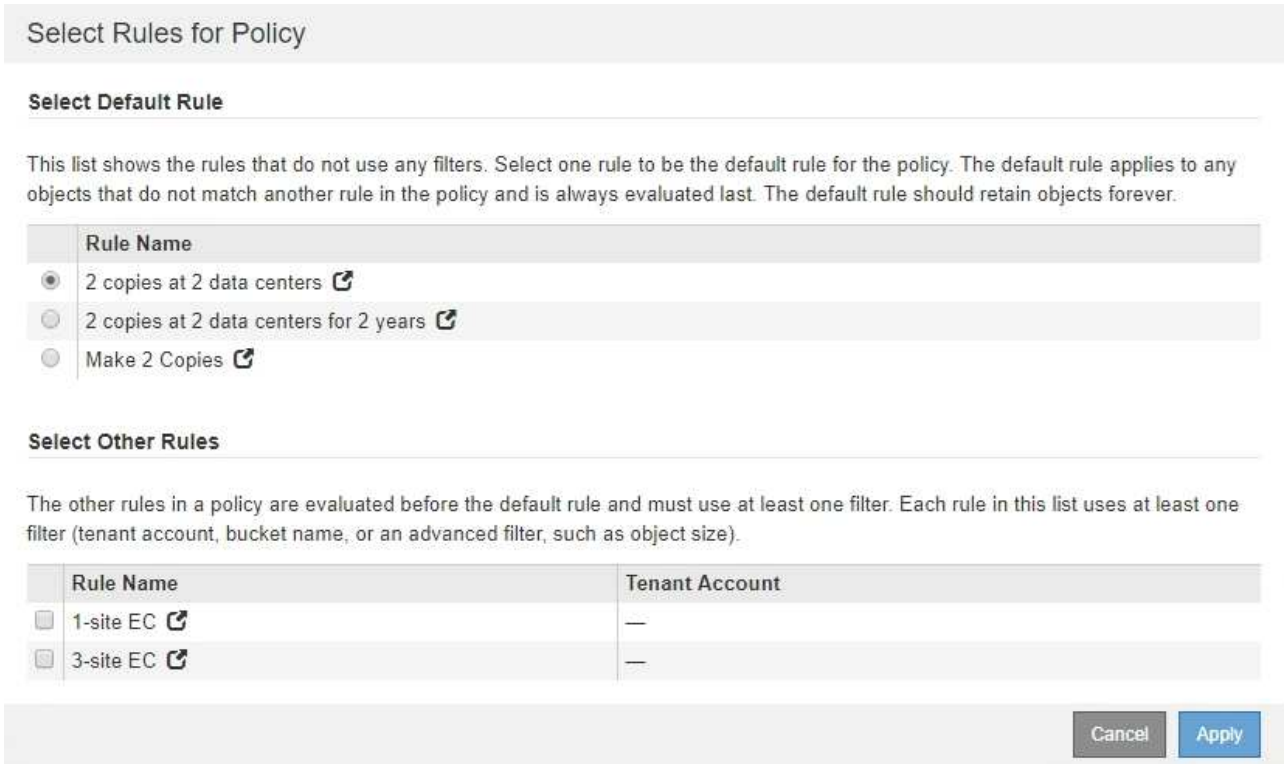
4. Insira o motivo pelo qual você está criando uma nova política proposta no campo **motivo da mudança**.

   Você deve inserir pelo menos 1 e não mais de 128 carateres.

5. Para adicionar regras à política, selecione **Selecionar regras**.

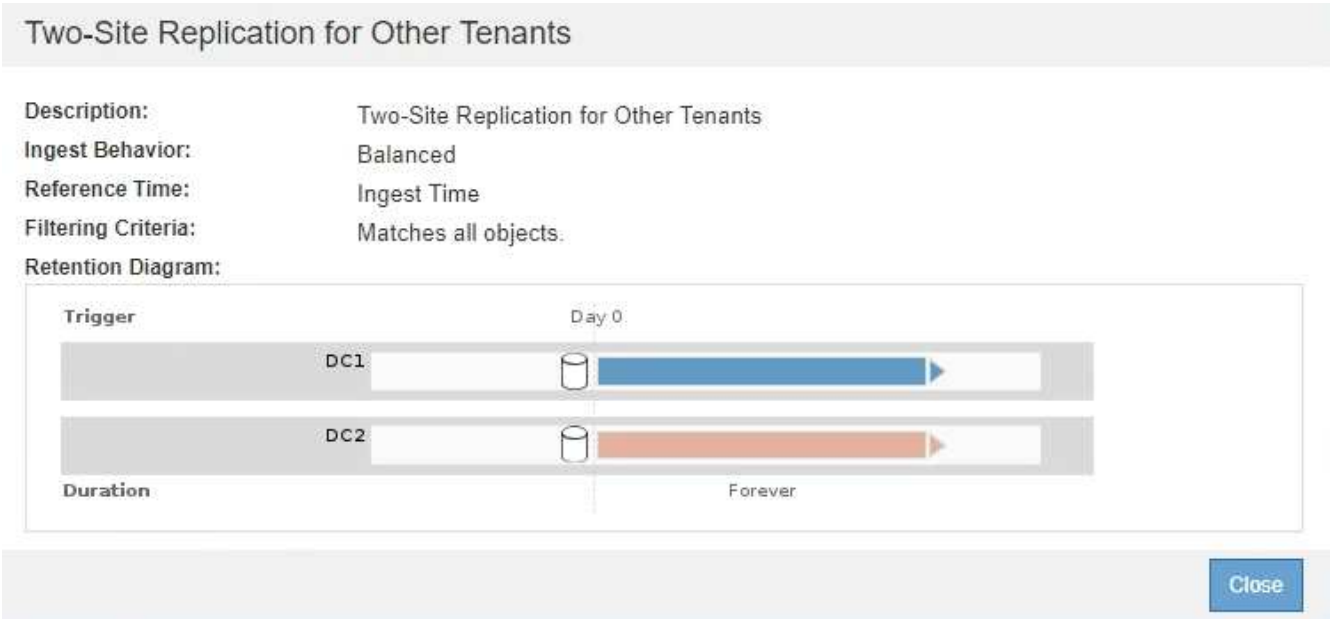
   A caixa de diálogo Selecionar regras para política é exibida, com todas as regras definidas listadas. Se você estiver clonando uma política:

   - 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, um botão permite mover a regra para o final da nova política.



6. Selecione um nome de regra ou o ícone mais detalhes para exibir as configurações dessa regra.

   Este exemplo mostra os detalhes de uma regra ILM que faz duas cópias replicadas em dois sites.



7. Na seção **Selecionar regra padrão**, selecione uma regra padrão para a política proposta.

   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.

> Se nenhuma regra estiver listada na seção Selecionar regra padrão, você deverá sair da página de política ILM e criar uma regra padrão.
>
> "Criando uma regra ILM padrão"

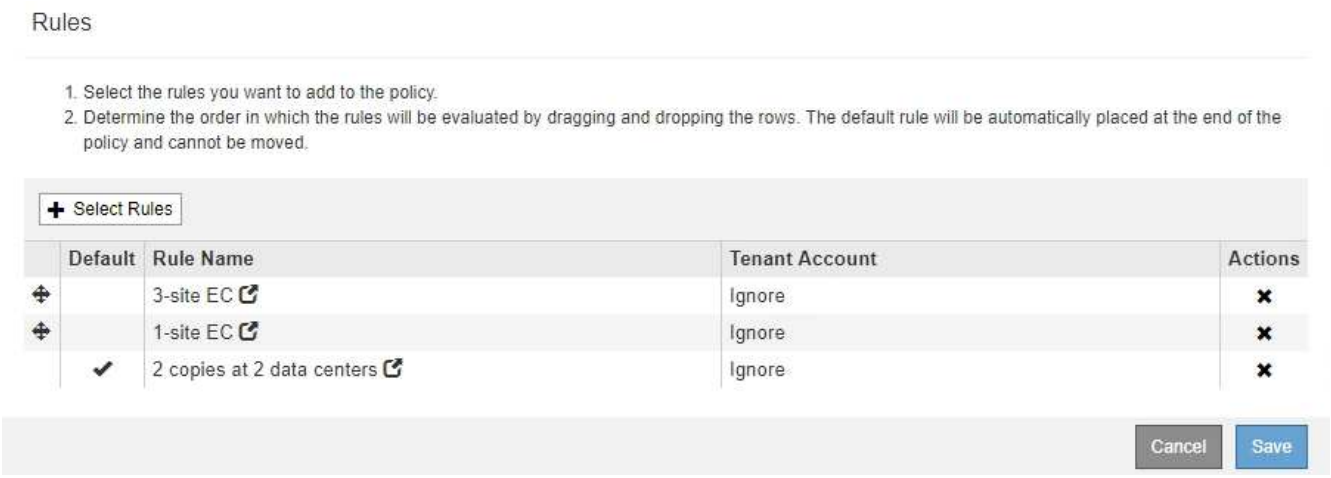
Não use a regra fazer 2 cópias de estoque como a regra padrão para uma política. A regra fazer 2 cópias usa um único pool de storage, todos os nós de storage, que contém todos os locais. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.

8. Na seção **Selecionar outras regras**, selecione quaisquer outras regras que você deseja incluir na política.

   As outras regras são avaliadas antes da regra padrão e devem usar pelo menos um filtro (conta de locatário, nome do intervalo ou um filtro avançado, como tamanho do objeto).

9. Quando terminar de selecionar regras, selecione **aplicar**.

   As regras selecionadas são listadas. A regra padrão está no final, com as outras regras acima dela.



Um aviso aparece se a regra padrão não retiver 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 mais tempo).

10. Arraste e solte as linhas para as regras não padrão para determinar a ordem em que essas regras serão avaliadas.

    Não é possível mover a regra padrão.

Você deve confirmar se as regras ILM estão na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando na parte superior.

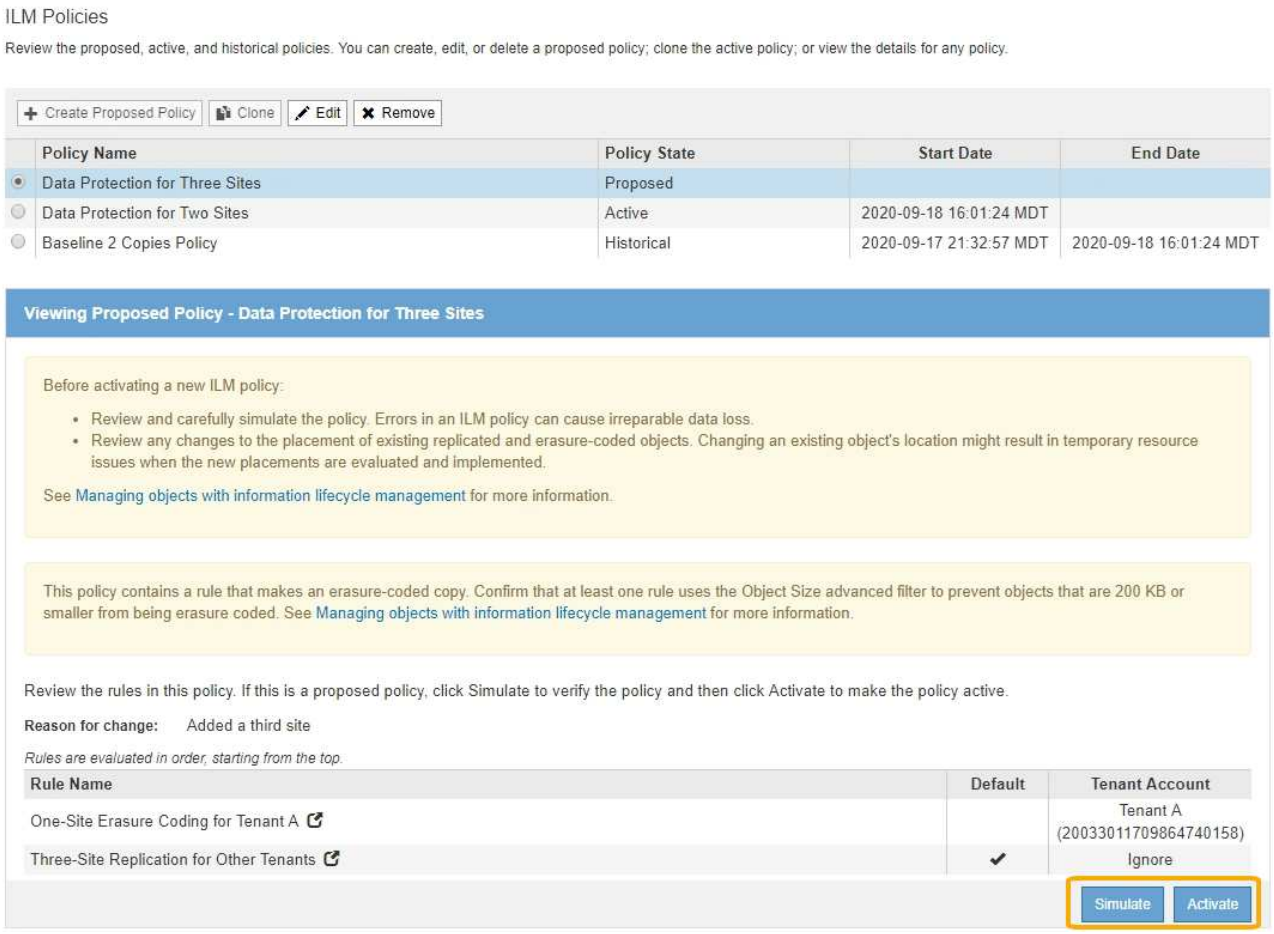
11. Conforme necessário, clique no ícone de exclusão ✖para excluir quaisquer regras que você não deseja na

política ou selecione **Selecionar regras** para adicionar mais regras.

12. Quando terminar, selecione **Guardar**.

    A página de políticas ILM é atualizada:

    - A política que você salvou é mostrada como proposta. As políticas propostas não têm datas de início e fim.
    - Os botões **Simulate** e **Activate** estão ativados.



13. Vá para "Simulando uma política ILM".

Informações relacionadas

"O que é uma política ILM"

"Gerenciando objetos com o S3 Object Lock"

Criar uma política ILM depois que o bloqueio de objetos S3 estiver ativado

Se a configuração global S3 Object Lock estiver ativada, as etapas para criar uma política serão ligeiramente diferentes. Você deve garantir que a política ILM esteja em conformidade com os requisitos de buckets que têm o bloqueio de objeto S3 ativado.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

- A configuração global de bloqueio de objetos S3D já deve estar ativada para o sistema StorageGRID.

> Se a configuração global S3 Object Lock não tiver sido ativada, use as instruções gerais para criar uma política proposta.
>
> "Criando uma política proposta de ILM"

- Você deve ter criado as regras ILM compatíveis e não compatíveis que deseja adicionar à política proposta. Conforme necessário, você pode salvar uma política proposta, criar regras adicionais e editar a política proposta para adicionar as novas regras.

  "Exemplo 7: Política de ILM compatível para bloqueio de objetos S3"

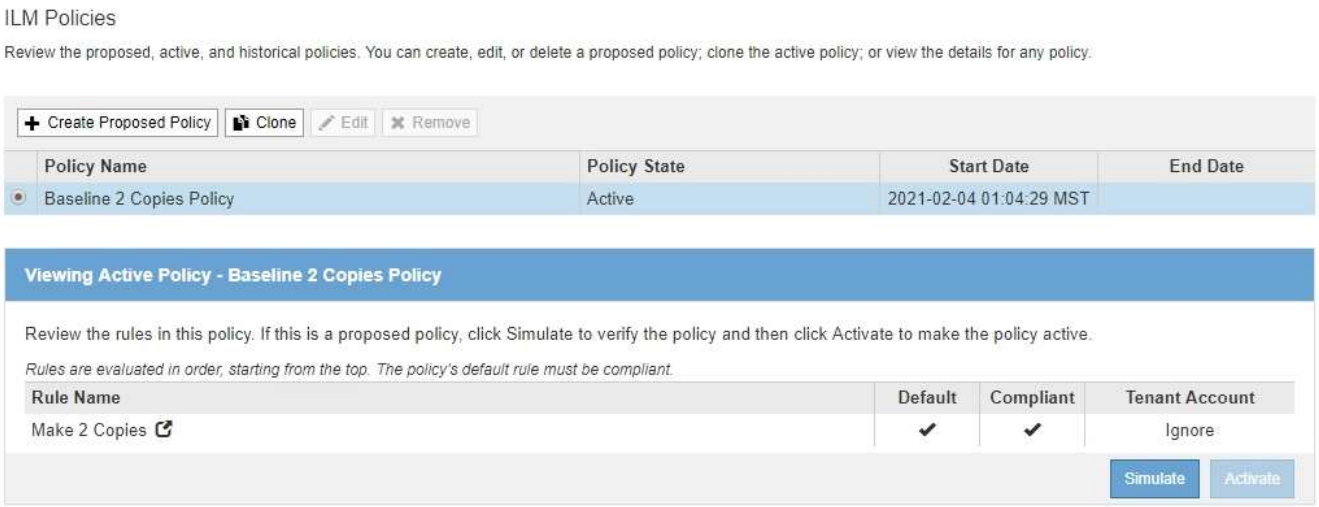
- Você deve ter criado uma regra ILM padrão compatível para a política.

  "Criando uma regra ILM padrão"

Passos

1. Selecione **ILM** > **políticas**.

   É apresentada a página ILM Policies (políticas ILM). Se a configuração Global S3 Object Lock estiver ativada, a página ILM Policies (políticas ILM) indica quais regras ILM são compatíveis.



2. Digite um nome exclusivo para a política proposta no campo **Nome**.

   Você deve inserir pelo menos 1 e não mais de 64 carateres.

3. Insira o motivo pelo qual você está criando uma nova política proposta no campo **motivo da mudança**.

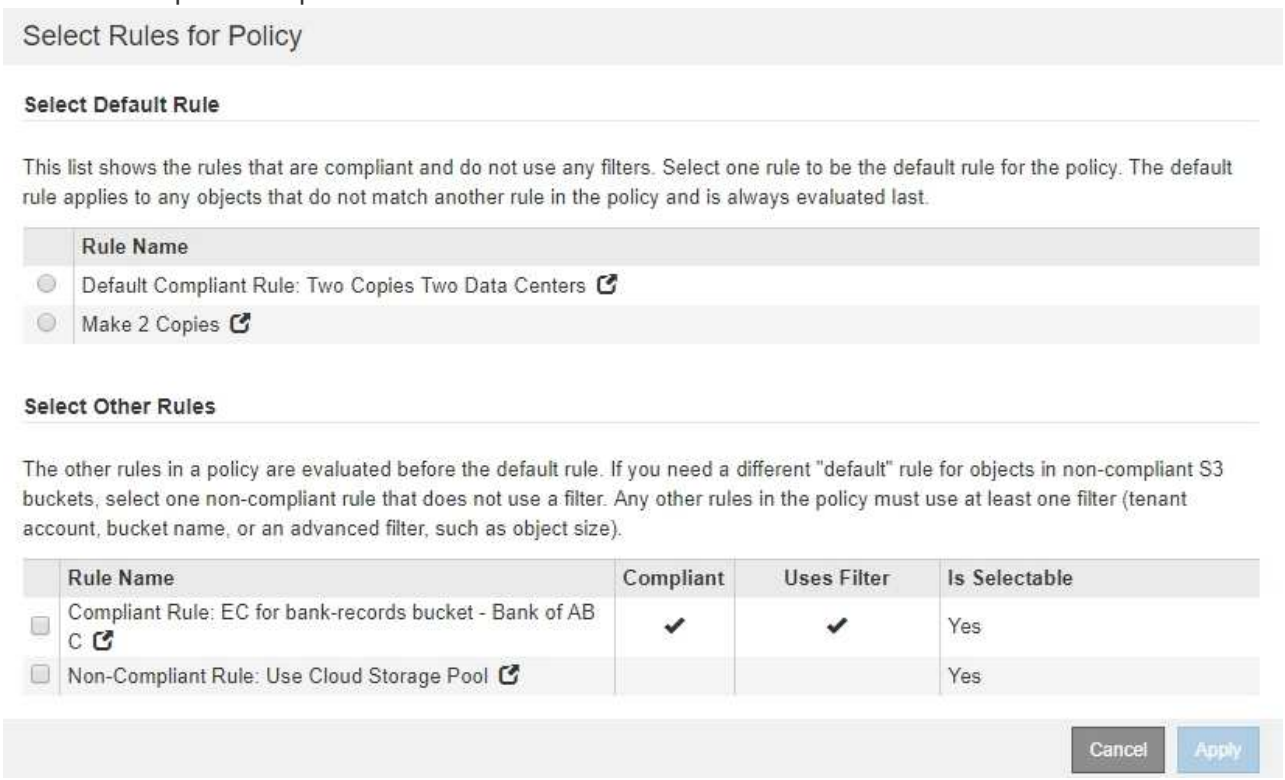
   Você deve inserir pelo menos 1 e não mais de 128 carateres.

4. Para adicionar regras à política, selecione **Selecionar regras**.

   A caixa de diálogo Selecionar regras para política é exibida, com todas as regras definidas listadas.

   - A seção Selecionar regra padrão lista as regras que podem ser o padrão para uma política compatível. Inclui regras em conformidade que não usam filtros.

◦ A seção Selecionar outras regras lista as outras regras compatíveis e não compatíveis que podem ser selecionadas para esta política.



5. Selecione um nome de regra ou o ícone mais detalhes para exibir as configurações dessa regra.
6. Na seção **Selecionar regra padrão**, selecione uma regra padrão para a política proposta.

   A tabela nesta seção lista apenas as regras que são compatíveis e não usam filtros.

   > Se nenhuma regra estiver listada na seção Selecionar regra padrão, você deverá sair da página de política ILM e criar uma regra padrão compatível.
   >
   > "Criando uma regra ILM padrão"

   > Não use a regra fazer 2 cópias de estoque como a 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.

7. Na seção **Selecionar outras regras**, selecione quaisquer outras regras que você deseja incluir na política.

   a. Se você precisar de uma regra diferente de "falha" para objetos em buckets S3 não compatíveis, opcionalmente, selecione uma regra não compatível que não use um filtro.

      Por exemplo, você pode querer usar um pool de armazenamento em nuvem ou um nó de arquivamento 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. Assim que você selecionar uma regra, a coluna **é selecionável** mostra **não** para quaisquer outras regras não compatíveis sem filtros.

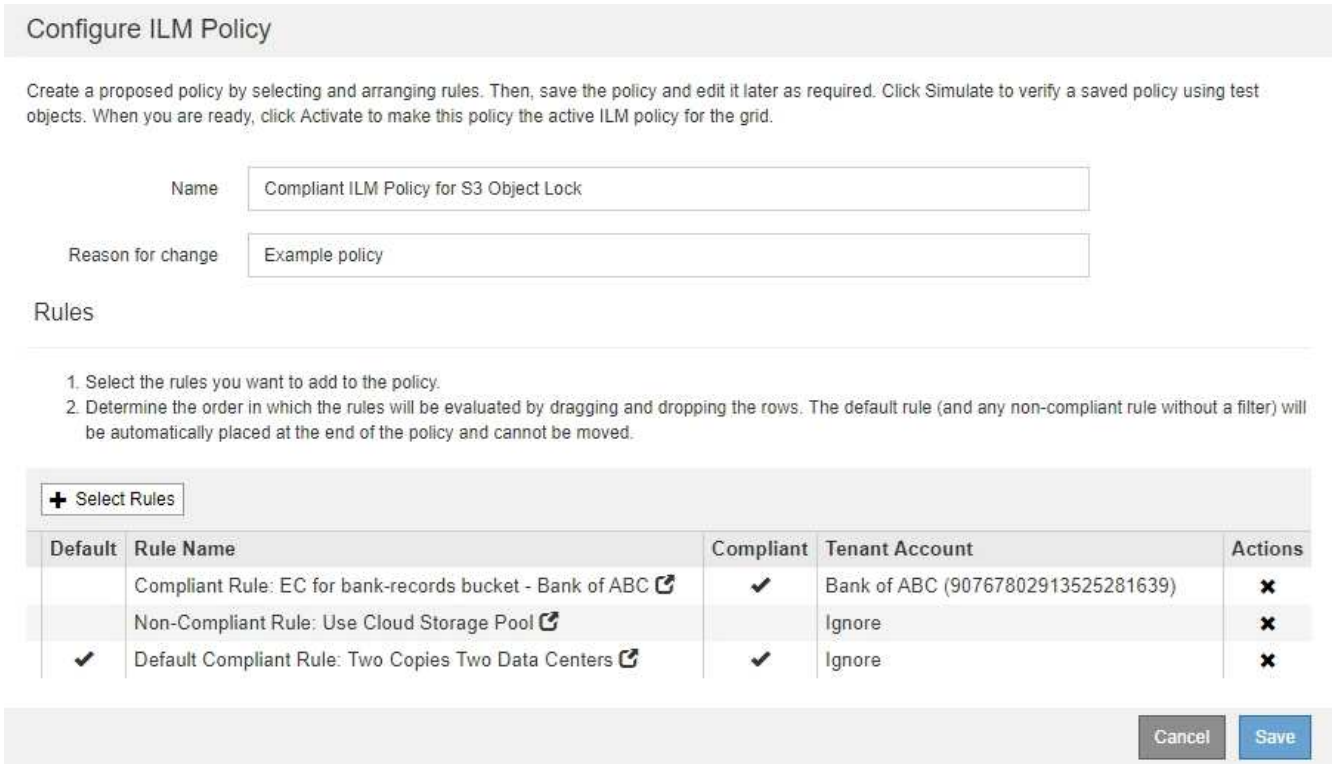
a. Selecione quaisquer outras regras compatíveis ou não compatíveis que você deseja usar na política.

   As outras regras devem usar pelo menos um filtro (conta de locatário, nome do bucket ou um filtro avançado, como tamanho do objeto).

8. Quando terminar de selecionar as regras, selecione **aplicar**.

   As regras selecionadas são listadas. A regra padrão está no final, com as outras regras acima dela. Se você também selecionou uma regra "falha" não compatível, essa regra será adicionada como regra segunda a última na política.

   Neste exemplo, a última regra, 2 cópias 2 Data Centers, é a regra padrão: Ela é compatível e não tem filtros. A regra segunda a última, Cloud Storage Pool, também não tem filtros, mas não é compatível.



   .

9. Arraste e solte as linhas para as regras não padrão para determinar a ordem em que essas regras serão avaliadas.

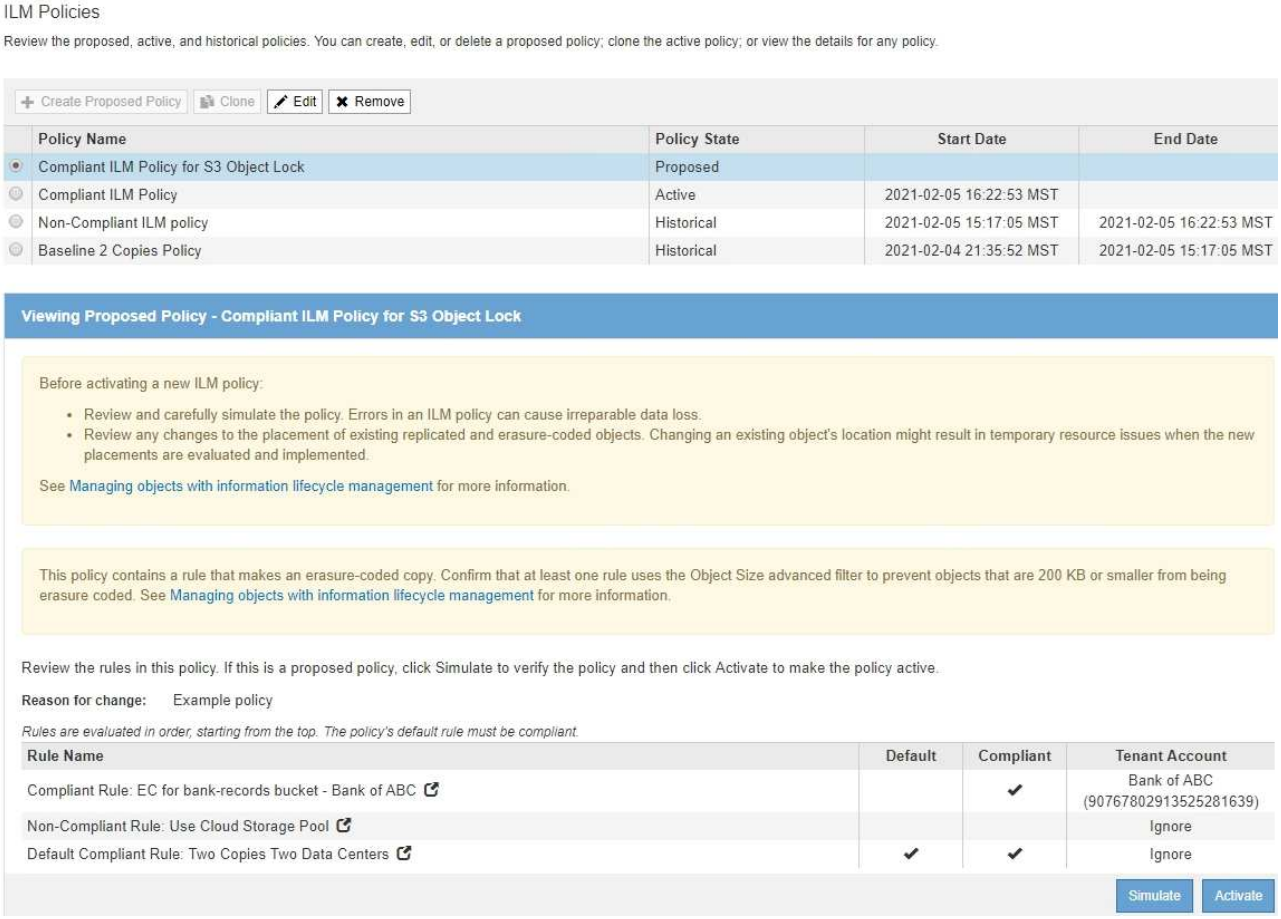
   Você não pode mover a regra padrão ou a regra "falha" não compatível.

   > 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.

10. Conforme necessário, clique no ícone de exclusão ✖para excluir quaisquer regras que você não deseja na política ou selecione **Selecionar regras** para adicionar mais regras.
11. Quando terminar, selecione **Guardar**.

    A página de políticas ILM é atualizada:

- A política que você salvou é mostrada como proposta. As políticas propostas não têm datas de início e fim.
- Os botões **Simulate** e **Activate** estão ativados.



12. Vá para "Simulando uma política ILM".

Simulando uma política ILM

Você deve simular uma política proposta em objetos de teste antes de ativar a política e aplicá-la aos dados de produção. A janela de simulação fornece um ambiente autônomo que é seguro para políticas de teste antes de serem ativadas e aplicadas aos dados no ambiente de produção.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve saber o bucket/object-key S3 ou o container/object-name Swift para cada objeto que deseja testar e você já deve ter ingerido esses objetos.

Sobre esta tarefa

Você deve selecionar cuidadosamente os objetos que deseja que a política proposta teste. Para simular uma política completamente, você deve testar pelo menos um objeto para cada filtro em cada regra.

Por exemplo, se uma política incluir uma regra para combinar objetos no bucket A e outra regra para corresponder objetos no bucket B, você deve selecionar pelo menos um objeto do bucket A e um objeto do bucket B para testar a política completamente. Se a política incluir uma regra padrão para colocar todos os

outros objetos, você deve testar pelo menos um objeto de outro intervalo.

Ao simular uma política, aplicam-se as seguintes considerações:

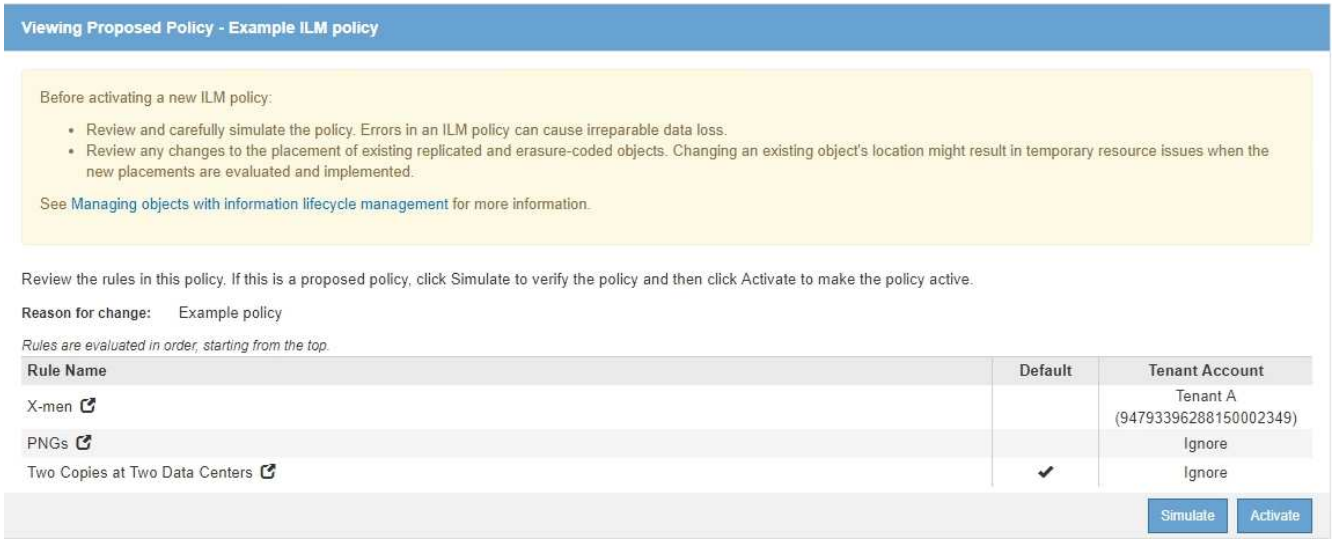
- Depois de fazer alterações em uma política, salve a política proposta. Em seguida, simule o comportamento da política proposta salva.
- Ao simular uma política, as regras ILM na política filtram os objetos de teste, para que você possa ver qual regra foi aplicada a cada objeto. No entanto, nenhuma cópia de objeto é feita e nenhum objeto é colocado. Executar uma simulação não modifica seus dados, regras ou política de forma alguma.
- A página Simulação mantém os objetos testados até que você feche, navegue para longe ou atualize a página de políticas ILM.
- Simulação retorna o nome da regra correspondente. Para determinar qual pool de armazenamento ou perfil de codificação de apagamento estão em vigor, você pode exibir o Diagrama de retenção clicando no nome da regra ou no ícone mais detalhes.
- Se o Controle de versão S3 estiver ativado, a política só será simulada em relação à versão atual do objeto.

Passos

1. Selecione e organize as regras e salve a política proposta.

   A política neste exemplo tem três regras:

Nome da regra	Filtro	Tipo de cópias	Retenção
X-men	• Inquilino A • Metadados do usuário (série x-man)	2 cópias em dois data centers	2 anos
PNGs	A chave termina com .png	2 cópias em dois data centers	5 anos
Duas cópias de dois data centers	*Nenhum*	2 cópias em dois data centers	Para sempre

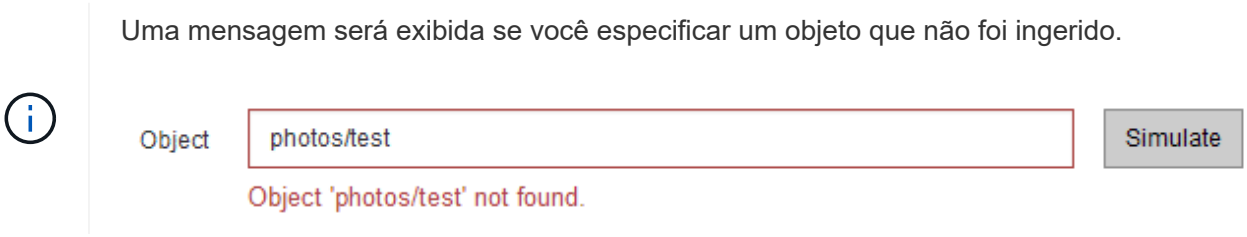


2. Clique em **simular**.

   É apresentada a caixa de diálogo Simulation ILM Policy (Política ILM de simulação).

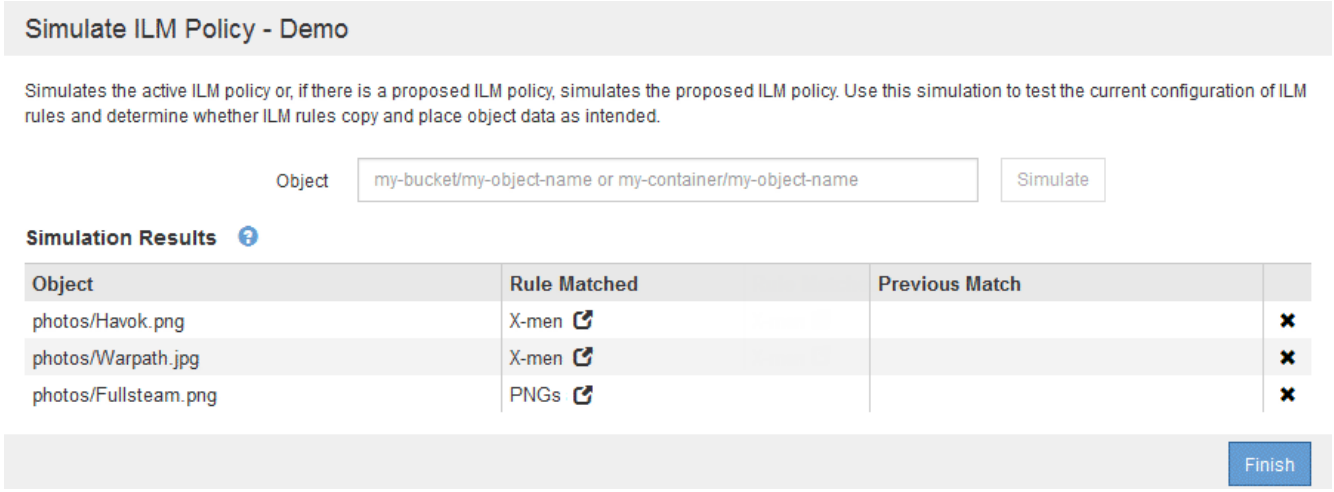
3. No campo **Object**, insira o bucket/object-key S3 ou o container/object-name Swift para um objeto de teste e clique em **Simulate**.

   Uma mensagem será exibida se você especificar um objeto que não foi ingerido.



4. Em **resultados da simulação**, confirme se cada objeto foi correspondido pela regra correta.

   No exemplo, os `Havok.png` objetos e `Warpath.jpg` foram corretamente combinados pela regra X-meN. O `Fullsteam.png` objeto, que não inclui `series=x-men` metadados do usuário, não foi correspondido pela regra X-meN, mas foi corretamente correspondido pela regra PNGs. A regra padrão não foi usada porque todos os três objetos foram correspondidos por outras regras.



Exemplos para simular políticas ILM

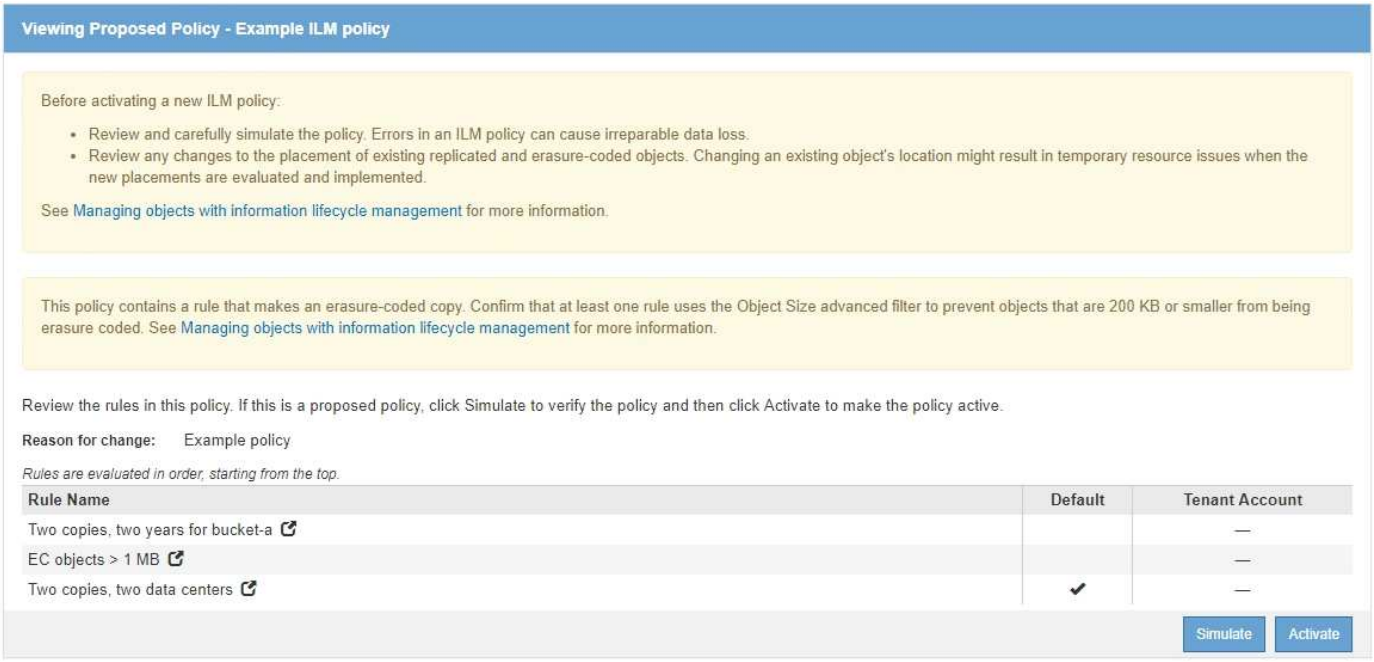
Esses exemplos mostram como você pode verificar regras ILM simulando a política ILM antes de ativá-la.

Exemplo 1: Verificando regras ao simular uma política de ILM proposta

Este exemplo mostra como verificar regras ao simular uma política proposta.

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 é a regra padrão e não inclui nenhum filtro.



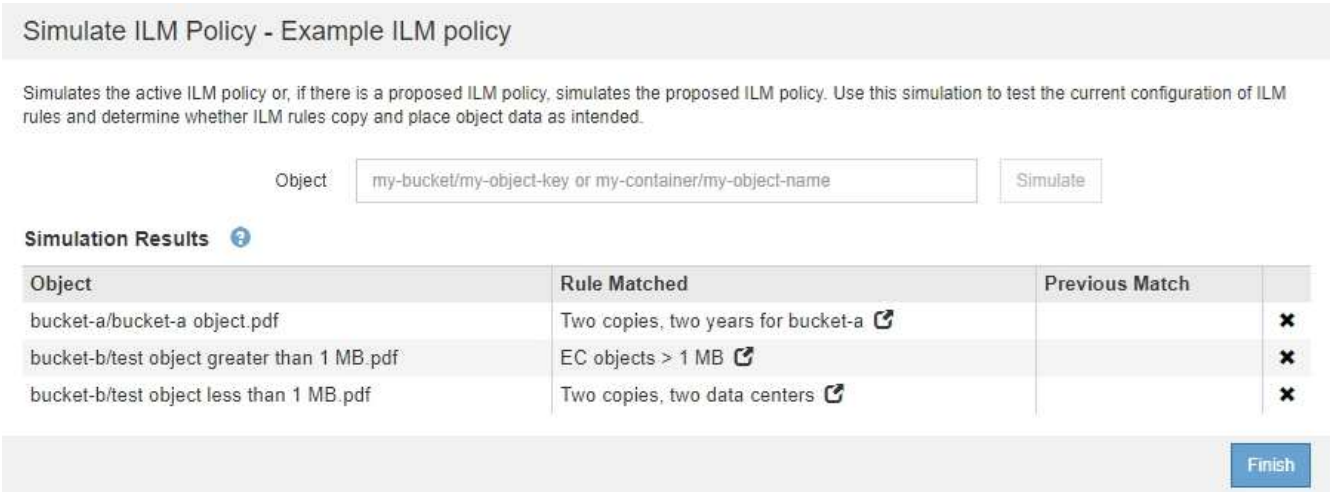
Passos

1. Depois de adicionar as regras e salvar a política, clique em **simular**.

   A caixa de diálogo simular política de ILM é exibida.

2. No campo **Object**, insira o bucket/object-key S3 ou o container/object-name Swift para um objeto de teste e clique em **Simulate**.

   Os resultados da simulação são exibidos, mostrando qual regra na política corresponde a cada objeto testado.



3. Confirme se cada objeto foi correspondido pela regra correta.

   Neste exemplo:

   a. `bucket-a/bucket-a object.pdf` corresponde corretamente à primeira regra, que filtra os objetos no `bucket-a`.

   b. `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.

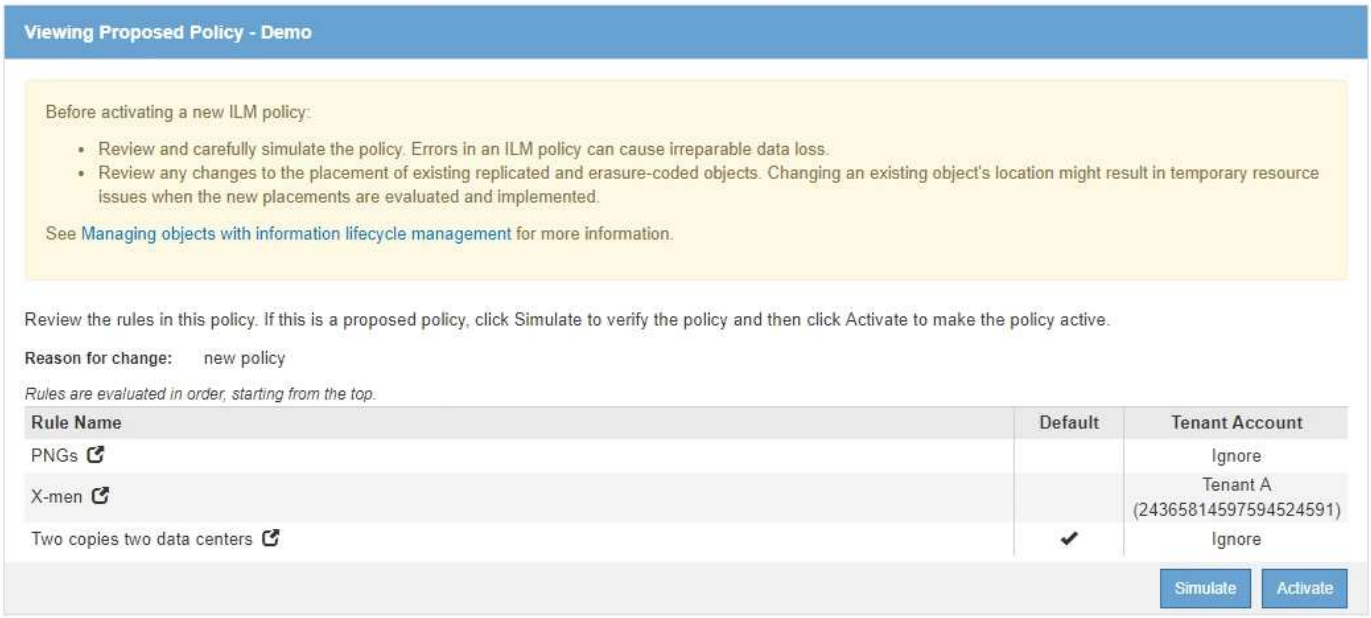
c. `bucket-b/test object less than 1 MB.pdf` não corresponde aos filtros nas duas primeiras regras, por isso será colocado pela regra padrão, que não inclui filtros.

Exemplo 2: Reordenando regras ao simular uma política de ILM proposta

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:

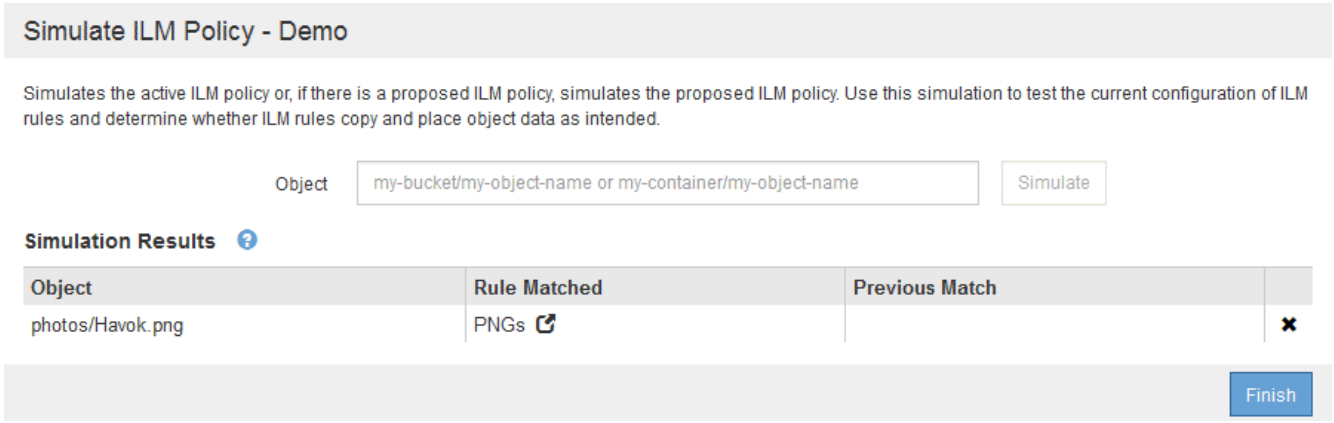
- A primeira regra, **PNGs**, filtra os nomes das chaves que terminam em `.png`.
- A segunda regra, **X-meN**, aplica-se apenas a objetos para o locatário A e filtra os metadados `series=x-men` do usuário.
- A última regra, **duas cópias dois data centers**, é a regra padrão, que corresponde a quaisquer objetos que não correspondam às duas primeiras regras.



Passos

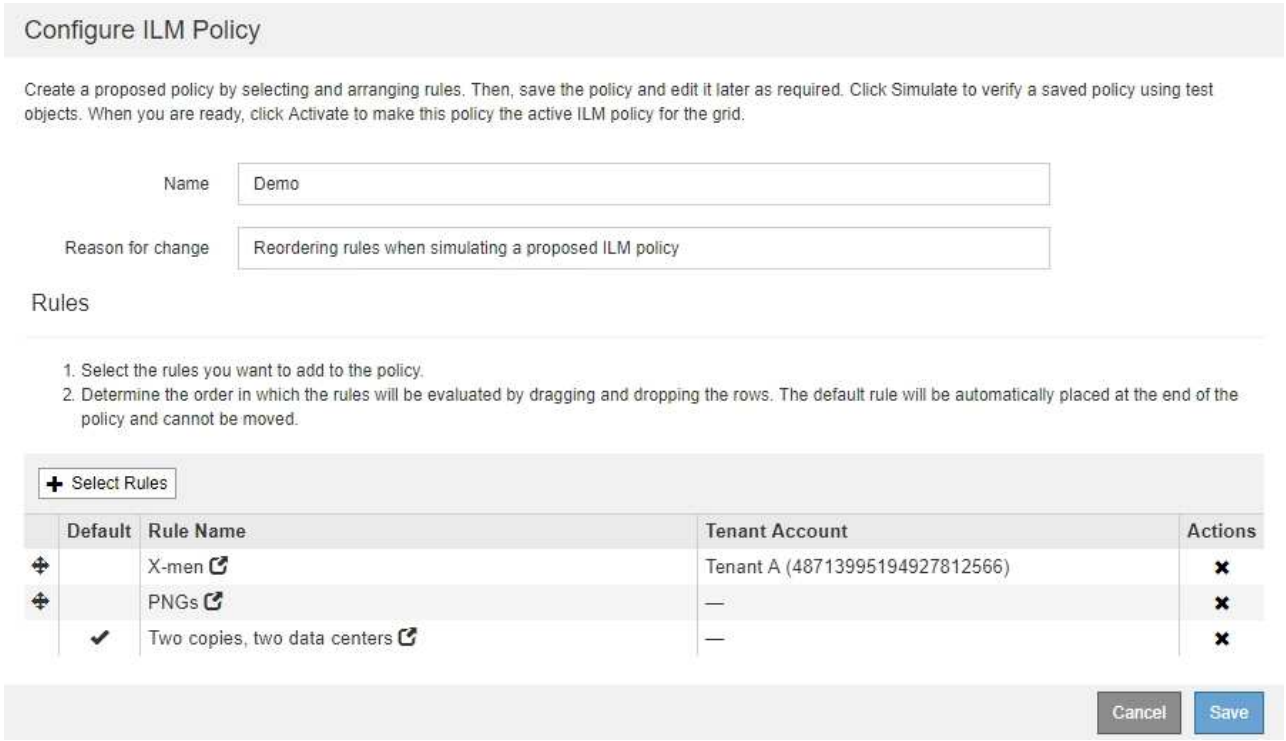
1. Depois de adicionar as regras e salvar a política, clique em **simular**.
2. No campo **Object**, insira o bucket/object-key S3 ou o container/object-name Swift para um objeto de teste e clique em **Simulate**.

   Os resultados da simulação aparecem, mostrando que o `Havok.png` objeto foi correspondido pela regra **PNGs**.



No entanto, a regra que o `Havok.png` objeto foi destinado a testar foi a regra **X-men**.

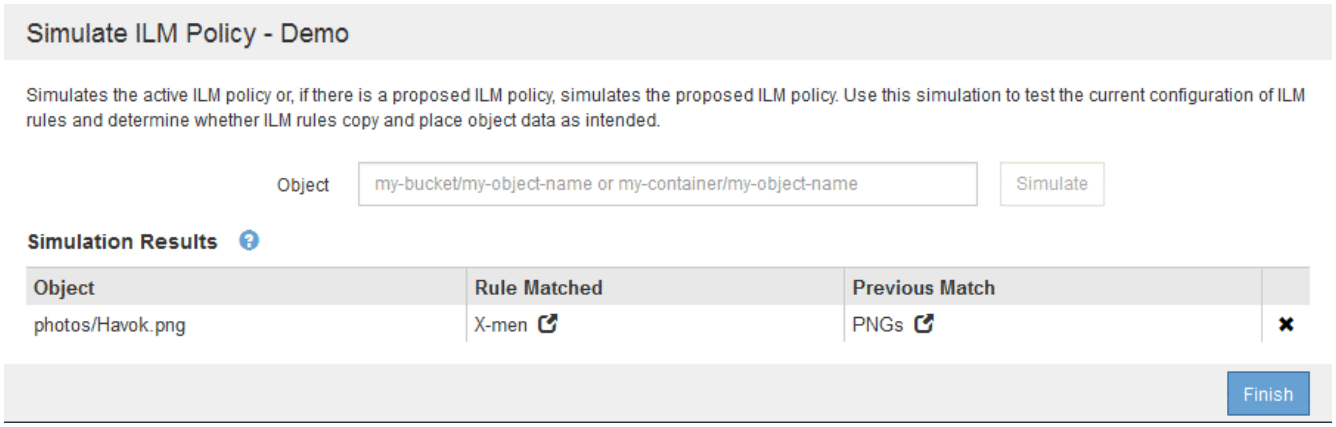
3. Para resolver o problema, reordene as regras.
   a. Clique em **Finish** para fechar a página Simulate ILM Policy.
   b. Clique em **Editar** para editar a política.
   c. Arraste a regra **X-man** para o topo da lista.



   d. Clique em **Salvar**.

4. Clique em **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.

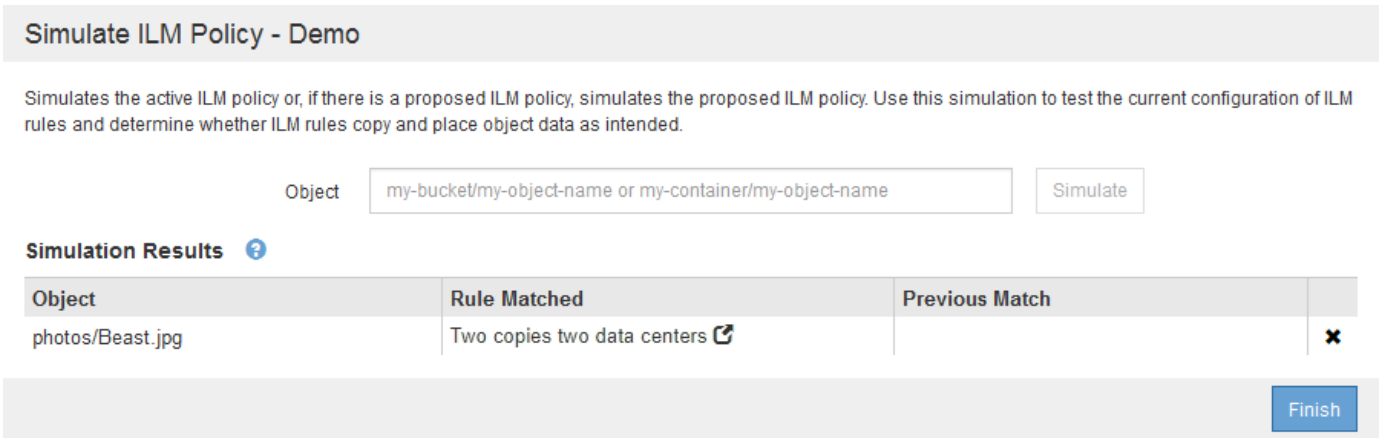


Se você permanecer na página Configurar políticas, poderá simular novamente uma política depois de fazer alterações sem precisar digitar novamente os nomes dos objetos de teste.

Exemplo 3: Corrigindo uma regra ao simular uma política de ILM proposta

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.

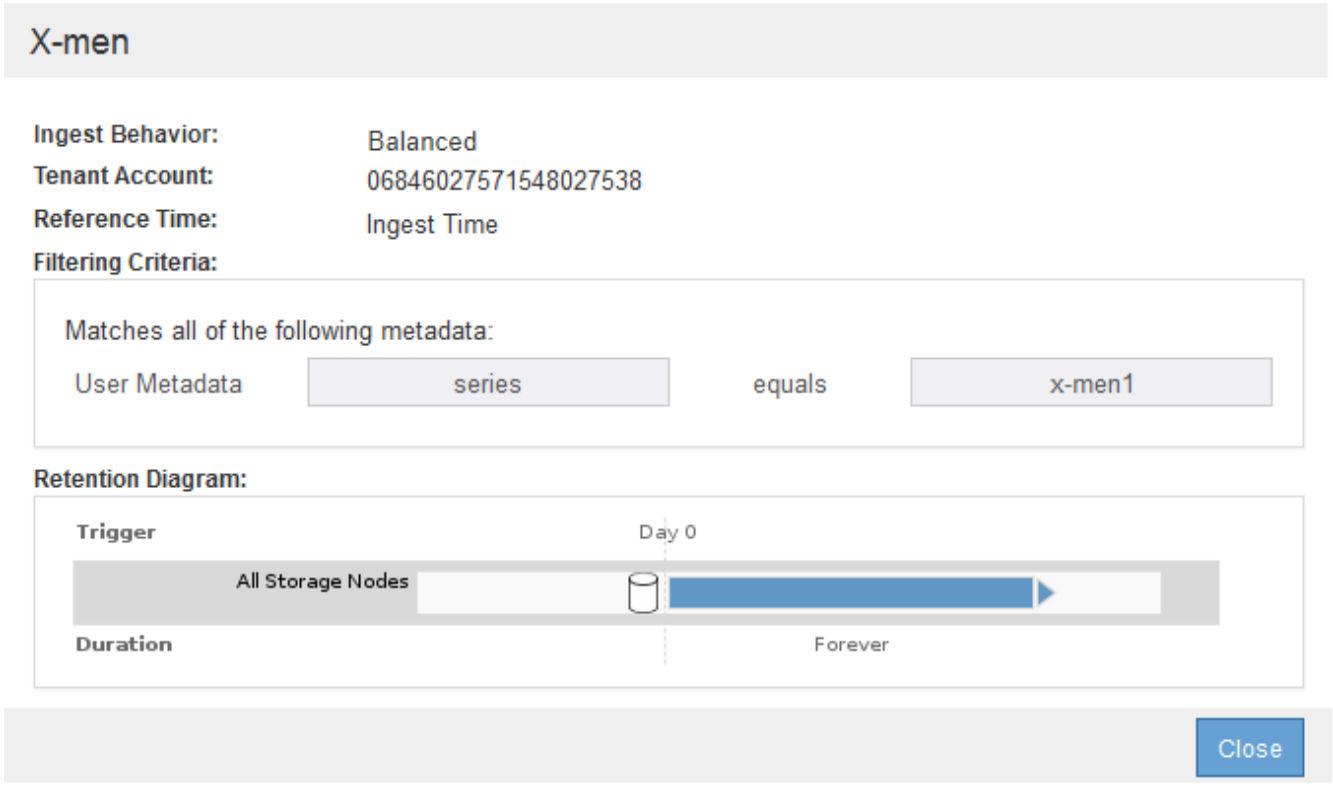


Quando um objeto de teste não é correspondido pela regra esperada na política, você deve examinar cada regra na política e corrigir quaisquer erros.

Passos

1. Para cada regra na política, exiba as configurações da regra clicando no nome da regra ou no ícone mais detalhes em qualquer caixa de diálogo em que a regra é exibida.
2. Revise a conta de locatário da regra, o tempo de referência e os critérios de filtragem.

   Neste exemplo, os metadados da regra X-meN incluem um erro. O valor dos metadados foi inserido como "'x-men1" em vez de "'x-men."



3. Para resolver o erro, corrija a regra da seguinte forma:
   - Se a regra fizer parte da política proposta, 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.

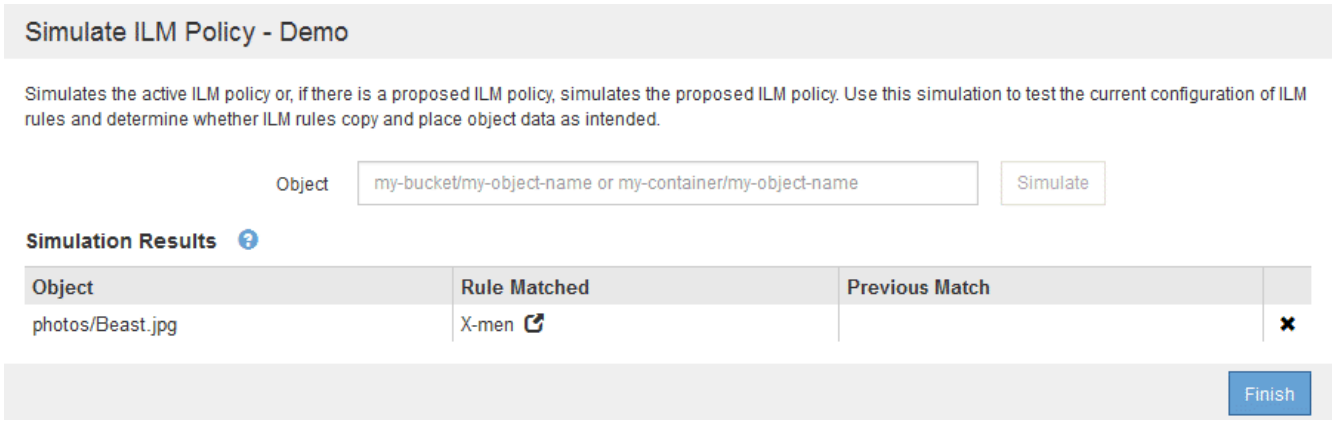
Opção	Descrição
Clonar a regra	i. Selecione **ILM** > **regras**. ii. Selecione a regra incorreta e clique em **Clone**. iii. Altere as informações incorretas e clique em **Salvar**. iv. Selecione **ILM** > **políticas**. v. Selecione a política proposta e clique em **Editar**. vi. Clique em **Selecionar regras**. vii. Marque a caixa de seleção da nova regra, desmarque a caixa de seleção da regra original e clique em **aplicar**. viii. Clique em **Salvar**.

Opção	Descrição
Editando a regra	i. Selecione a política proposta e clique em **Editar**. ii. Clique no ícone de exclusão ✖para remover a regra incorreta e clique em **Salvar**. iii. Selecione **ILM** > **regras**. iv. Selecione a regra incorreta e clique em **Editar**. v. Altere as informações incorretas e clique em **Salvar**. vi. Selecione **ILM** > **políticas**. vii. Selecione a política proposta e clique em **Editar**. viii. Selecione a regra corrigida, clique em **Apply** e clique em **Save**.

4. Execute a simulação novamente.

> ⓘ Como você navegou para fora da página de políticas ILM para editar a regra, os objetos que você inseriu anteriormente para simulação não são mais exibidos. Você deve digitar novamente os nomes dos objetos.

Neste exemplo, a regra X-meN corrigida agora corresponde ao `Beast.jpg` objeto com base nos `series=x-men` metadados do usuário, conforme esperado.



Ativar a política ILM

Depois de adicionar regras ILM a uma política ILM proposta, simule a política e confirme que ela se comporta como você espera, você está pronto para ativar a política proposta.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Tem de ter guardado e simulado a política de ILM proposta.

> ⚠ 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.

Sobre esta tarefa

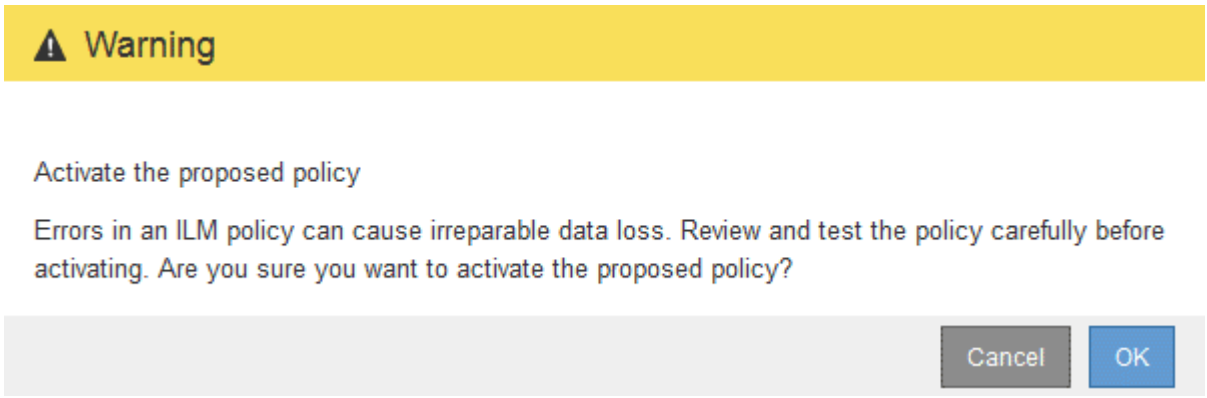
Quando você ativa uma política de ILM, o sistema distribui a nova política para todos os nós. No entanto, a nova política ativa pode não ter efeito até que todos os nós de grade estejam disponíveis para receber a nova política. Em alguns casos, o sistema espera implementar uma nova política ativa para garantir que os objetos de grade não sejam removidos acidentalmente.

- Se você fizer alterações de política que aumentem a redundância ou a durabilidade dos dados, 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 será marcada como ""ativa"", mas ela não entrará em vigor até que todos os nós estejam online e disponíveis.

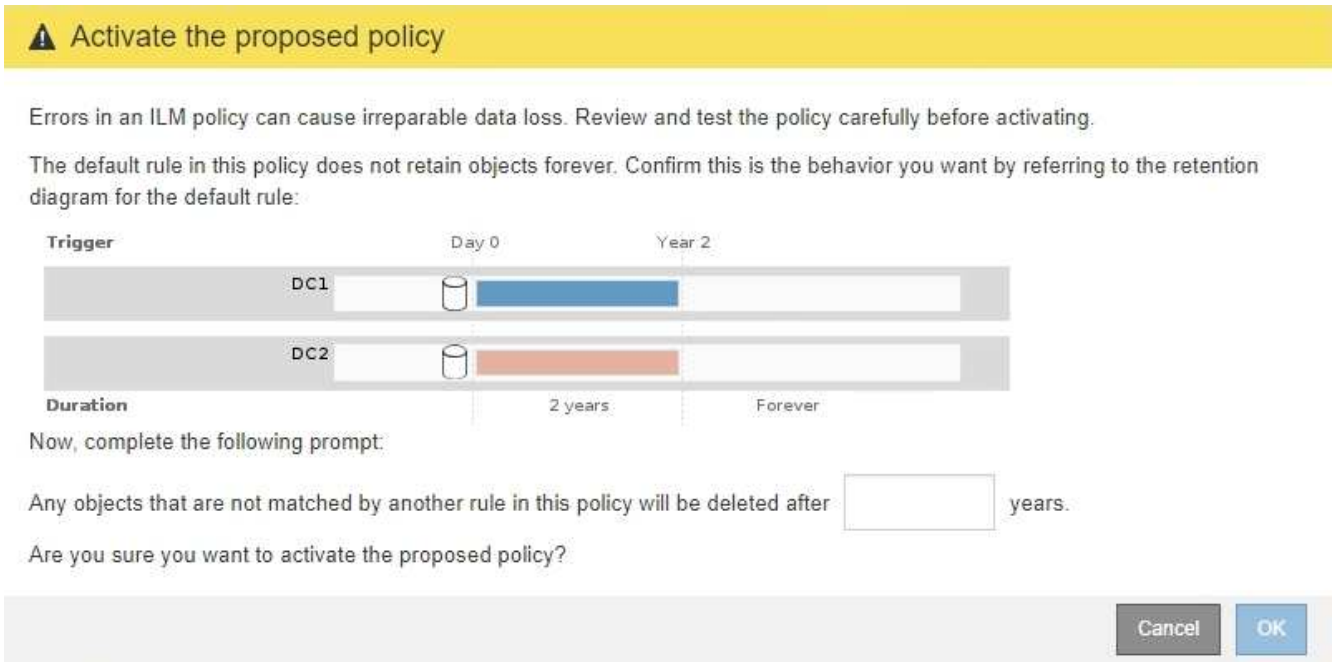
Passos

1. Quando estiver pronto para ativar uma política proposta, selecione a política na página políticas ILM e clique em **Ativar**.

   É apresentada uma mensagem de aviso, solicitando-lhe que confirme que pretende ativar a política proposta.

   Um prompt aparece na mensagem de aviso se a regra padrão da política não retiver objetos para sempre. Neste exemplo, o diagrama de retenção mostra que a regra padrão excluirá objetos após 2 anos. Você deve digitar **2** na caixa de texto para confirmar que quaisquer objetos não correlacionados por outra regra na política serão removidos do StorageGRID após 2 anos.

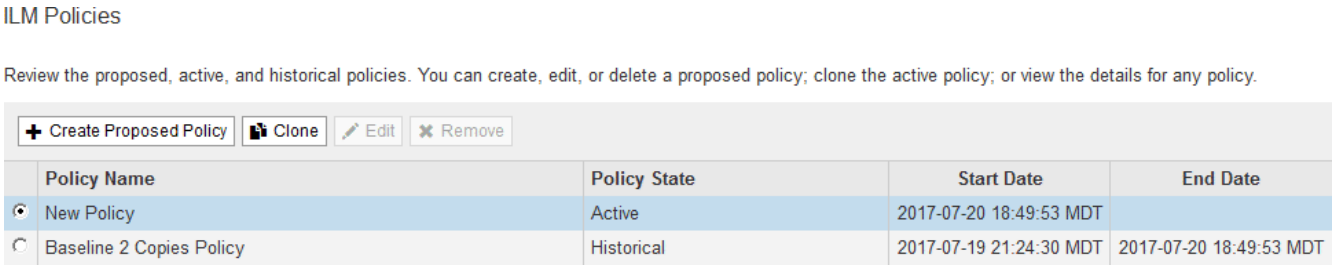


2. Clique em **OK**.

Resultado

Quando uma nova política ILM tiver sido ativada:

- A política é mostrada com um estado de política ativo na tabela na página políticas de ILM. A entrada Data Início indica a data e a hora em que a política foi ativada.



- A política anteriormente ativa é mostrada com um Estado Histórico da Política. As entradas Data de início e Data de término indicam quando a política se tornou ativa e quando ela não estava mais em vigor.

Informações relacionadas

"Exemplo 6: Alterando uma política ILM"

Verificando uma política ILM com pesquisa de metadados de objeto

Depois de ativar uma política ILM, você deve ingerir objetos de teste representativos no sistema StorageGRID. Em seguida, você deve fazer uma pesquisa de metadados de objeto para confirmar que as cópias estão sendo feitas conforme o pretendido e colocadas nos locais corretos.

O que você vai precisar

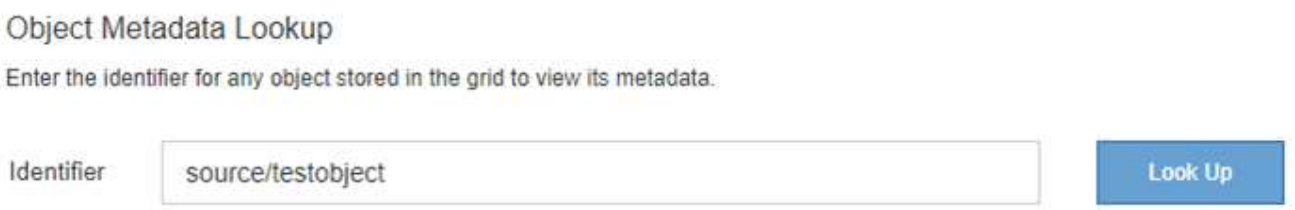
- Você deve ter um identificador de objeto, que pode ser um dos seguintes:
  - **UUID**: O Identificador universalmente exclusivo do objeto. Introduza o UUID em todas as maiúsculas.

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

Passos

1. Ingira o objeto.
2. Selecione **ILM** > **Object Metadata Lookup**.
3. Digite o identificador do objeto no campo **Identificador**.

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



4. Clique em **Procurar**.

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

   - Metadados do sistema, incluindo o ID do objeto (UUID), o 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",
```


5. 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, consulte as informações sobre como entender as mensagens de auditoria.

Informações relacionadas

"Rever registos de auditoria"

"Use S3"

"Use Swift"

Trabalhando com regras de ILM e políticas de ILM

Depois de criar regras ILM e uma política ILM, você poderá continuar trabalhando com elas, modificando sua configuração à medida que seus requisitos de storage mudarem.

Excluindo uma regra ILM

Para manter a lista de regras atuais do ILM gerenciável, exclua quaisquer regras do ILM que você provavelmente não usará.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

> Não é possível excluir uma regra ILM se ela for usada atualmente na política ativa ou na política proposta. Se você precisar excluir uma regra ILM que é usada em uma política, execute estas etapas primeiro:
>
> 1. Clonar a política ativa ou editar a política proposta.
> 2. Remova a regra ILM da política.
> 3. Salve, simule e ative a nova política para garantir que os objetos estejam protegidos conforme esperado.

Passos

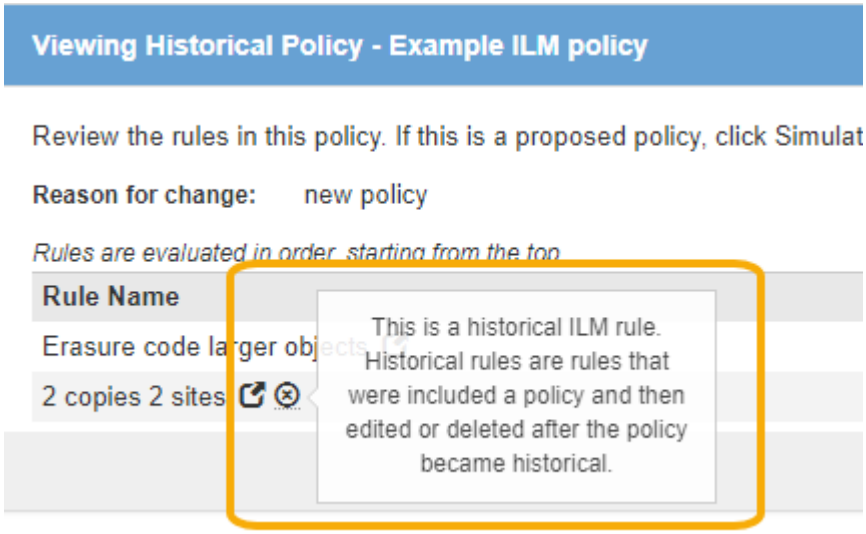
1. Selecione **ILM** > **regras**.
2. Revise a entrada da tabela para a regra que deseja remover.

   Confirme se a regra não é usada na política ILM ativa ou na política ILM proposta.

3. Se a regra que você deseja remover não estiver em uso, selecione o botão de opção e selecione **Remover**.
4. Selecione **OK** para confirmar que deseja excluir a regra ILM.

   A regra ILM é excluída.

Se você excluir uma regra que é usada em uma política histórica, um ⊗ ícone aparecerá para a regra quando você exibir a política, o que indica que a regra se tornou uma regra histórica.



Informações relacionadas

"Criando uma política ILM"

Editar uma regra ILM

Talvez seja necessário editar uma regra ILM para alterar um filtro ou uma instrução de colocação.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

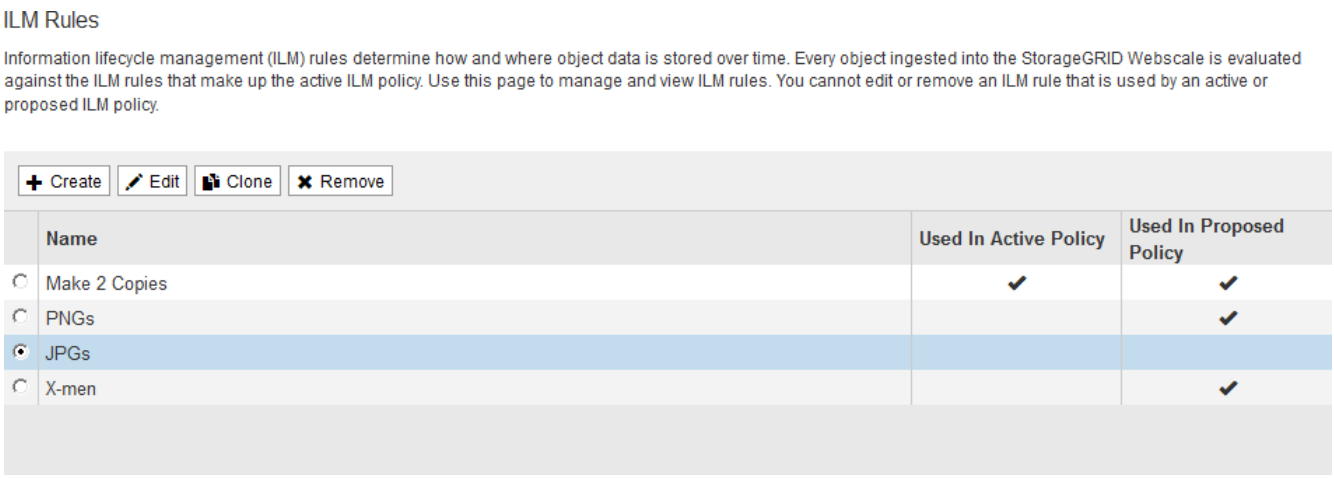
Não é possível editar uma regra se ela estiver sendo usada na política ILM proposta ou na política ILM ativa. Em vez disso, você pode clonar essas regras e fazer as alterações necessárias na cópia clonada. Você também não pode editar a regra ILM de estoque (fazer 2 cópias) ou regras ILM criadas antes da versão 10,3 do StorageGRID.

Antes de adicionar uma regra editada à política ILM ativa, esteja ciente de que uma alteração nas instruções de posicionamento de um objeto pode causar um aumento de carga no sistema.

Passos

1. Selecione **ILM** > **regras**.

   A página regras do ILM é exibida. Esta página mostra todas as regras disponíveis e indica quais regras estão sendo usadas na política ativa ou na política proposta.



2. Selecione uma regra que não esteja sendo usada e clique em **Editar**.

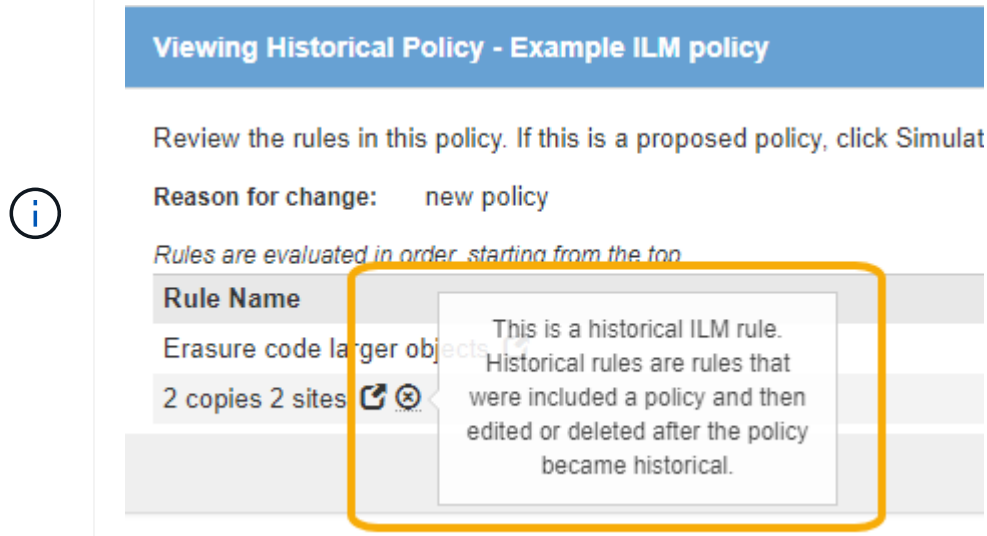
   O assistente Editar regra ILM é aberto.

3. Complete as páginas do assistente Editar regra ILM, seguindo as etapas para criar uma regra ILM e usar filtros avançados, conforme necessário.

   Ao editar uma regra ILM, você não pode alterar seu nome.

4. Clique em **Salvar**.

Se você editar uma regra que é usada em uma política histórica, um ⊗ ícone aparecerá para a regra quando você exibir a política, o que indica que a regra se tornou uma regra histórica.



Informações relacionadas

"Criando uma regra ILM"

"Usando filtros avançados em regras ILM"

Clonar uma regra ILM

Não é possível editar uma regra se ela estiver sendo usada na política ILM proposta ou na política ILM ativa. Em vez disso, você pode clonar uma regra e fazer as alterações necessárias à cópia clonada. Então, se necessário, você pode remover a regra original da política proposta e substituí-la pela versão modificada. Você não pode clonar uma regra ILM se ela foi criada usando o StorageGRID versão 10,2 ou anterior.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

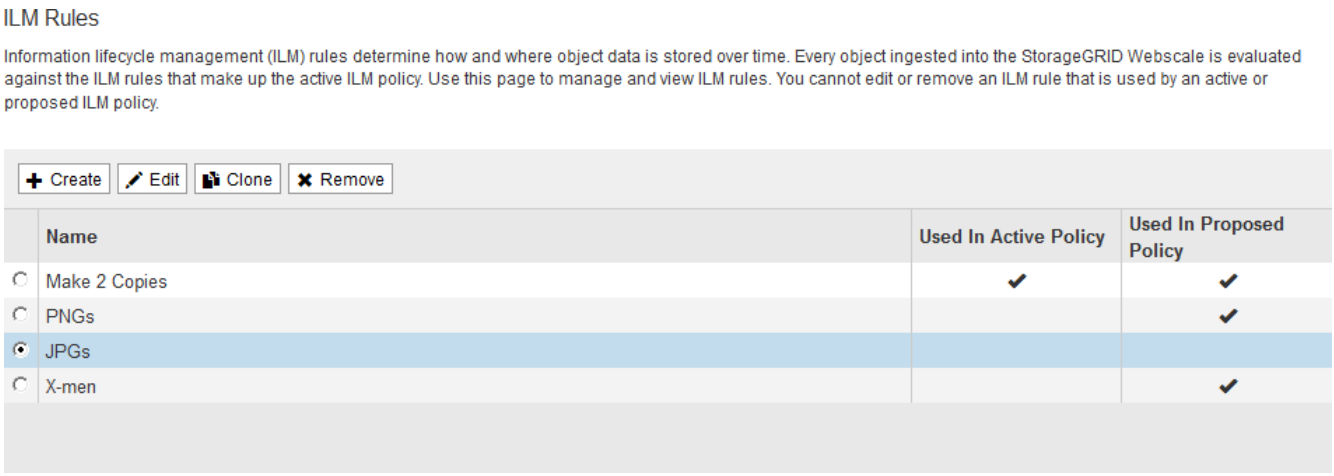
Sobre esta tarefa

Antes de adicionar uma regra clonada à política ILM ativa, esteja ciente de que uma alteração nas instruções de posicionamento de um objeto pode causar um aumento de carga no sistema.

Passos

1. Selecione **ILM** > **regras**.

   A página regras do ILM é exibida.



2. Selecione a regra ILM que deseja clonar e clique em **Clone**.

   O assistente criar regra ILM é aberto.

3. Atualize a regra clonada seguindo as etapas para editar uma regra ILM e usando filtros avançados.

   Ao clonar uma regra ILM, você deve inserir um novo nome.

4. Clique em **Salvar**.

   A nova regra ILM é criada.

Informações relacionadas

"Trabalhando com regras de ILM e políticas de ILM"

"Usando filtros avançados em regras ILM"

Visualizar a fila de atividades da política ILM

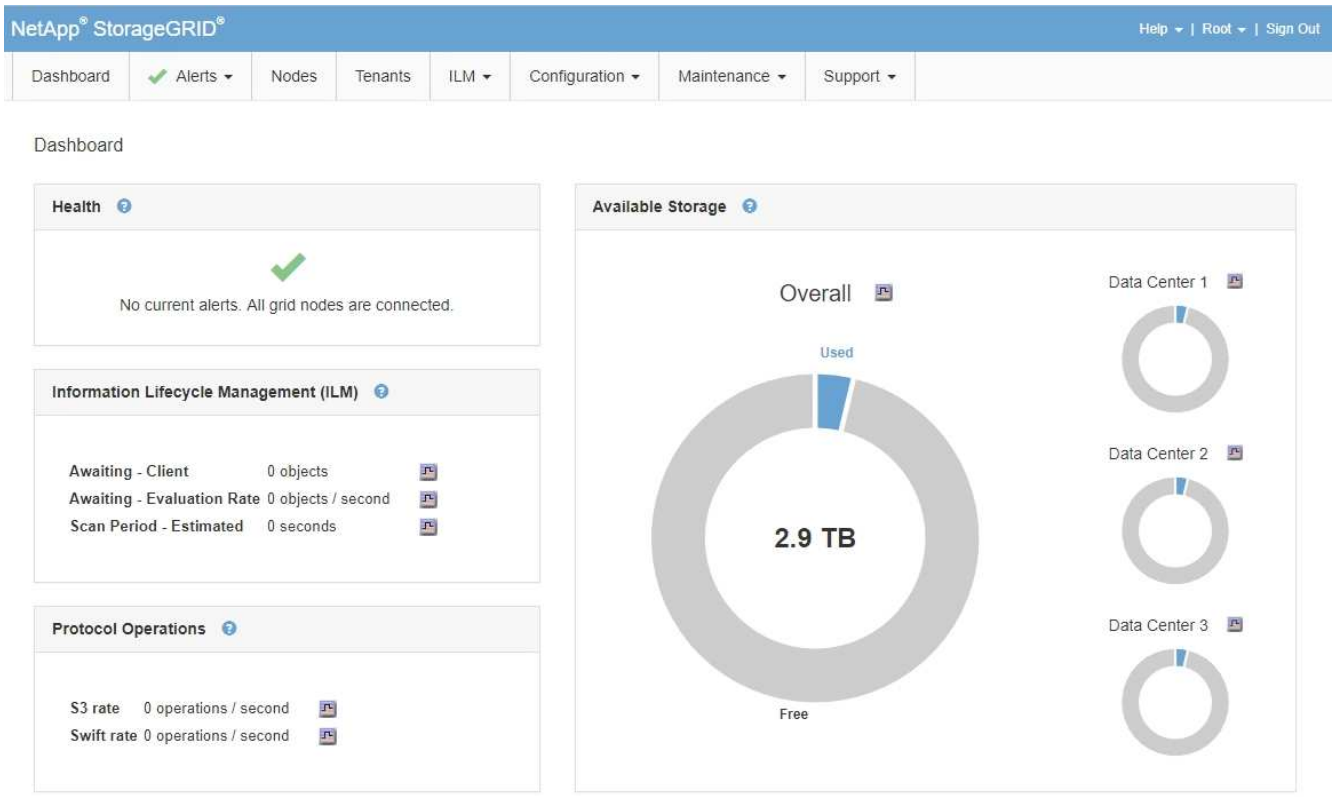
Você pode exibir o número de objetos que estão na fila a serem avaliados em relação à política ILM a qualquer momento. Você pode querer monitorar a fila de processamento ILM para determinar o desempenho do sistema. Uma fila grande pode indicar que o sistema não é capaz de acompanhar a taxa de ingestão, a carga dos aplicativos cliente é muito grande ou que existe alguma condição anormal.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Painel**.



2. Monitore a seção Gerenciamento do ciclo de vida das informações (ILM).

   Você pode clicar no ponto de interrogação para ver uma descrição dos itens nesta seção.

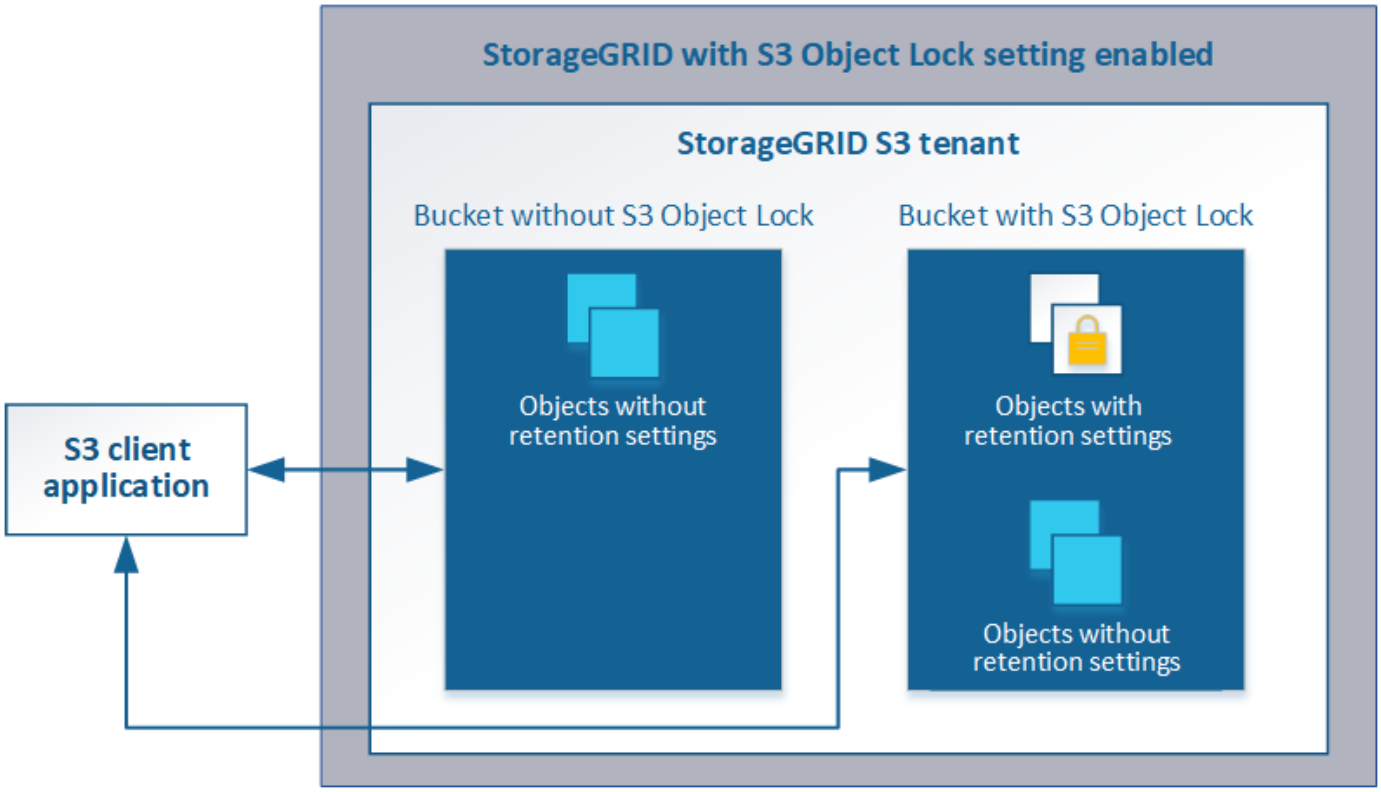
Gerenciando objetos com o S3 Object Lock

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).

Como mostrado na figura, quando a configuração global de bloqueio de objeto S3D está ativada para um sistema StorageGRID, uma conta de locatário S3D pode criar buckets com ou sem bloqueio de objeto S3D ativado. Se um bucket tiver o bloqueio de objeto S3 ativado, os aplicativos cliente S3 podem, opcionalmente, especificar configurações de retenção para qualquer versão de objeto nesse bucket. Uma versão de objeto deve ter configurações de retenção especificadas para ser protegida pelo bloqueio de objeto S3.



O recurso bloqueio de objetos do StorageGRID S3 fornece um modo de retenção único equivalente ao modo de conformidade do Amazon S3. Por padrão, uma versão de objeto protegido não pode ser substituída ou excluída por nenhum usuário. O recurso bloqueio de objetos do StorageGRID S3 não suporta um modo de governança e não permite que usuários com permissões especiais ignorem as configurações de retenção ou excluam objetos protegidos.

Se um bucket tiver o bloqueio de objeto S3 ativado, o aplicativo cliente S3 pode, opcionalmente, especificar uma ou ambas as seguintes configurações de retenção no nível do objeto ao criar ou atualizar um objeto:

- **Retent-until-date**: Se a data de retent-until de uma versão de objeto for no futuro, o objeto pode ser recuperado, mas não pode ser modificado ou excluído. Conforme necessário, a data de retenção até um objeto pode ser aumentada, mas essa data não pode ser diminuída.
- **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.

Para obter detalhes sobre essas configurações, vá para ""usando o bloqueio de objetos S3"" em "S3 operações e limitações suportadas pela API REST".

Comparação do S3 Object Lock com a conformidade legada

O recurso bloqueio de objetos S3 no StorageGRID 11,5 substitui o recurso de conformidade que estava disponível nas versões anteriores do StorageGRID. Como o novo recurso de bloqueio de objetos do S3 está em conformidade com os requisitos do Amazon S3, ele deprecia o recurso proprietário de conformidade do StorageGRID, que agora é conhecido como ""conformidade legada"".

Se você ativou anteriormente a configuração de conformidade global, a nova configuração global de bloqueio

de objetos S3 será ativada automaticamente quando você atualizar para o StorageGRID 11,5. Os usuários do locatário não poderão mais criar novos buckets com a conformidade habilitada no StorageGRID 11,5. No entanto, conforme necessário, os usuários do locatário podem continuar a usar e gerenciar quaisquer buckets em conformidade legados existentes, incluindo a realização das seguintes tarefas:

- Inserir novos objetos em um bucket existente que tenha a conformidade legada habilitada.
- Aumento do período de retenção de um bucket existente que tem a conformidade legada habilitada.
- Alterar a configuração de exclusão automática para um bucket existente que tenha conformidade legada ativada.
- Colocar uma retenção legal em um bucket existente que tenha a conformidade legada habilitada.
- Levantar uma retenção legal.

"Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

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.

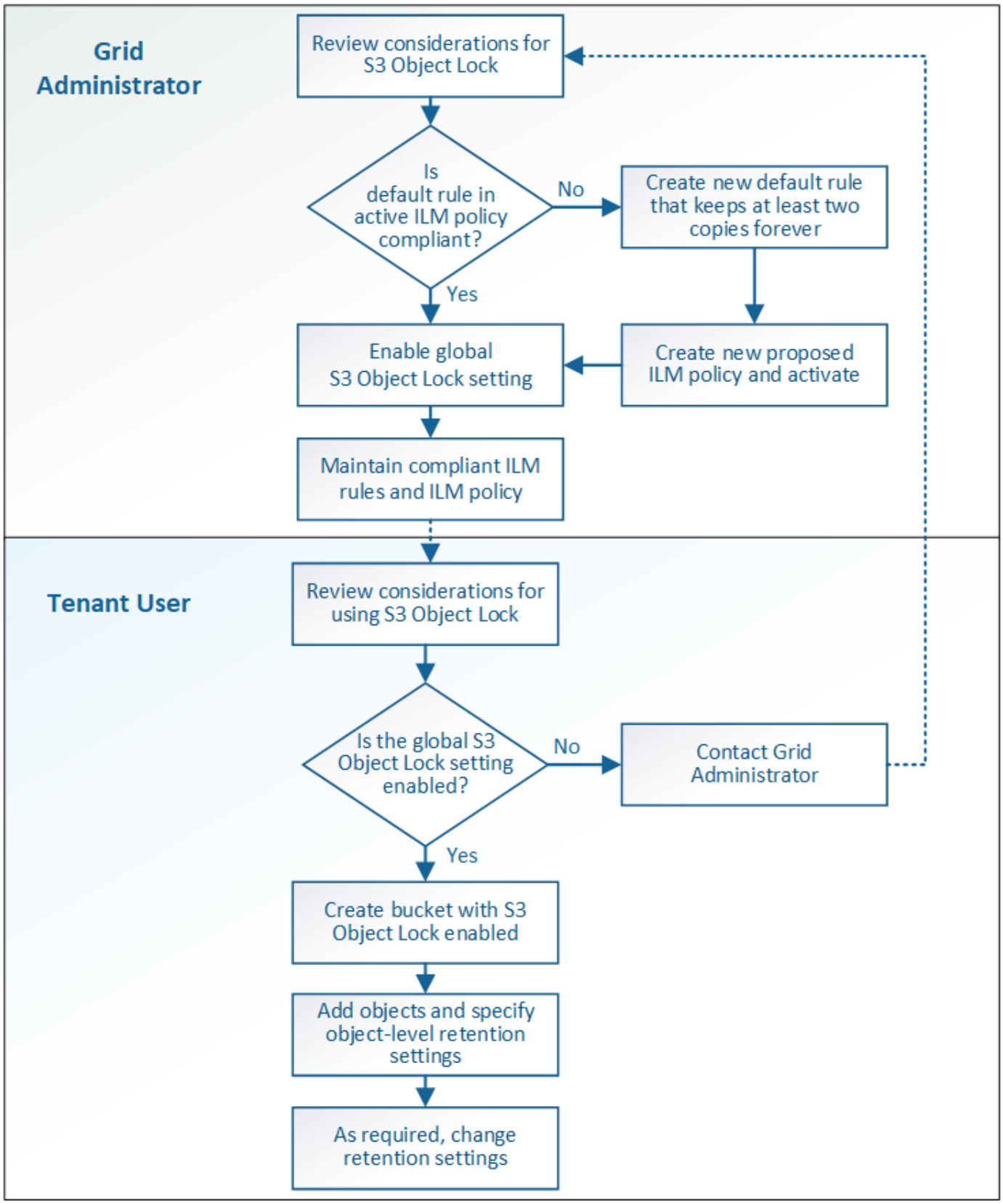
	S3 bloqueio de objetos (novo)	**Conformidade (legado)**
Como o recurso é ativado globalmente?	No Gerenciador de Grade, selecione **Configuração** > **Configurações do sistema** > **bloqueio de objetos S3**.	Já não é suportado. **Observação:** se você ativou previamente a configuração de conformidade global, a configuração global de bloqueio de objetos S3 será ativada automaticamente quando você atualizar para o StorageGRID 11,5.
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.	Os usuários não podem mais criar novos buckets com a conformidade ativada. No entanto, eles podem continuar adicionando novos objetos aos buckets em conformidade existentes.
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. O recurso de conformidade legado não permite o controle de versão do bucket.
Como a retenção de objetos é definida?	Os usuários podem definir uma data de retenção até cada versão do objeto.	Os usuários devem definir um período de retenção para todo o bucket. O período de retenção aplica-se a todos os objetos no balde.

	S3 bloqueio de objetos (novo)	Conformidade (legado)
Um bucket pode ter configurações padrão para retenção e retenção legal?	Não. Os buckets StorageGRID que têm o bloqueio de objeto S3 ativado não têm um período de retenção predefinido. Em vez disso, você pode especificar uma data de retenção até cada versão do objeto.	Sim
O período de retenção pode ser alterado?	A data de retenção até uma versão de objeto pode ser aumentada, mas nunca diminuída.	O período de retenção do 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?	Uma versão de objeto pode ser excluída após a data de retenção ser alcançada, assumindo que o objeto não está 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

Fluxo de trabalho para S3 Object Lock

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.

O diagrama de fluxo de trabalho mostra as etapas de alto nível para usar o bloqueio de objetos S3D. Estas etapas são executadas pelo administrador da grade e pelos usuários do locatário.



Tarefas de administração de grade

Como mostra o diagrama de fluxo de trabalho, um administrador de grade deve executar duas tarefas de alto nível antes que os usuários de S3 locatários possam usar o bloqueio de objeto S3:

1. Crie pelo menos uma regra ILM compatível e torne essa regra a regra padrão na política ILM ativa.
2. Ative a configuração global de bloqueio de objetos S3D para todo o sistema StorageGRID.

Tarefas do usuário do locatário

Depois que a configuração global S3 Object Lock for ativada, os locatários podem executar estas tarefas:

1. Crie buckets que tenham o bloqueio de objeto S3 ativado.
2. Adicione objetos a esses buckets e especifique períodos de retenção no nível do objeto e configurações de retenção legal.
3. Conforme necessário, atualize um período de retenção ou altere a configuração de retenção legal para um objeto individual.

Informações relacionadas

"Use uma conta de locatário"

"Use S3"

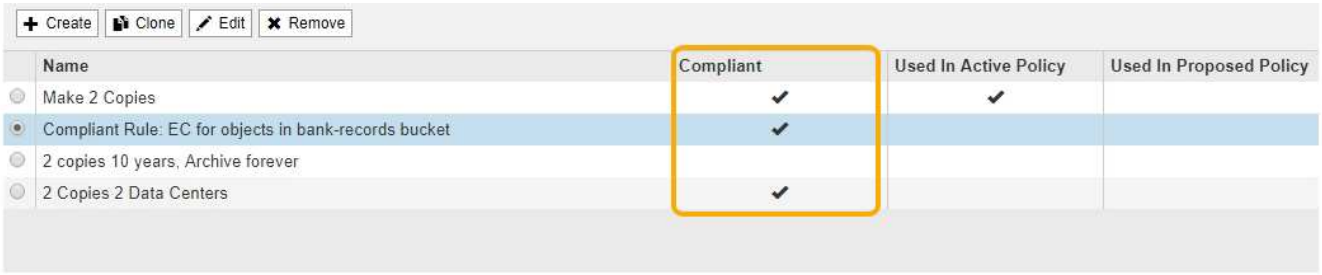
Requisitos para o bloqueio de objetos S3

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 na política ILM ativa 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, não é possível criar uma nova política ILM proposta ou ativar uma política ILM proposta existente, a menos que a regra padrão da política seja compatível. Depois que a configuração global S3 Object Lock tiver sido ativada, as páginas ILM Rules e ILM Policies indicam quais regras ILM são compatíveis.

  No exemplo a seguir, a página regras ILM lista três regras que são compatíveis com buckets com o bloqueio de objeto S3 ativado.

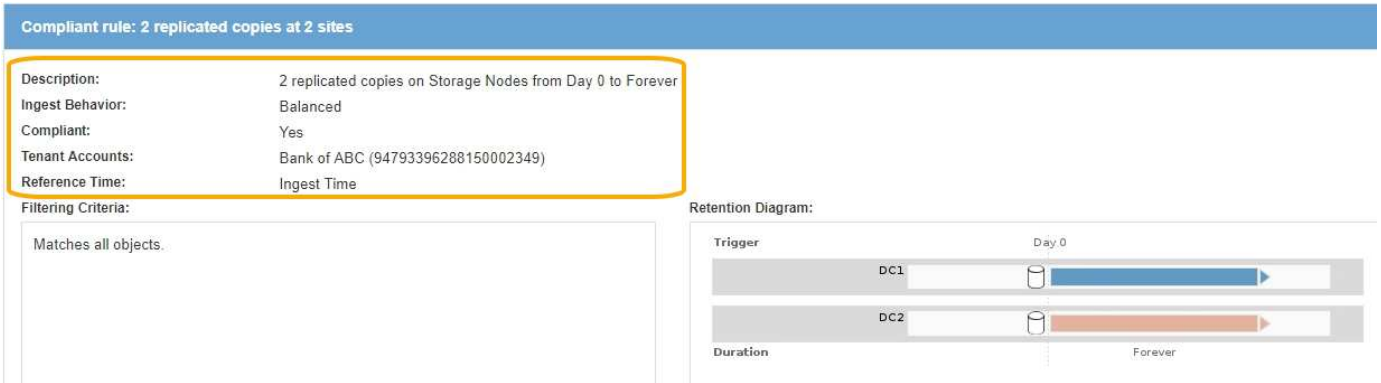


Requisitos para regras ILM compatíveis

Se você quiser ativar a configuração global S3 Object Lock, certifique-se de que a regra padrão na política ILM ativa 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 objeto não podem ser salvas em um pool de storage de nuvem.
- As cópias de objeto não podem ser guardadas nos nós de arquivo.
- 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".

Por exemplo, esta regra satisfaz os requisitos de buckets com o bloqueio de objeto S3 ativado. Ele armazena duas cópias de objeto replicadas do tempo de ingestão (dia 0) para "eternamente". Os objetos serão armazenados em nós de storage em dois data centers.



Requisitos para políticas de ILM ativas e propostas

Quando a configuração global S3 Object Lock está ativada, as políticas ILM ativas e propostas podem incluir regras compatíveis e não compatíveis.

- A regra padrão na política de ILM ativa ou proposta 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.

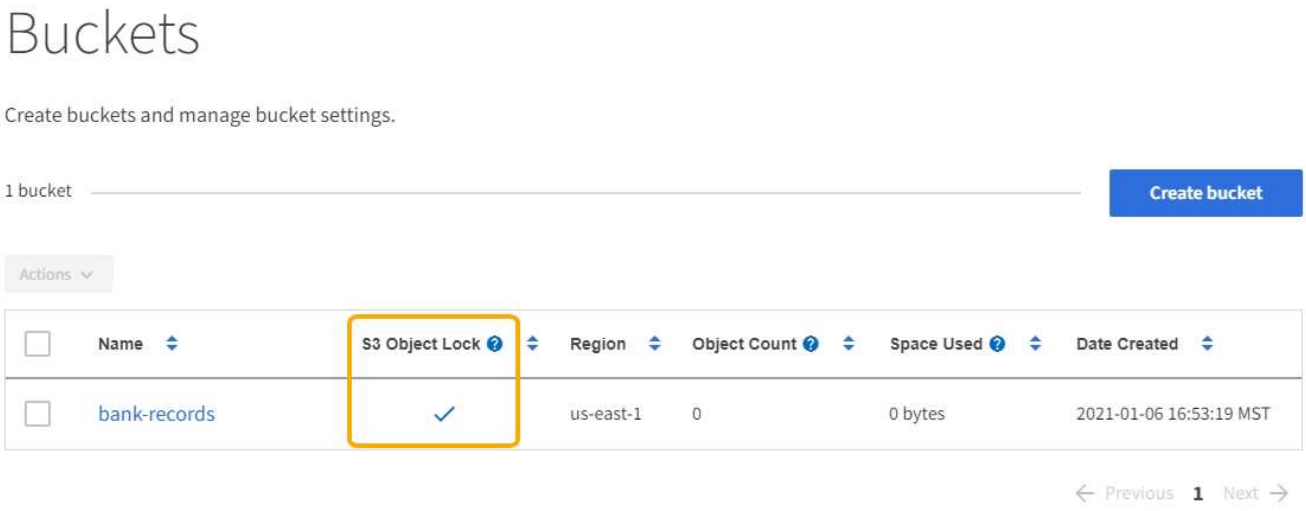
Uma política de ILM compatível pode incluir estas três regras:

1. Uma regra em conformidade que cria cópias codificadas de apagamento dos objetos em um bucket específico com o bloqueio de objeto S3 ativado. As cópias de EC são armazenadas 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 nós de arquivamento e armazenamentos que são copiados para sempre. Esta regra só se aplica a buckets que não têm o bloqueio de objeto S3 ou a conformidade legada ativada porque armazena apenas uma cópia de objeto para sempre e usa nós de arquivo.
3. Regra padrão em conformidade que cria duas cópias de objetos replicadas nos nós de storage do dia 0 para sempre. Esta regra se aplica a qualquer objeto em qualquer bucket que não tenha sido filtrado pelas duas primeiras regras.

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.

  Este exemplo do Gerenciador do Locatário mostra um bucket 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 S3D para um bucket existente.
- O controle de versão do bucket é necessário com o S3 Object Lock. Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket.
- Depois de criar um bucket com o bloqueio de objetos S3 ativado, não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão desse bucket.
- Um bucket do StorageGRID que tenha o bloqueio de objetos S3 ativado não tem um período de retenção padrão. Em vez disso, o aplicativo cliente S3 pode, opcionalmente, especificar uma data de retenção e uma configuração de retenção legal para cada versão de objeto adicionada a esse bucket.

- A configuração do ciclo de vida do bucket é compatível com buckets do ciclo de vida do objeto do S3.
- 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

- O aplicativo cliente S3 deve especificar configurações de retenção para cada objeto que precisa ser protegido pelo bloqueio de objetos S3.
- Você pode aumentar a data de retenção até uma versão de objeto, mas nunca pode diminuir esse valor.
- Se você for notificado de uma ação legal pendente ou investigação regulatória, poderá preservar informações relevantes colocando uma retenção legal em uma versão de objeto. Quando uma versão de objeto está sob uma retenção legal, esse objeto não pode ser excluído do StorageGRID, mesmo que tenha atingido sua data de retenção até. Assim que a retenção legal for levantada, a versão do objeto pode ser excluída se a data de retenção for atingida.
- S3 Object Lock requer o uso de buckets versionados. 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 três estágios:

1. * Ingestão de objetos*
   - Ao adicionar uma versão de objeto a um bucket com o bloqueio de objeto S3 ativado, o aplicativo cliente S3 pode, opcionalmente, especificar configurações de retenção para o objeto (reter até a data, retenção legal ou ambos). Em seguida, o StorageGRID gera metadados para esse objeto, que inclui um identificador de objeto exclusivo (UUID) e a data e hora de ingestão.
   - Depois que uma versão de objeto com configurações de retenção é ingerida, seus dados e metadados S3 definidos pelo usuário não podem ser modificados.
   - O StorageGRID armazena os metadados do objeto independentemente dos dados do objeto. Ele mantém três cópias de todos os metadados de objetos em cada local.
2. **Retenção de objetos**
   - Várias cópias do objeto são armazenadas pelo StorageGRID. O número exato e o tipo de cópias e os locais de storage são determinados pelas regras em conformidade na política de ILM ativa.
3. **Exclusão de objeto**
   - Um objeto pode ser excluído quando sua data de retenção é alcançada.
   - Não é possível eliminar um objeto que esteja sob uma guarda legal.

Informações relacionadas

"Use uma conta de locatário"

"Use S3"

"Comparação do S3 Object Lock com a conformidade legada"

"Exemplo 7: Política de ILM compatível para bloqueio de objetos S3"

"Rever registos de auditoria"

Habilitando 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.

O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter revisado o fluxo de trabalho do S3 Object Lock e você deve entender as considerações.
- A regra padrão na política ILM ativa deve ser compatível.

  "Criando uma regra ILM padrão"

  "Criando uma política ILM"

Sobre esta tarefa

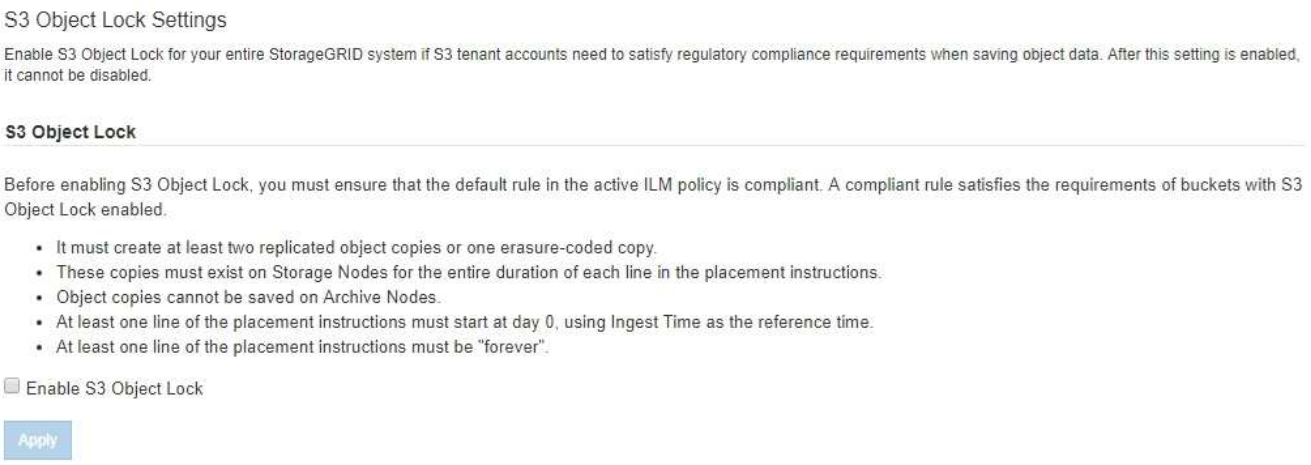
Um administrador de grade deve habilitar a configuração global S3 Object Lock para permitir que os usuários do locatário criem novos buckets com o S3 Object Lock ativado. Depois que esta definição estiver ativada, não poderá ser desativada.

> ⓘ Se você ativou a configuração de conformidade global usando uma versão anterior do StorageGRID, a nova configuração de bloqueio de objetos S3 será automaticamente ativada quando você atualizar para o StorageGRID versão 11,5. Você pode continuar usando o StorageGRID para gerenciar as configurações dos buckets em conformidade existentes. No entanto, não é possível criar mais buckets em conformidade.
>
> "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

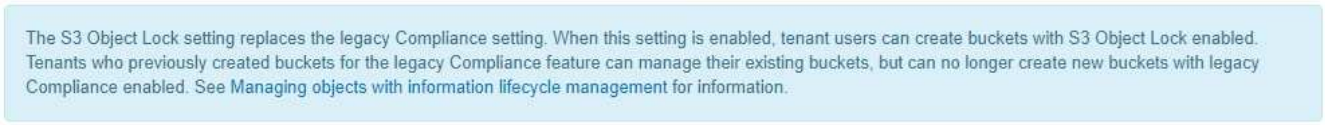
Passos

1. Selecione **Configuração** > **Definições do sistema** > **bloqueio de objetos S3**.

   A página Configurações de bloqueio de objetos S3 é exibida.

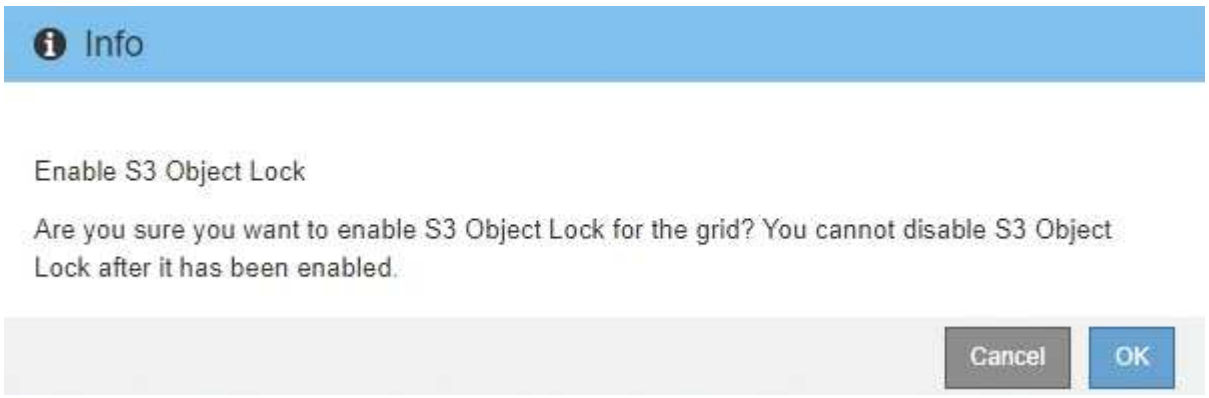


Se você ativou a configuração de conformidade global usando uma versão anterior do StorageGRID, a página inclui a seguinte nota:



2. Selecione **Ativar bloqueio de objetos S3**.
3. Selecione **aplicar**.

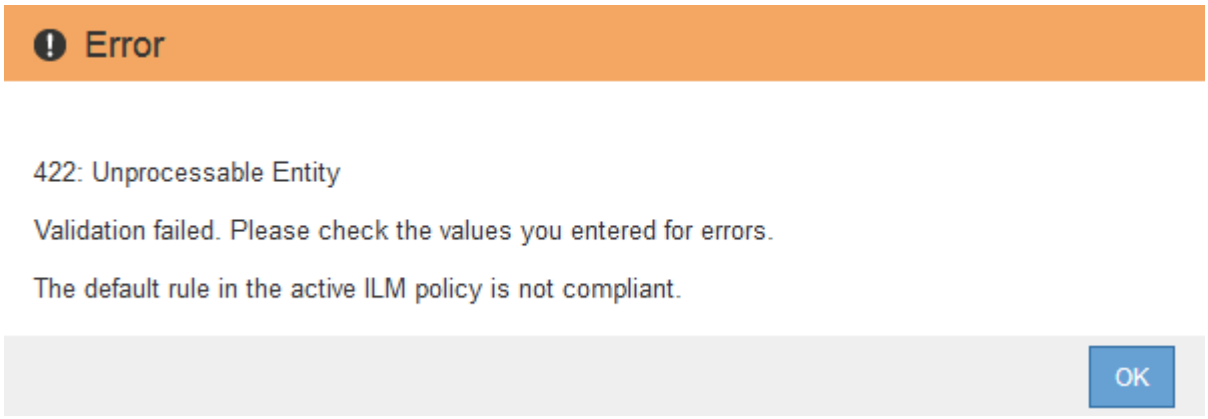
   Uma caixa de diálogo de confirmação é exibida e lembra que você não pode desativar o bloqueio de objeto S3 depois que ele estiver ativado.



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, indicando que você deve criar e ativar uma nova política ILM que inclua uma regra compatível como regra padrão. Selecione **OK** e crie uma nova política proposta, simule-a e ative-a.



Depois de terminar

Depois de ativar a configuração global S3 Object Lock, você pode querer criar uma nova política ILM. Depois que a configuração estiver ativada, a política ILM pode incluir opcionalmente uma regra padrão compatível e uma regra padrão não compatível. Por exemplo, você pode querer usar uma regra não compatível que não

tenha filtros para objetos em buckets que não tenham o bloqueio de objeto S3 ativado.

Informações relacionadas

"Criar uma política ILM depois que o bloqueio de objetos S3 estiver ativado"

"Criando uma regra ILM"

"Criando uma política ILM"

"Comparação do S3 Object Lock com a conformidade legada"

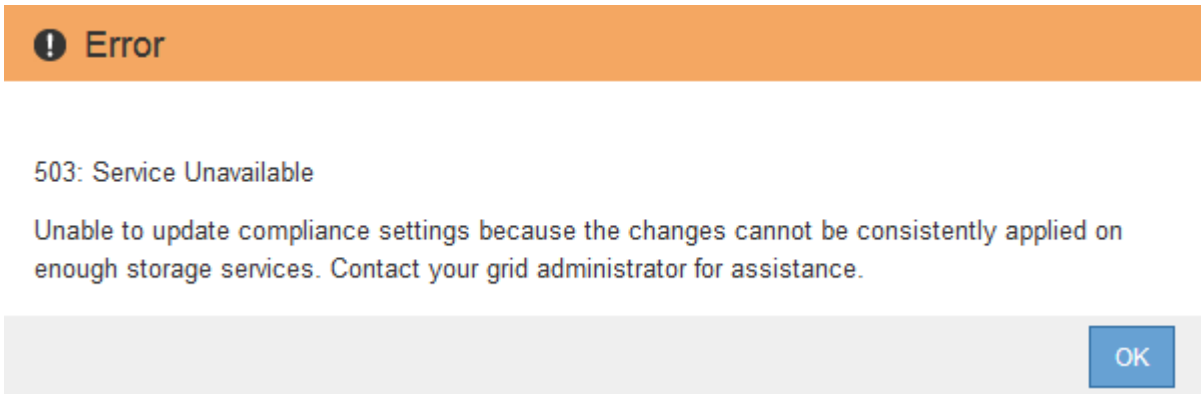
Resolução de erros de consistência ao atualizar o bloqueio de objetos S3 ou a configuração de conformidade legada

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 exibirá uma mensagem de erro. Especificamente:

- Os usuários do Gerenciador de locatários veem a seguinte mensagem de erro:



- Usuários de API de Gerenciamento de locatários e usuários de API S3 recebem um código de resposta de `503 Service Unavailable` texto de mensagem semelhante.

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 S3"

"Manter recuperar"

Exemplo de regras e políticas ILM

Você pode usar os exemplos nesta seção como um ponto de partida para suas próprias regras e políticas ILM.

- "Exemplo 1: Regras e política de ILM para armazenamento de objetos"
- "Exemplo 2: Regras de ILM e política para filtragem de tamanho de objeto EC"
- "Exemplo 3: Regras e política de ILM para melhor proteção para arquivos de imagem"
- "Exemplo 4: Regras ILM e política para objetos com versão S3"
- "Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"
- "Exemplo 6: Alterando uma política ILM"
- "Exemplo 7: Política de ILM compatível para bloqueio de objetos S3"

Exemplo 1: Regras e política de ILM para armazenamento de objetos

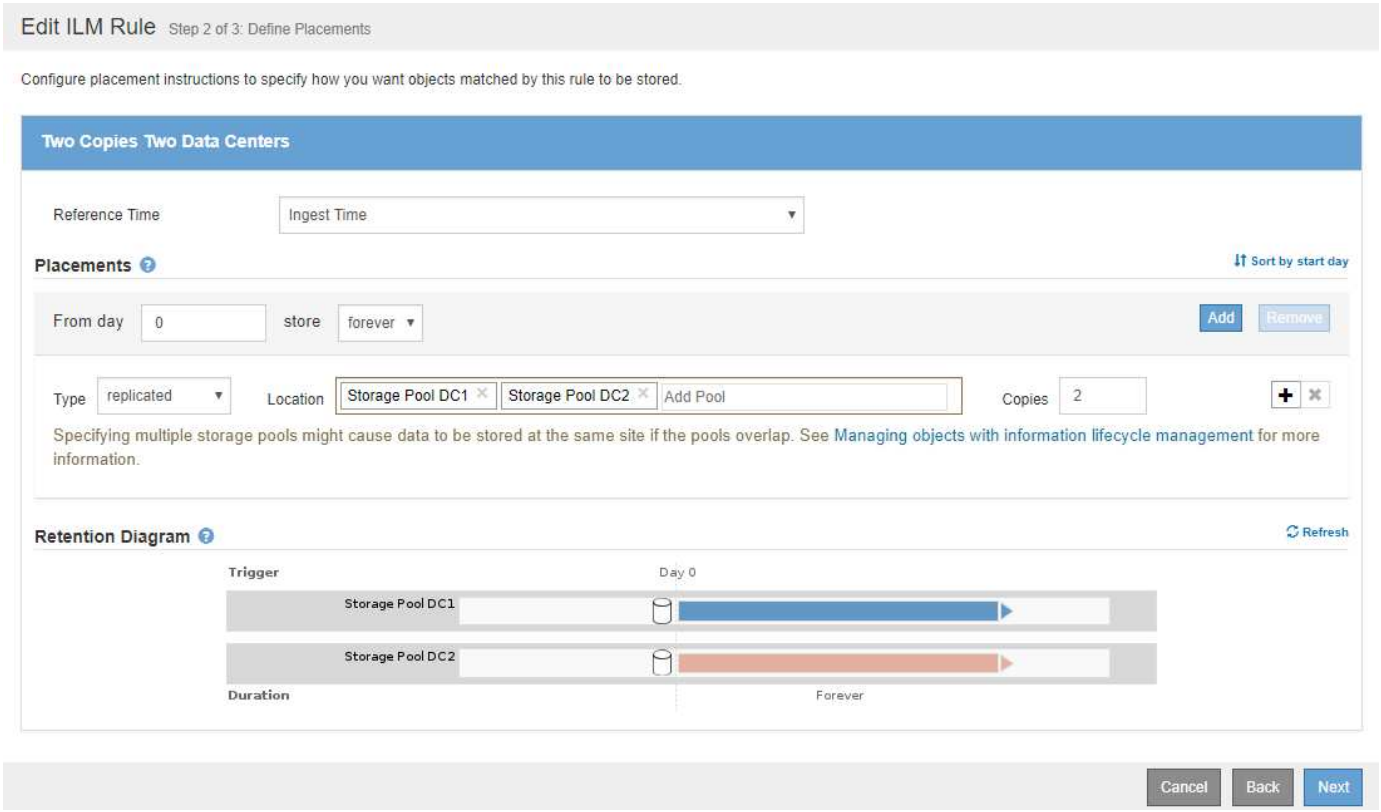
Você pode usar as seguintes regras e políticas de exemplo como ponto de partida ao definir uma política de ILM para atender aos requisitos de proteção e retenção de objetos.

> 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 política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Regra ILM 1 por exemplo 1: Copiar dados de objetos para dois data centers

Este exemplo de regra de ILM copia dados de objetos para pools de storage em dois data centers.

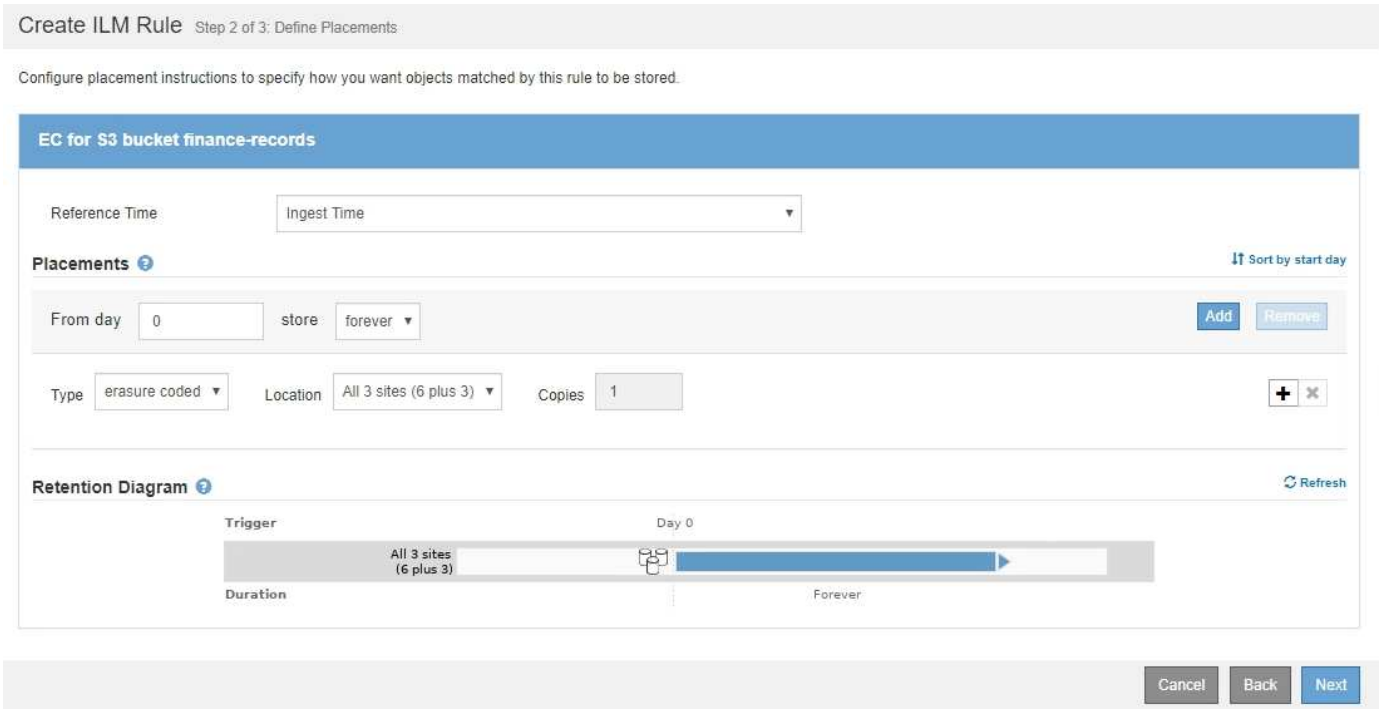
Definição de regra	Exemplo de valor
Pools de armazenamento	Dois pools de storage, cada um em data centers diferentes, denominados Storage Pool DC1 e Storage Pool DC2.
Nome da regra	Duas cópias de dois data centers
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	No dia 0, mantenha duas cópias replicadas para sempre: Uma no Storage Pool DC1 e uma no Storage Pool DC2.



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
Perfil de codificação de apagamento	• Um pool de storage em três data centers (todos os 3 locais) • Use o esquema de codificação de apagamento 6-3
Nome da regra	EC para Registros financeiros do bucket S3
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	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

O sistema StorageGRID permite que você projete políticas sofisticadas e complexas de ILM; no entanto, na prática, a maioria das políticas de ILM são simples.

Uma política ILM típica para uma topologia de vários sites pode incluir regras ILM, como as seguintes:

- Na ingestão, use a codificação de apagamento 6-3 para armazenar todos os objetos pertencentes ao bucket S3 nomeados `finance-records` em três data centers.
- 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 em dois data centers, DC1 e DC2.

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.

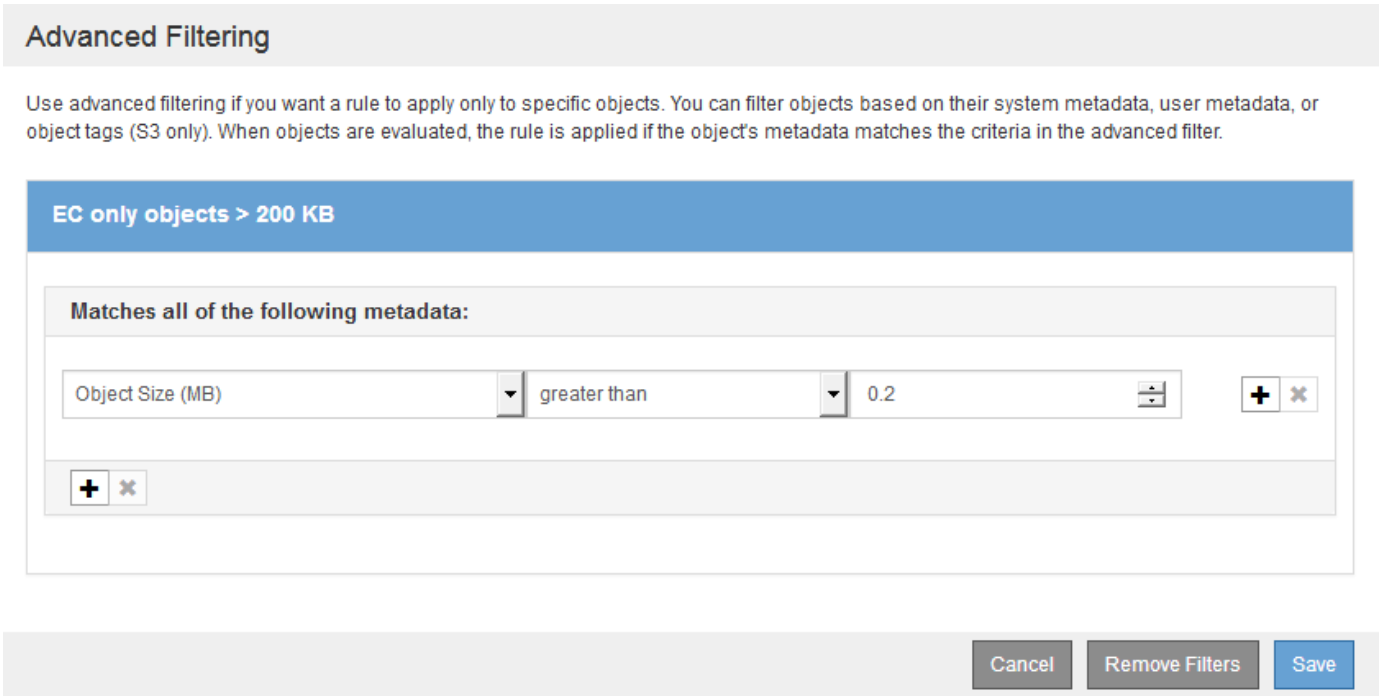
> As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule a política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Regra ILM 1 por exemplo 2: Use EC para todos os objetos maiores que 200 KB

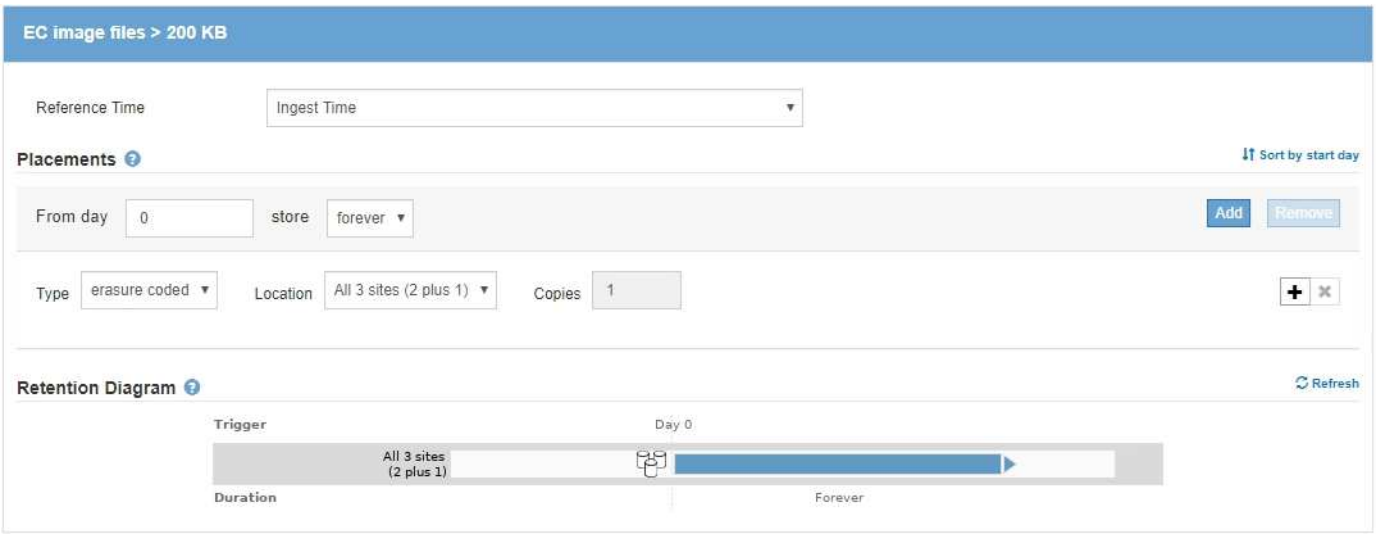
Este exemplo de exclusão de regra ILM codifica todos os objetos com mais de 200 KB (0,20 MB).

Definição de regra	Exemplo de valor
Nome da regra	Objetos somente EC > 200 KB

Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Filtragem Avançada para tamanho Objeto	Tamanho do objeto (MB) maior que 0,20
Colocação de conteúdo	Crie uma cópia codificada por apagamento 2-1 usando três sites



As instruções de colocação especificam que uma cópia codificada por apagamento 2-1 seja criada usando todos os três sites.

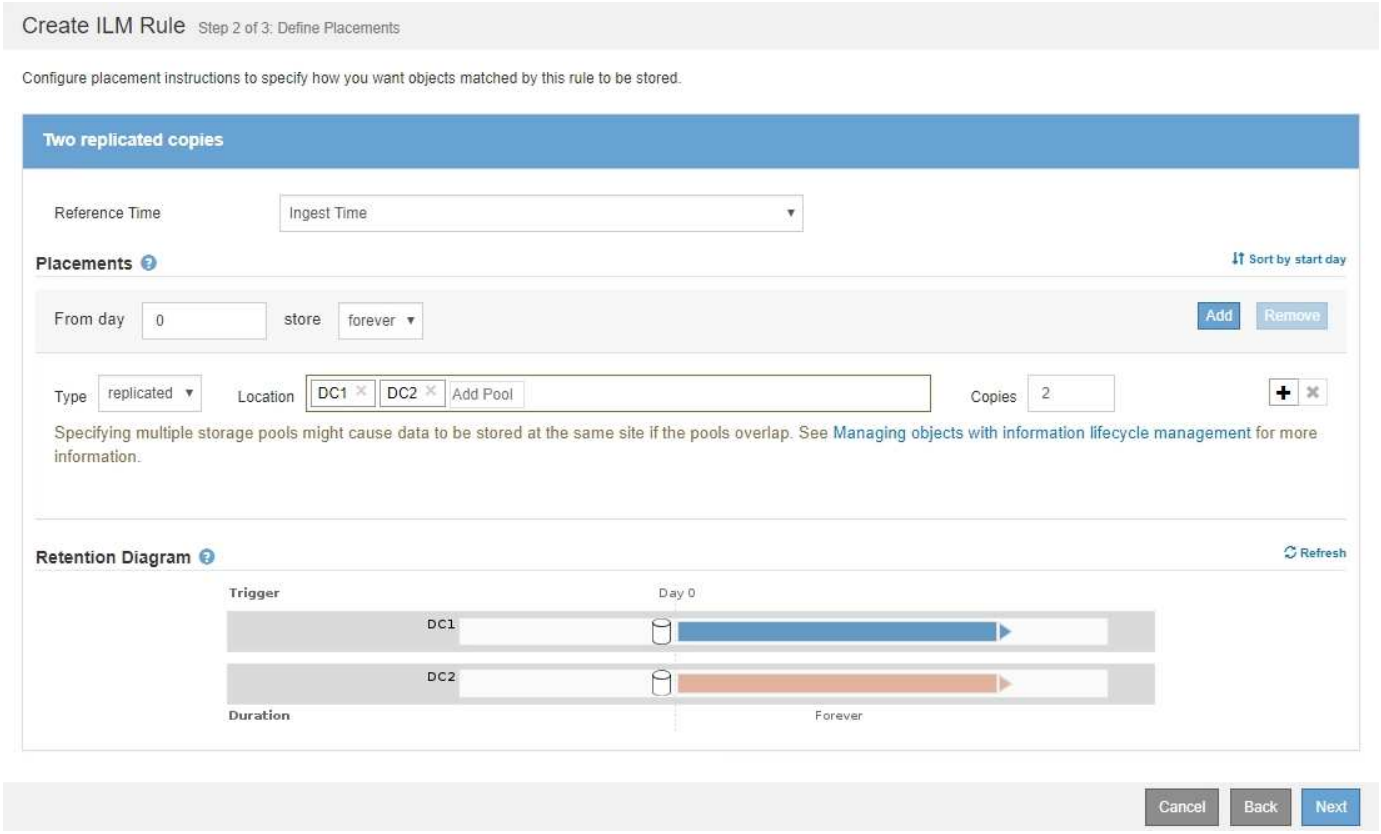


Regra ILM 2 por exemplo 2: Duas cópias replicadas

Este exemplo de regra ILM cria duas cópias replicadas e não filtra pelo tamanho do objeto. Esta regra é a

segunda regra da política. Como a regra ILM 1, por exemplo, 2, filtra todos os objetos maiores que 200 KB, a regra ILM 2, por exemplo, 2, aplica-se apenas a objetos com 200 KB ou menores.

Definição de regra	Exemplo de valor
Nome da regra	Duas cópias replicadas
Tempo de referência	Tempo de ingestão
Filtragem Avançada para tamanho Objeto	Nenhum
Colocação de conteúdo	Crie duas cópias replicadas e salve-as em dois data centers, DC1 e DC2



Política de ILM, por exemplo, 2: Use EC para objetos maiores que 200 KB

Nesta política de exemplo, objetos com mais de 200 KB são codificados para apagamento. Duas cópias replicadas são feitas de todos os outros objetos.

Este exemplo de política ILM inclui as seguintes regras ILM:

- Codificar para apagamento todos os objetos com mais de 200 KB.
- Se um objeto não corresponder à primeira regra ILM, use a regra ILM padrão para criar duas cópias replicadas desse objeto. Como objetos com mais de 200 KB foram filtrados pela regra 1, a regra 2 aplica-se apenas a objetos com 200 KB ou menos.

Exemplo 3: Regras e política de ILM para melhor proteção para arquivos de imagem

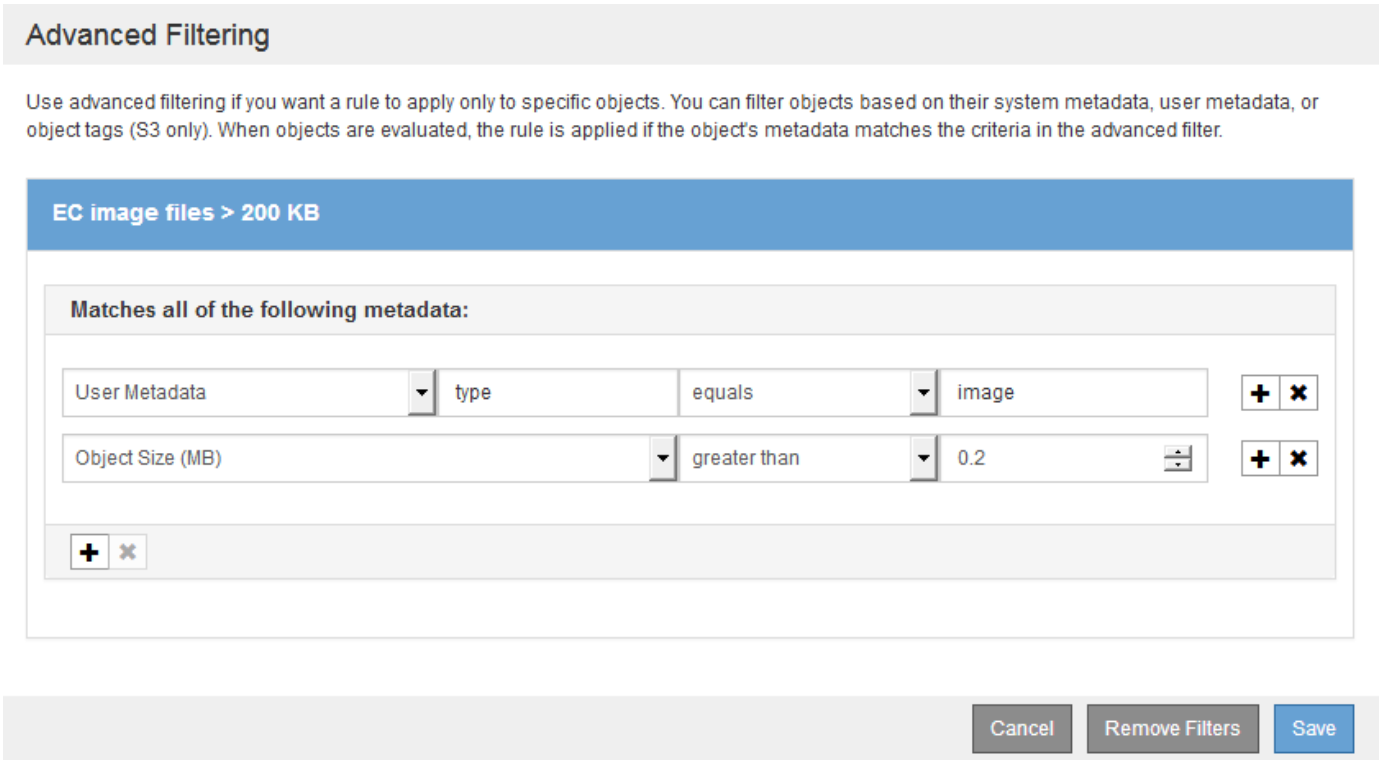
Você pode usar as regras e a política de exemplo a seguir para garantir que imagens maiores de 200 KB sejam codificadas para apagamento e que três cópias sejam feitas de imagens menores.

> 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 política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

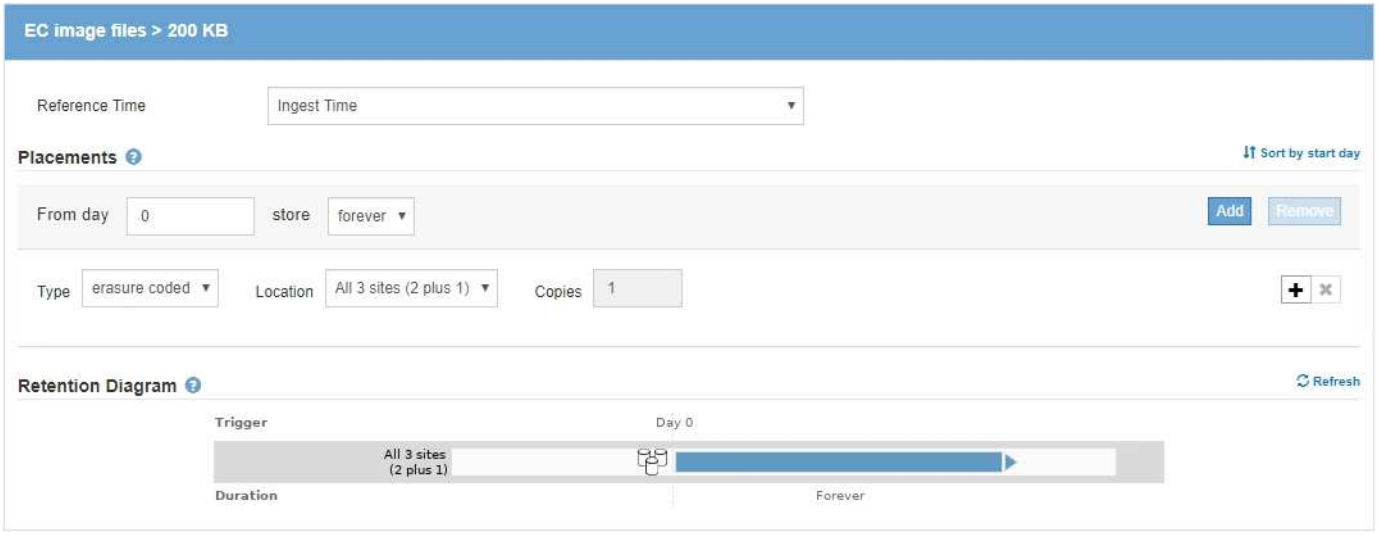
Regra ILM 1 por exemplo 3: Use EC para arquivos de imagem maiores que 200 KB

Este exemplo de regra ILM usa filtragem avançada para codificar todos os arquivos de imagem com mais de 200 KB.

Definição de regra	Exemplo de valor
Nome da regra	Ficheiros de imagem EC > 200 KB
Tempo de referência	Tempo de ingestão
Filtragem avançada para metadados do usuário	O tipo de metadados do usuário é igual a arquivos de imagem
Filtragem Avançada para tamanho Objeto	Tamanho do objeto (MB) maior que 0,2
Colocação de conteúdo	Crie uma cópia codificada por apagamento 2-1 usando três sites



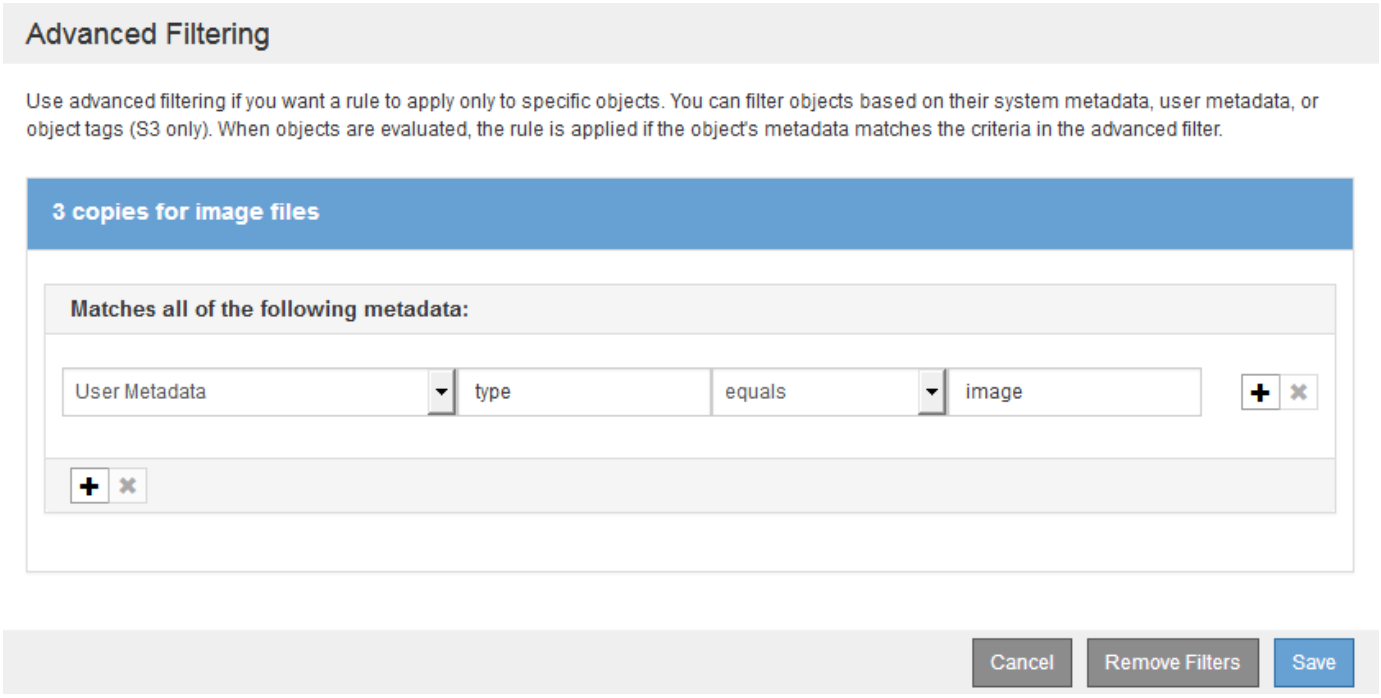
Como essa regra é configurada como a primeira regra na política, a instrução de posicionamento de codificação de apagamento só se aplica a imagens maiores que 200 KB.



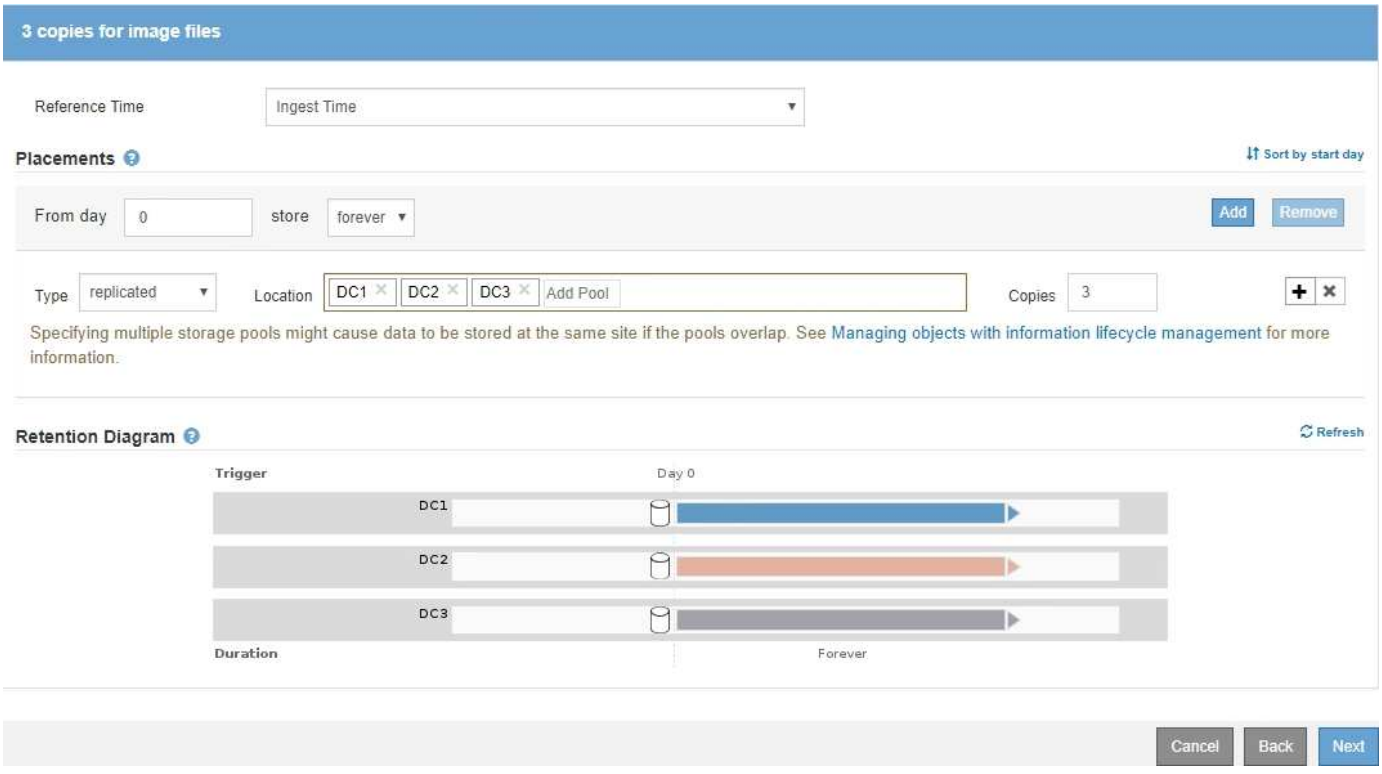
Regra ILM 2 por exemplo 3: Replique 3 cópias para todos os arquivos de imagem restantes

Este exemplo de regra ILM usa filtragem avançada para especificar que os arquivos de imagem sejam replicados.

Definição de regra	Exemplo de valor
Nome da regra	3 cópias para arquivos de imagem
Tempo de referência	Tempo de ingestão
Filtragem avançada para metadados do usuário	O tipo de metadados do usuário é igual a arquivos de imagem
Colocação de conteúdo	Crie 3 cópias replicadas em todos os nós de storage



Como a primeira regra na política já corresponde a arquivos de imagem maiores que 200 KB, essas instruções de colocação só se aplicam a arquivos de imagem 200 KB ou menores.



Política ILM, por exemplo, 3: Melhor proteção para arquivos de imagem

Neste exemplo, a política ILM usa três regras ILM para criar uma política que codifique arquivos de imagem com mais de 200 KB (0,2 MB), crie cópias replicadas para arquivos de imagem com 200 KB ou menos e faça duas cópias replicadas para qualquer arquivo que não seja de imagem.

Este exemplo de política ILM inclui regras que executam o seguinte:

- Todos os arquivos de imagem com mais de 200 KB.
- Crie três cópias de quaisquer arquivos de imagem restantes (ou seja, imagens com 200 KB ou menos).
- Aplique a regra padrão a quaisquer objetos restantes (ou seja, todos os 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 **hora não atual** como tempo de referência.

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 política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

> Se você criar políticas ILM para gerenciar versões de objetos não atuais, saiba que você deve conhecer o UUID ou CBID da versão do objeto para simular a política. Para encontrar UUUID e CBID de um objeto, use Object Metadata Lookup enquanto o objeto ainda estiver atual.

Informações relacionadas

"Como objetos com versão S3 são excluídos"

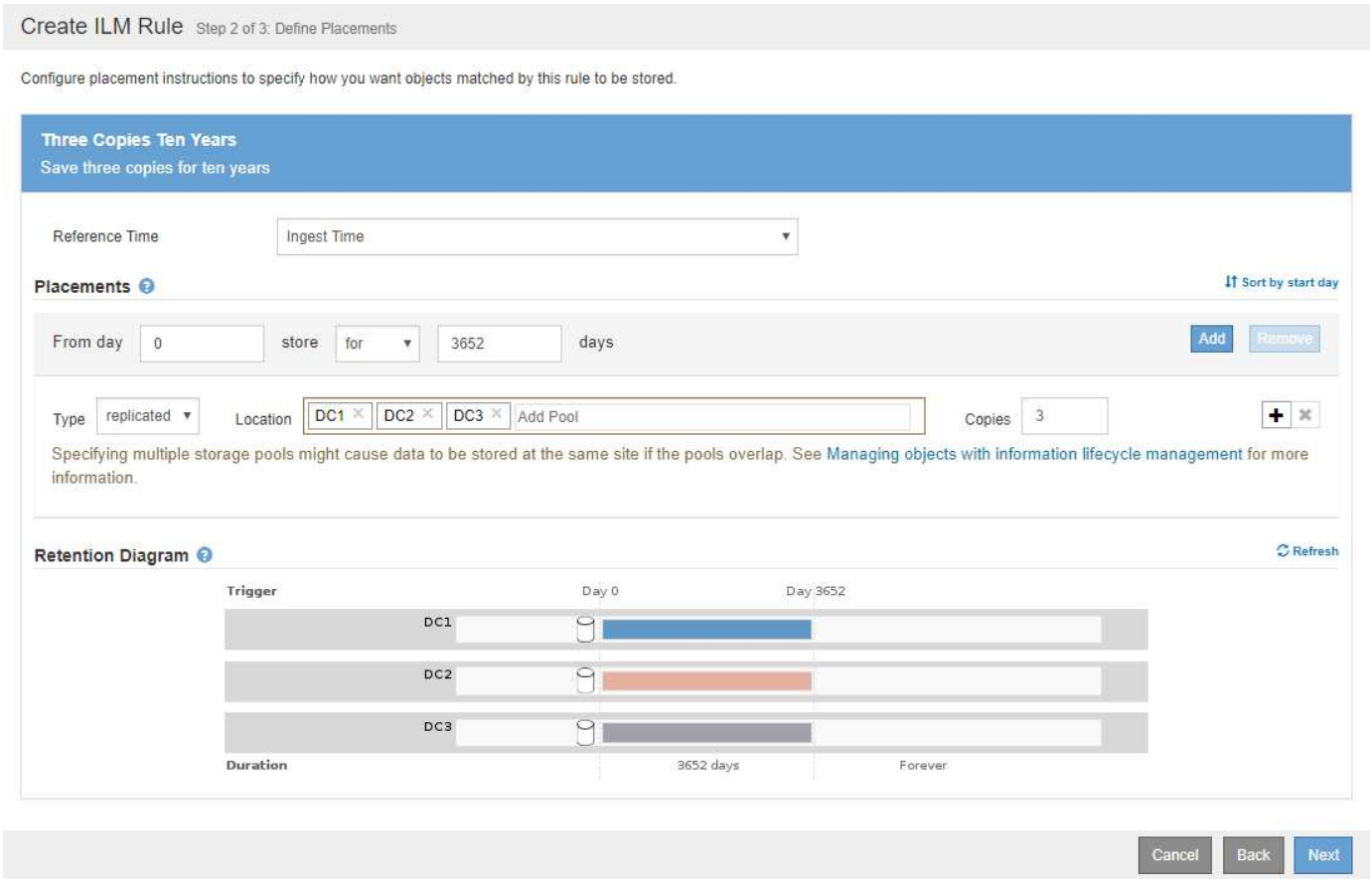
"Verificando uma política ILM com pesquisa de metadados de objeto"

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 data centers 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 storage, cada um em data centers diferentes, denominados DC1, DC2 e DC3.
Nome da regra	Três cópias dez anos
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	No dia 0, mantenha três cópias replicadas por 10 anos (3.652 dias), uma em DC1, uma em DC2 e uma em DC3. No final de 10 anos, exclua todas as cópias do objeto.



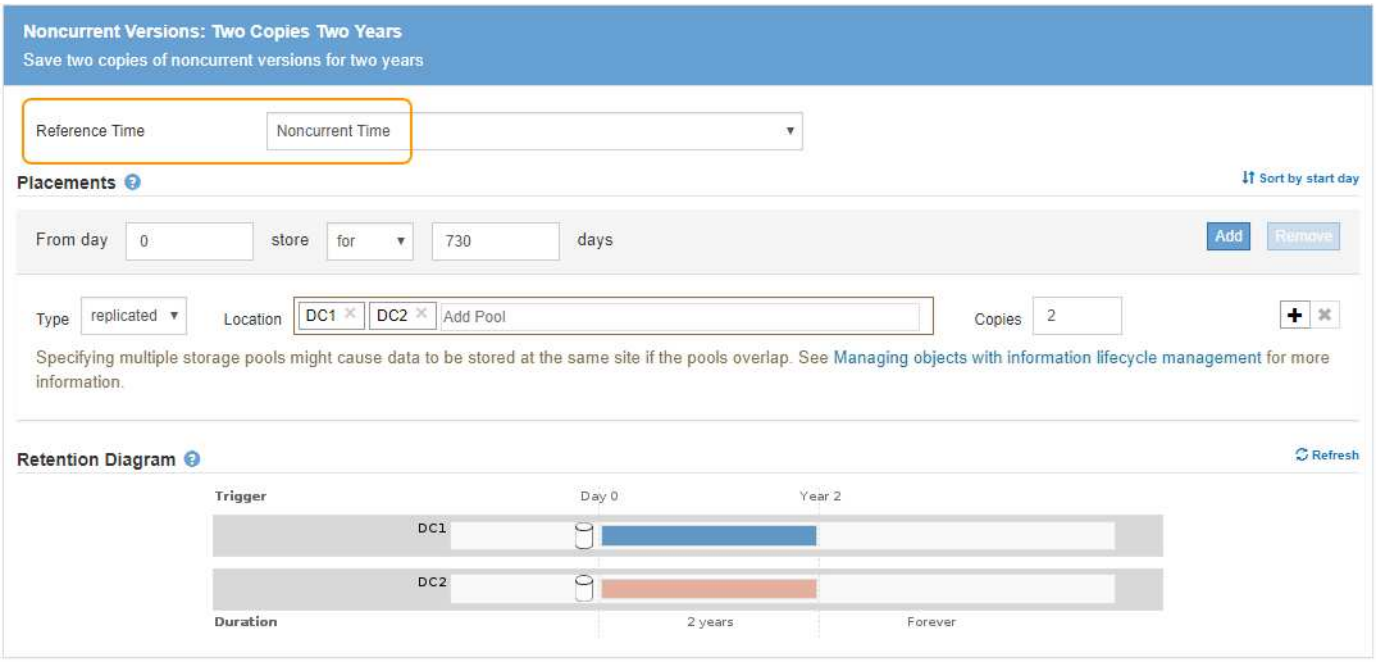
Regra ILM 2 por exemplo 4: Salve duas cópias de versões não atuais por 2 anos

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. Esta regra usa a opção **hora não atual** para hora de referência.

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 storage, cada um em data centers diferentes, denominados DC1 e DC2.
Nome da regra	Versões não atuais: Duas cópias dois anos
Tempo de referência	Hora não atual
Colocação de conteúdo	No dia 0 em relação à hora 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 em DC1 e uma em DC2. 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 tempo 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 de tempo não atual.

- Na obtenção, crie três cópias replicadas e armazene uma cópia em cada um dos três data centers. 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).

> Para simular versões de objetos não atuais, você deve usar o UUID ou CBID dessa versão. Enquanto o objeto ainda estiver atual, você pode usar a Pesquisa de metadados de Objeto para encontrar seus UUID e CBID.

- A versão atual do objeto seria correspondida pela segunda regra. Quando a versão atual do objeto for 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 ILM ocorrer, essa versão não atual é correspondida pela primeira regra. Como resultado, a cópia em DC3 é purgada e as duas cópias em DC1 e DC2 são armazenadas por mais 2 anos.

Informações relacionadas

"Verificando uma política ILM com pesquisa de metadados de objeto"

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 política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Informações relacionadas

"Como os objetos são ingeridos"

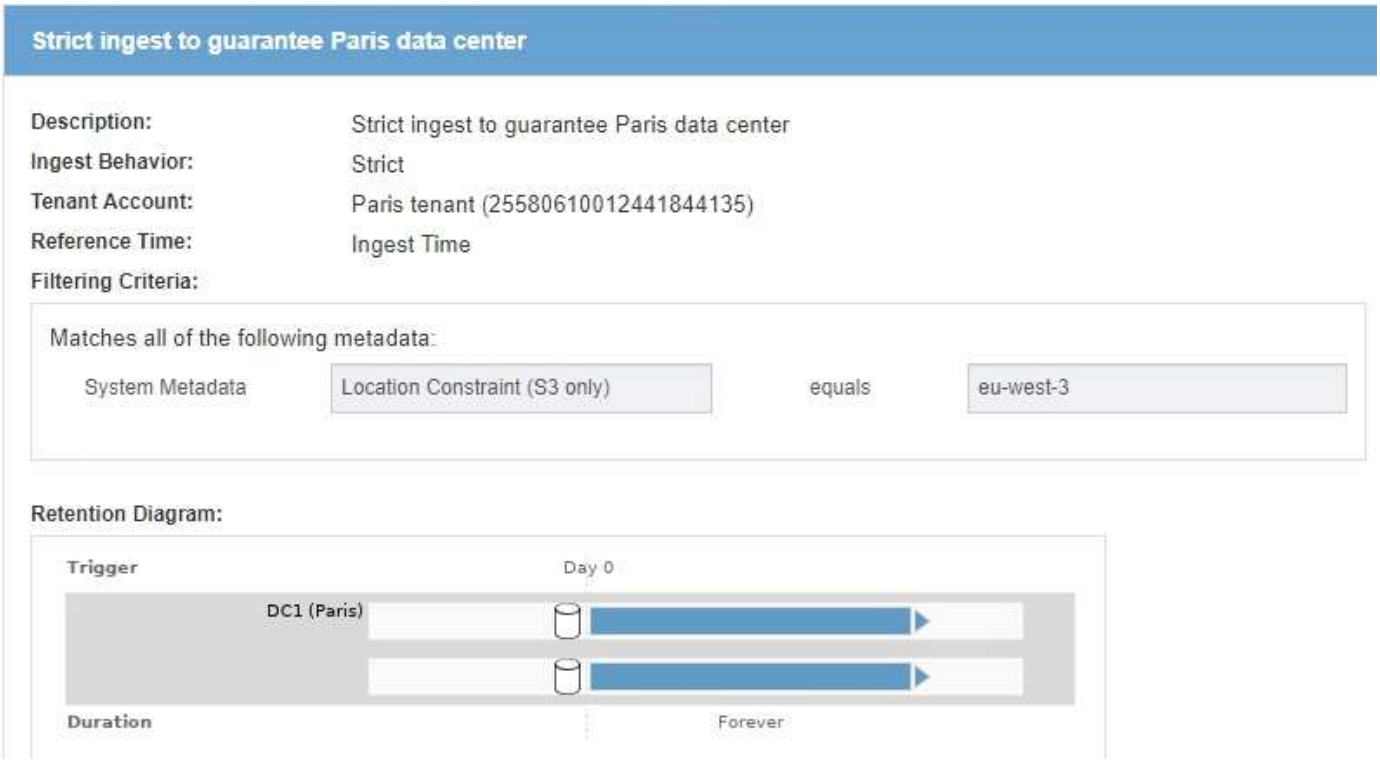
"Etapa 3 de 3: Definir o comportamento de ingestão"

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
Filtragem avançada	A restrição de localização é igual à eu-West-3
Pools de armazenamento	DC1 (Paris)
Nome da regra	Ingestão rigorosa para garantir o data center de Paris
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	No dia 0, mantenha duas cópias replicadas para sempre em DC1 (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.

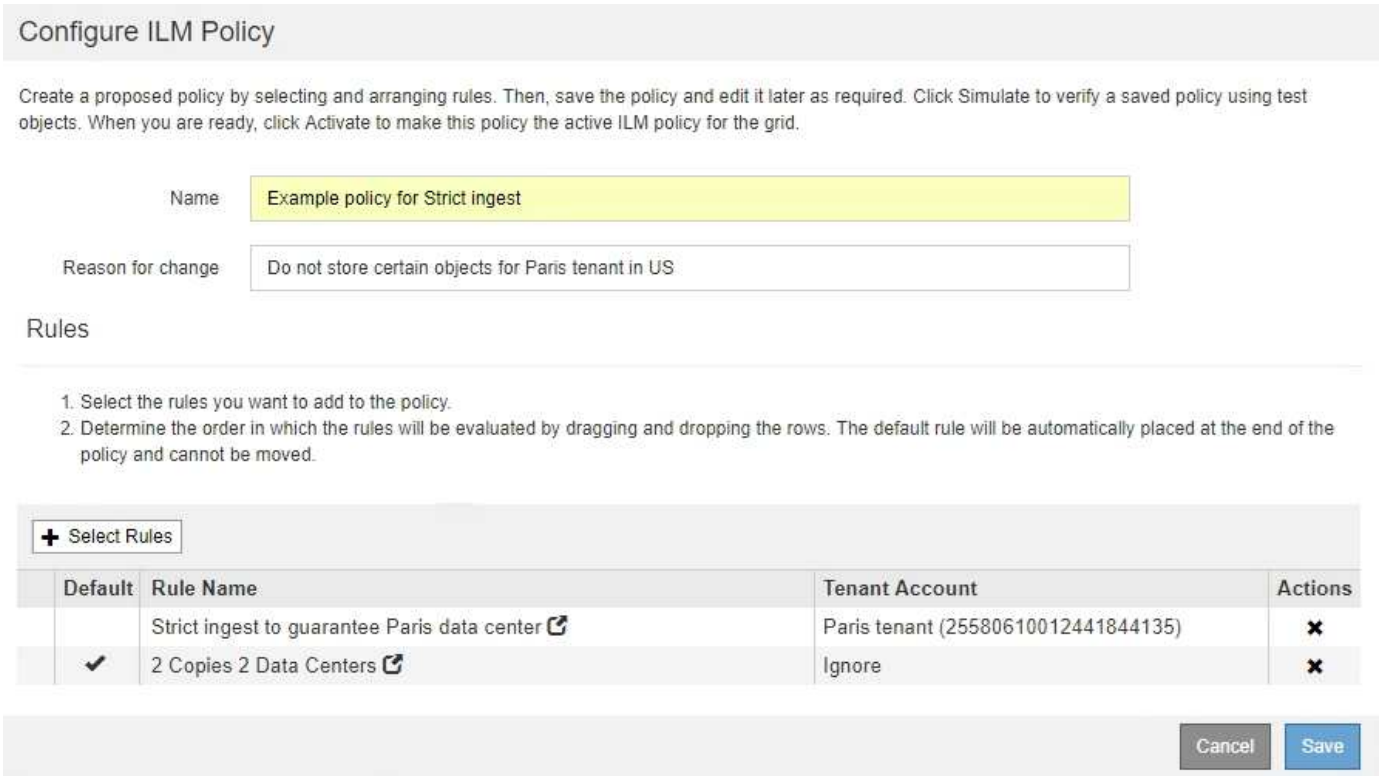
Definição de regra	Exemplo de valor
Conta de locatário	Ignorar
Filtragem avançada	*Não especificado*
Pools de armazenamento	DC1 (Paris) e DC2 (EUA)
Nome da regra	2 cópias 2 Data Centers
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	No dia 0, mantenha duas cópias replicadas para sempre em 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: Alterando uma política ILM

Talvez seja necessário criar e ativar uma nova política de ILM se sua proteção de dados precisar mudar ou adicionar novos sites.

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 a política ILM ativa precisa ser revisada para armazenar dados no novo site.

> 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 política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Como a alteração de 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.

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.

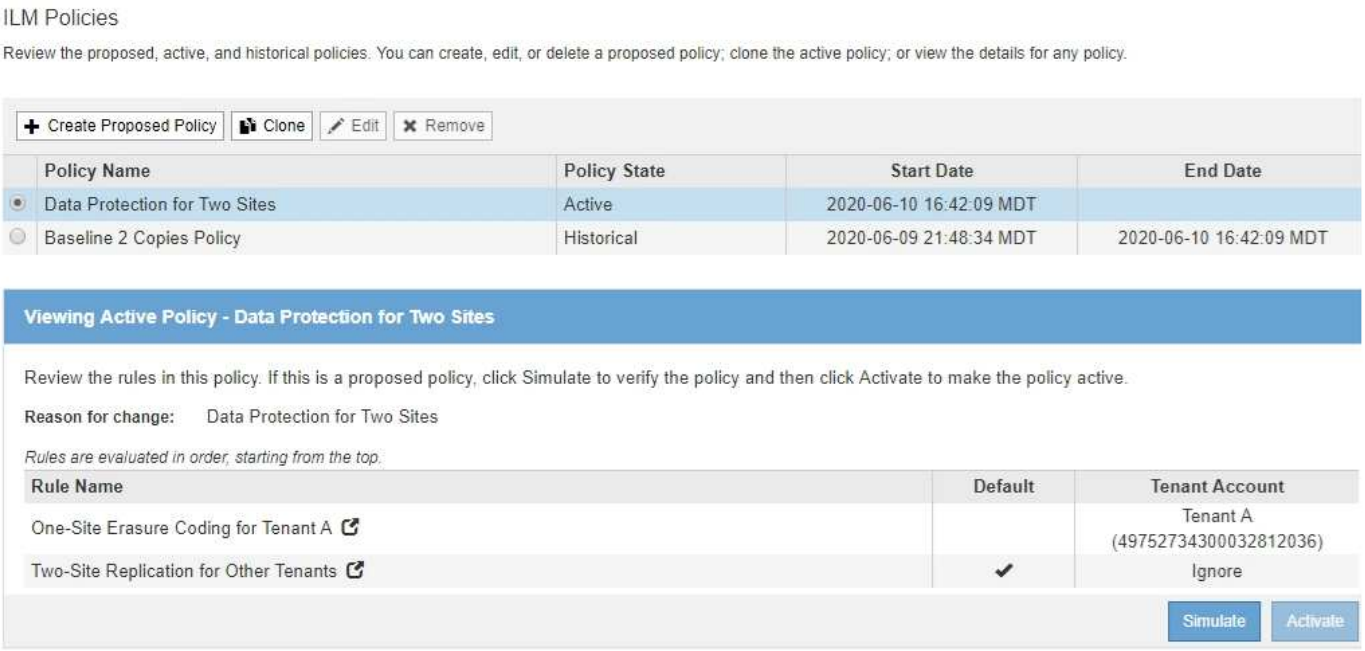
- Alterar o tipo de cópias necessárias para objetos existentes; por exemplo, converter uma grande porcentagem de objetos replicados em objetos codificados por apagamento.
- Mover cópias de objetos existentes para um local completamente diferente; por exemplo, mover um grande número de objetos de ou para um pool de armazenamento em nuvem ou de ou para um local remoto.

Informações relacionadas

"Criando uma política ILM"

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.

> A primeira regra neste exemplo usa um filtro avançado para garantir que a codificação de apagamento não seja usada para objetos pequenos. Qualquer um dos objetos do Tenant A menores de 200 KB será protegido pela segunda regra, que usa replicação.

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	Centro de dados 1
Colocação de conteúdo	Codificação de apagamento 2-1 no Data Center 1 do dia 0 para sempre

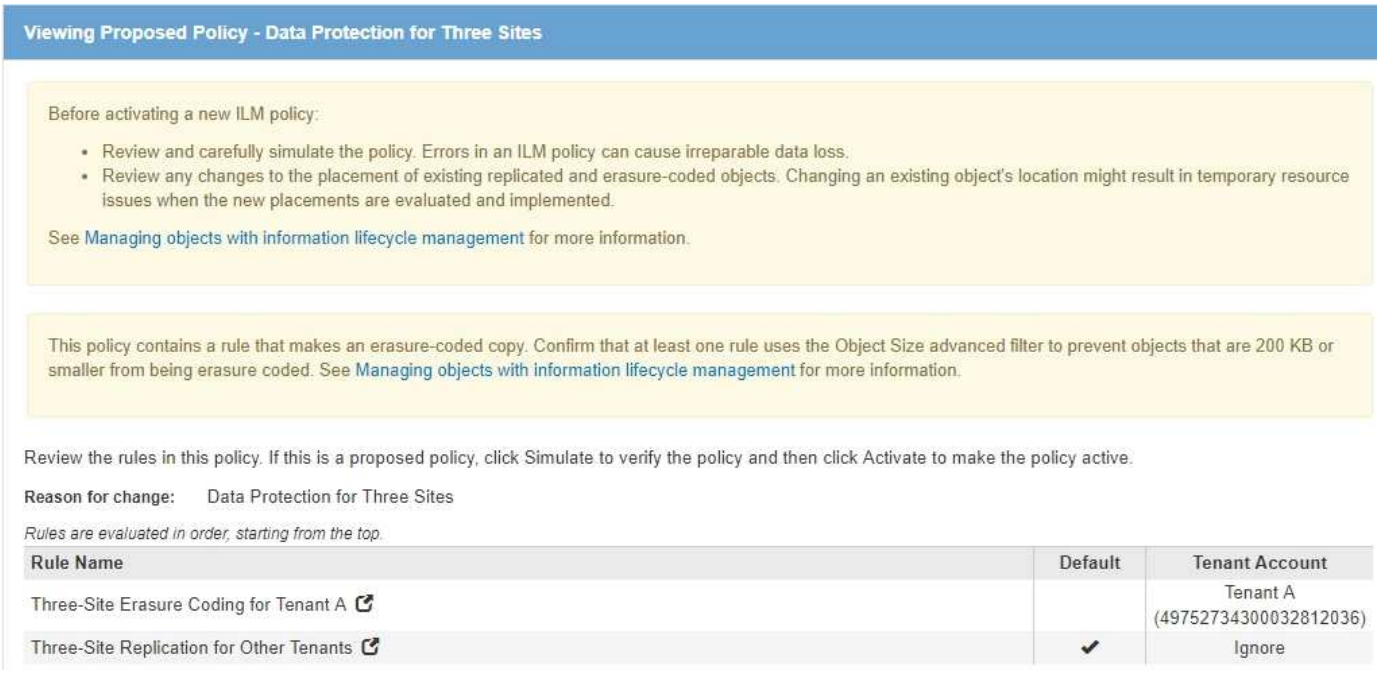
Regra 2: Replicação de dois locais para outros locatários

Definição de regra	Exemplo de valor
Nome da regra	Replicação de dois locais para outros locatários
Conta de locatário	Ignorar
Pools de armazenamento	Data Center 1 e data center 2
Colocação de conteúdo	Duas cópias replicadas do dia 0 para sempre: Uma cópia no data center 1 e uma cópia no data center 2.

Proposta de política de ILM, por exemplo, 6: Proteção de dados em três locais

Neste exemplo, a política ILM está sendo atualizada para um sistema StorageGRID de três locais.

Depois de executar uma expansão para adicionar o novo local, o administrador de grade criou dois novos pools de storage: Um pool de storage para o Data Center 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 proposta, que é 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 3 Data Centers (inclui Data Center 1, Data Center 2 e Data Center 3)
Colocação de conteúdo	Codificação de apagamento 2-1 em todos os 3 Data Centers, desde o dia 0 até 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	Data Center 1, Data Center 2 e Data Center 3
Colocação de conteúdo	Três cópias replicadas do dia 0 para sempre: Uma cópia no data center 1, uma cópia no data center 2 e uma cópia no data center 3.

Ativar a política de ILM proposta, por exemplo, 6

Quando você ativa uma nova política proposta de 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 Data Center 1. Na nova política proposta de ILM, os objetos pertencentes ao Tenant A serão protegidos usando codificação de apagamento 2-1 nos Data Centers 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 data center 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 data centers.

> Os fragmentos 2 mais 1 existentes no Data Center 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 Data Centers 1 e 2. Na nova política de ILM proposta, os objetos pertencentes a outros locatários serão protegidos usando três cópias replicadas em pools de storage nos Data Centers 1, 2 e 3.

Quando a nova política ILM é ativada, ocorrem as seguintes operações ILM:

- Quando qualquer Locatário que não o Locatário A ingere um novo objeto, o StorageGRID cria três cópias e salva uma cópia em cada data center.
- 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 Data Center 1 e no Data Center 2 continuam atendendo aos requisitos de replicação da nova regra ILM, o StorageGRID só precisa criar uma nova cópia do objeto para o Data Center 3.

Impacto da ativação desta política no desempenho

Quando a política de ILM proposta neste exemplo é ativada, o desempenho geral deste sistema StorageGRID será temporariamente afetado. Níveis mais altos 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 Data Center 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 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 política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Informações relacionadas

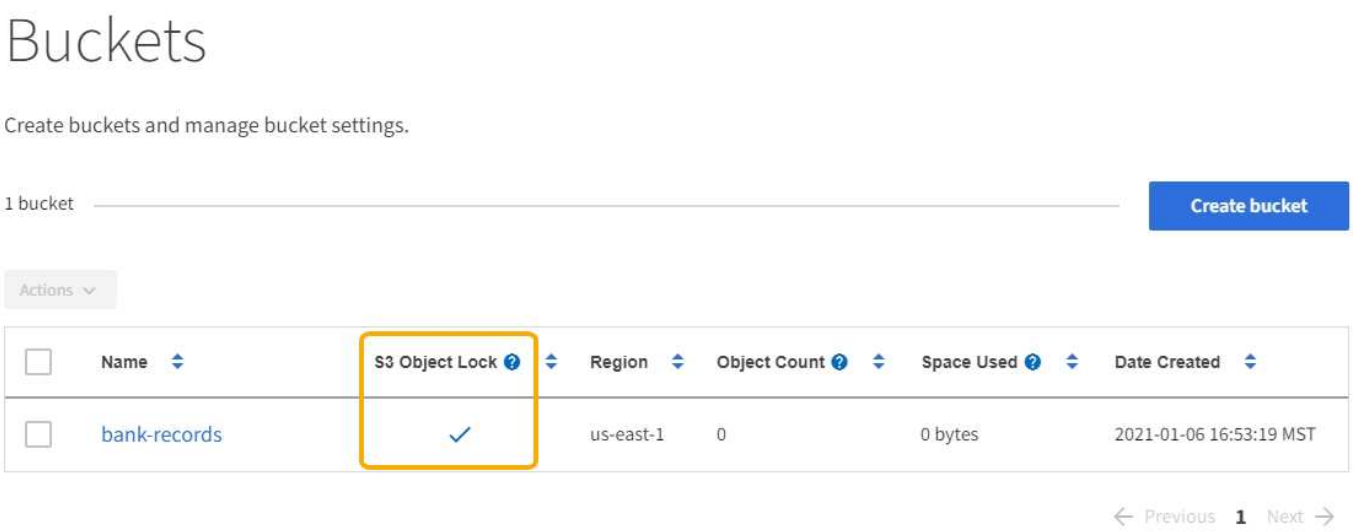
"Gerenciando objetos com o S3 Object Lock"

"Criando 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`.

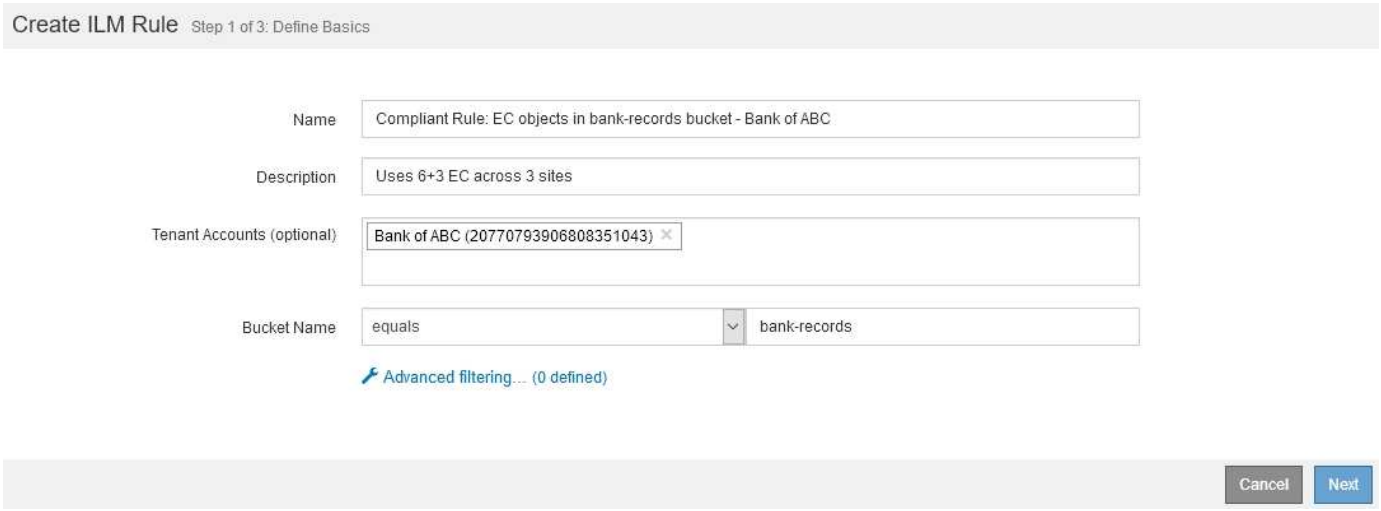
Definição para cada objeto	Exemplo de valor
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30 de dezembro de 2030) Cada versão de objeto tem sua `retain-until-date` própria configuração. Esta definição pode ser aumentada, mas não diminuída.
`legal hold`	`"OFF"` (Não em vigor) Uma retenção legal pode ser 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 pode ser excluído mesmo que o `retain-until-date` tenha sido alcançado.

Regra 1 do ILM para o bloqueio de objetos S3 exemplo: Perfil de codificação de apagamento com correspondência de bucket

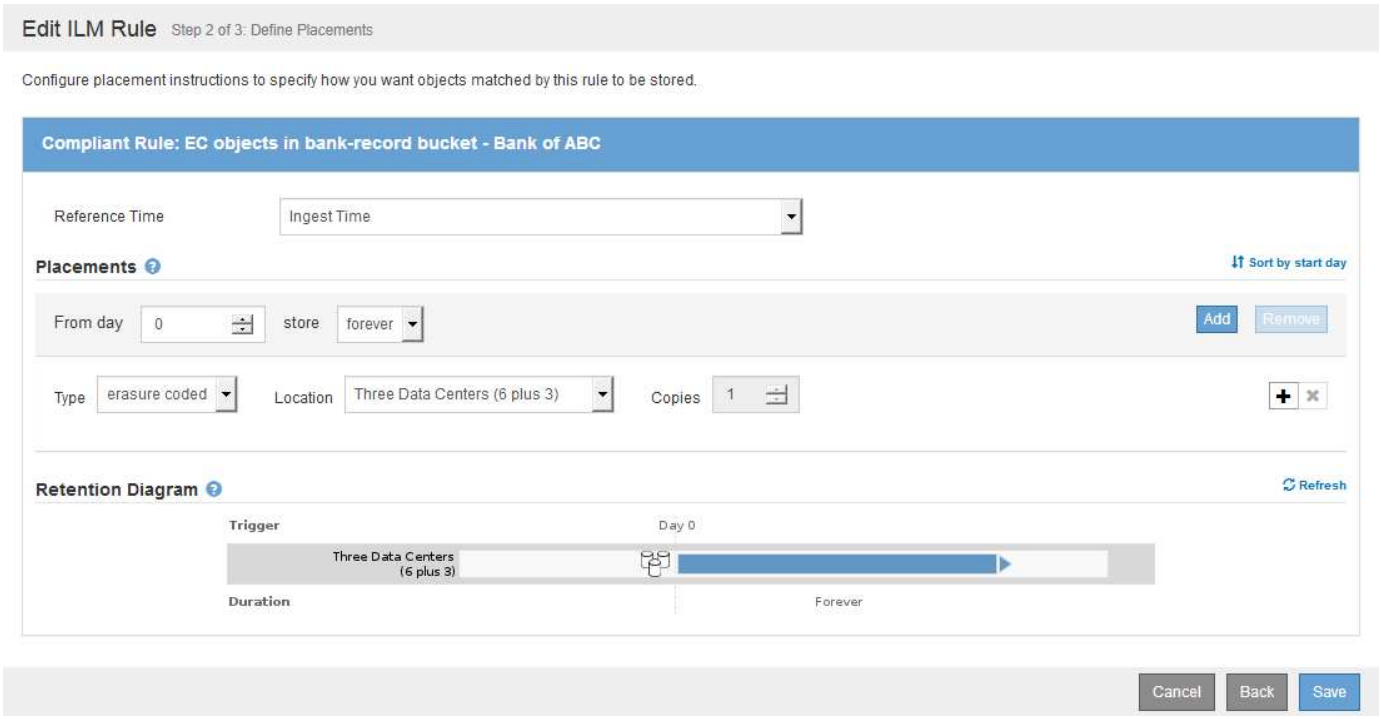
Este exemplo de regra ILM aplica-se apenas à conta de locatário S3 chamada Bank of ABC. Ele corresponde a qualquer objeto no `bank-records` bucket e, em seguida, usa a codificação de apagamento para armazenar o objeto em nós de storage em três locais de data center usando um 6 perfil de codificação de apagamento de mais de 3 anos. Essa regra atende aos requisitos dos buckets com o S3 Object Lock ativado: Uma cópia codificada por apagamento 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 - Bank of ABC
Conta de locatário	Banco do ABC

Definição de regra	Exemplo de valor
Nome do balde	`bank-records`
Filtragem avançada	Tamanho do objeto (MB) maior que 0,20 **Nota:** este filtro garante que a codificação de apagamento não seja usada para objetos de 200 KB ou menores.



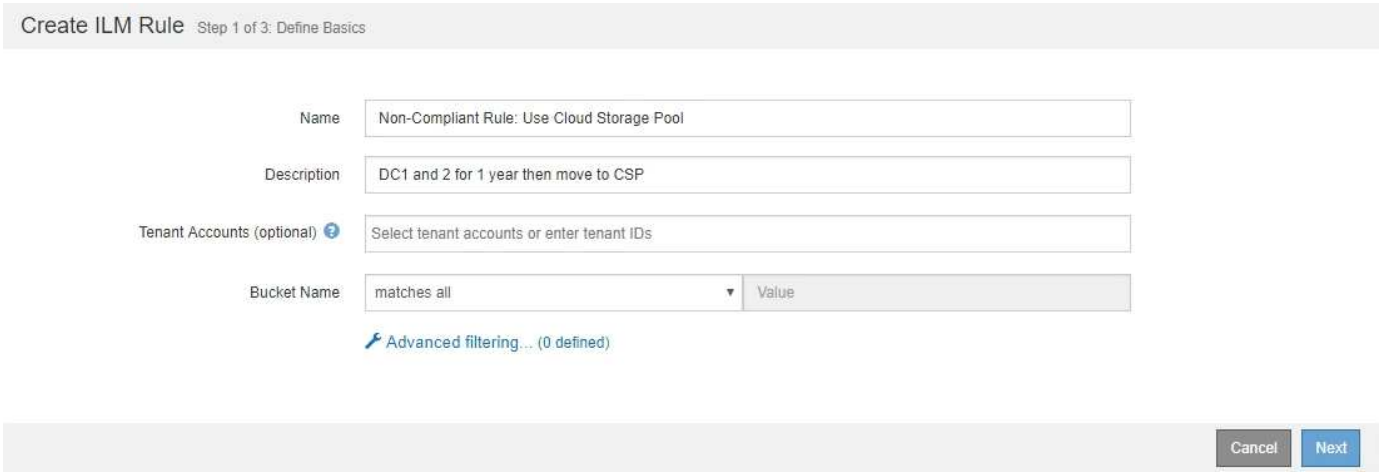
Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Colocações	Desde o dia 0 loja para sempre
Perfil de codificação de apagamento	• Crie uma cópia codificada por apagamento em nós de storage em três locais de data center • Usa o esquema de codificação de apagamento 6-3



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 balde	Não especificado, mas só se aplicará a buckets que não tenham o bloqueio de objeto S3 (ou o recurso de conformidade legado) habilitado.
Filtragem avançada	Não especificado

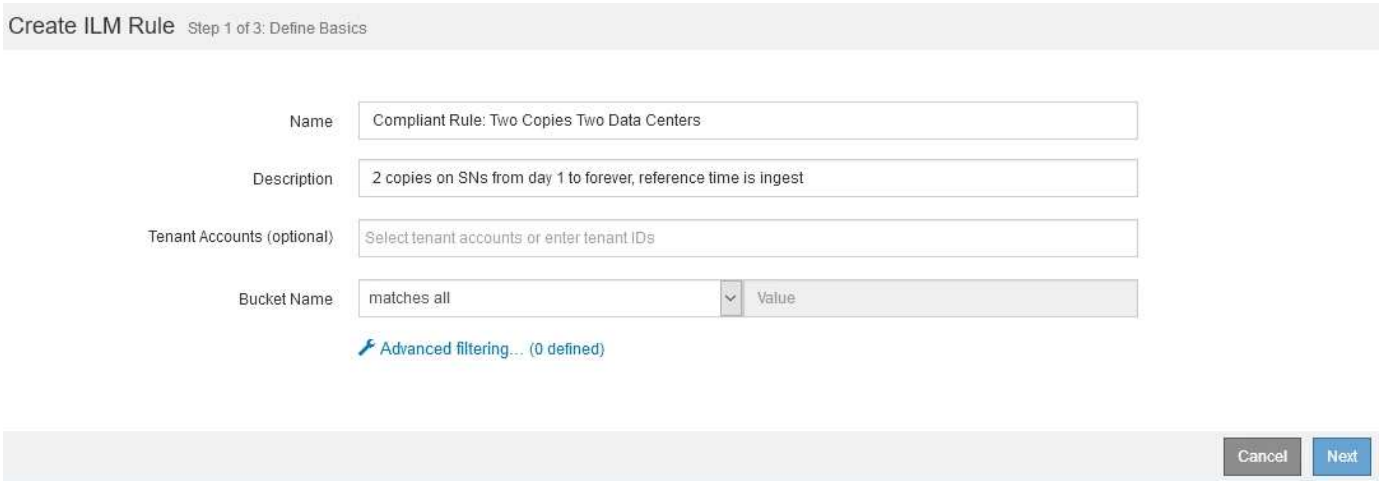


Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Colocações	• No dia 0, mantenha duas cópias replicadas nos nós de storage no data center 1 e no data center 2 por 365 dias • Após 1 ano, mantenha uma cópia replicada em um pool de storage de nuvem para sempre

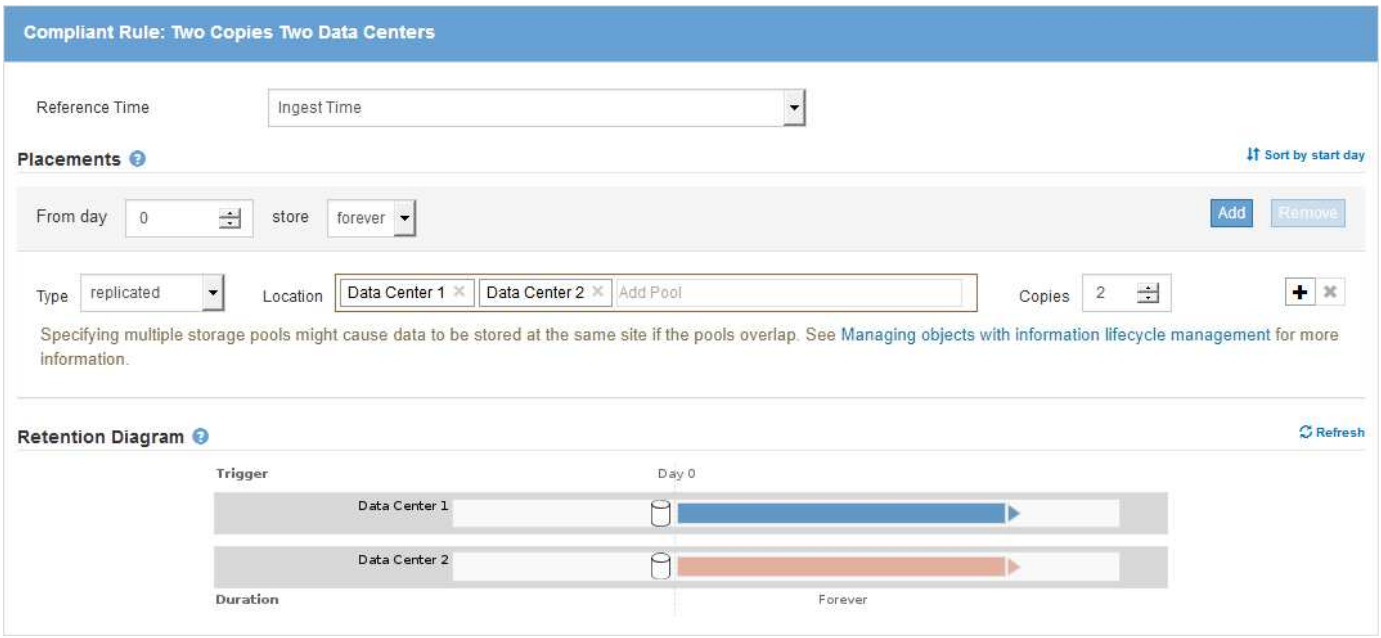
Regra ILM 3 para o exemplo de bloqueio de objetos S3: Regra padrão

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 e atende aos requisitos dos buckets com o bloqueio de objeto S3 ativado: Duas cópias de objeto são mantidas nos nós de storage 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 balde	Não especificado
Filtragem avançada	Não especificado



Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
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 proposta.

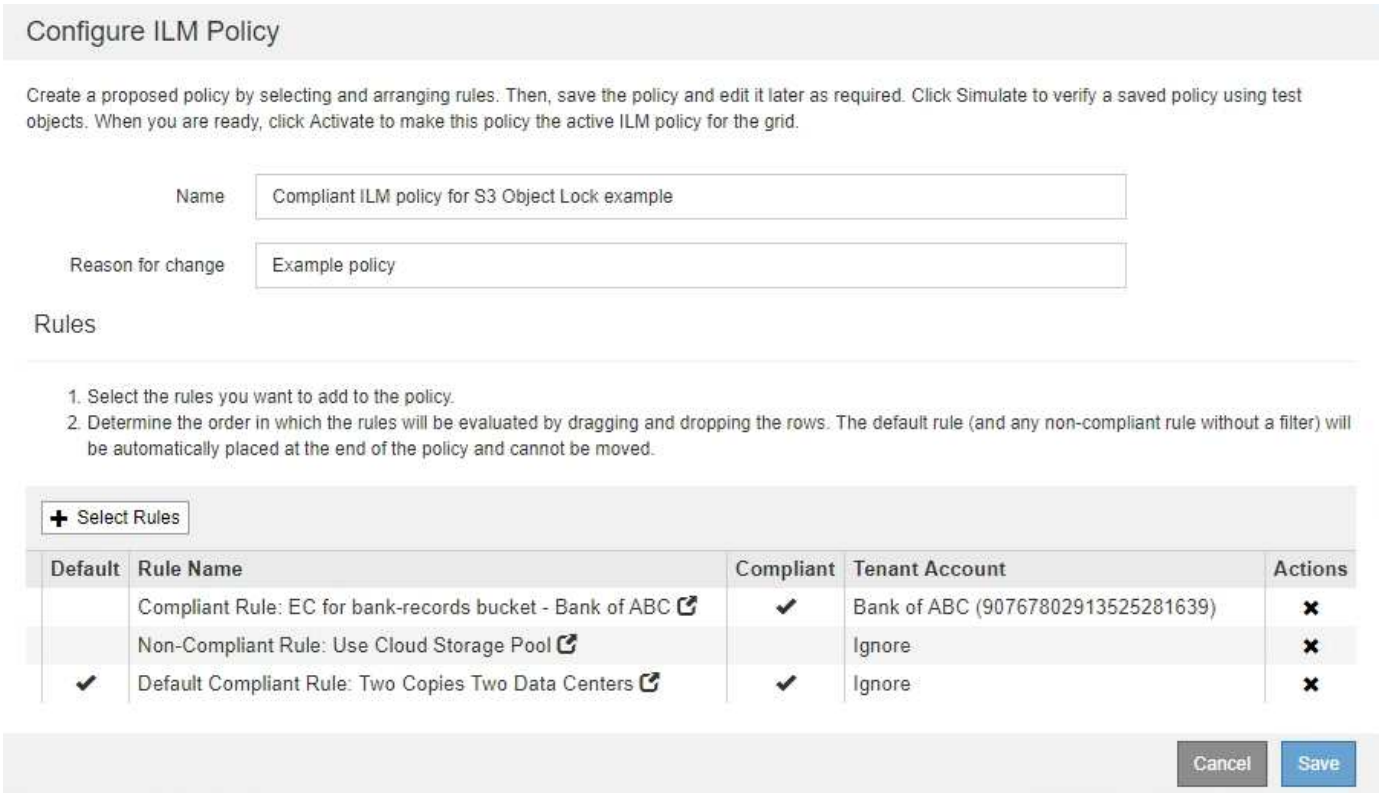
Adicionando regras à política

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 200 KB 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.



Simulando a política proposta

Depois de adicionar regras em sua política proposta, escolher uma regra compatível padrão e organizar as outras regras, você deve simular a política testando objetos do bucket com o bloqueio de objeto 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 200 KB 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 200 KB 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.

Ativar a política

Quando você estiver completamente satisfeito que a nova política protege os dados de objetos conforme esperado, você pode ativá-los.

Endurecimento do sistema

Conheça as configurações do sistema, as práticas recomendadas e as recomendações para proteger um sistema StorageGRID contra ameaças à segurança.

- "Endurecimento de um sistema StorageGRID"
- "Diretrizes de fortalecimento para atualizações de software"
- "Diretrizes de fortalecimento para redes StorageGRID"
- "Diretrizes de fortalecimento para nós de StorageGRID"
- "Diretrizes de fortalecimento para certificados de servidor"
- "Outras diretrizes de endurecimento"]

Endurecimento de um sistema StorageGRID

O fortalecimento do sistema é o processo de eliminar o maior número possível de riscos de segurança a partir de um sistema StorageGRID.

Este documento fornece uma visão geral das diretrizes de proteção específicas do StorageGRID. Estas diretrizes são um suplemento às melhores práticas padrão do setor para o endurecimento do sistema. Por exemplo, essas diretrizes assumem que você usa senhas fortes para StorageGRID, usa HTTPS em vez de HTTP e ativa autenticação baseada em certificado quando disponível.

À medida que você instala e configura o StorageGRID, você pode usar essas diretrizes para ajudá-lo a cumprir quaisquer objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informações.

O StorageGRID segue a política de manipulação de vulnerabilidades *NetApp*. Vulnerabilidades relatadas são verificadas e resolvidas de acordo com o processo de resposta a incidentes de segurança do produto.

Considerações gerais para endurecer um sistema StorageGRID

Ao endurecer um sistema StorageGRID, você deve considerar 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 contentor Docker 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.
- Quais os requisitos e convenções de segurança seguidos pela sua organização. Talvez seja necessário cumprir requisitos específicos de regulamentação ou de empresas.

Informações relacionadas

"Política de manipulação de vulnerabilidades"

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.

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, acesse a página de download do software StorageGRID. Para obter instruções passo a passo para atualizar o software StorageGRID, consulte as instruções para atualizar o StorageGRID. Para obter instruções sobre como aplicar um hotfix, consulte as instruções de recuperação e manutenção.

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.

Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

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.

Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

Upgrade 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.

Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

Informações relacionadas

"NetApp Downloads: StorageGRID"

"Atualizar o software"

"Manter recuperar"

"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.

Diretrizes para a 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 a rede de administração

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 a lista de portas internas no guia de instalação da sua plataforma.
- 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 a 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 a lista de portas internas no guia de instalação da sua plataforma.
- Aceite o tráfego de clientes de entrada apenas em endpoints explicitamente configurados. Consulte as informações sobre como gerenciar redes de clientes não confiáveis nas instruções para administrar o StorageGRID.

Informações relacionadas

"Diretrizes de rede"

"Primário de grelha"

"Administrar o StorageGRID"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Instale o VMware"

Diretrizes de fortalecimento para nós de StorageGRID

Os nós do StorageGRID podem ser implantados em máquinas virtuais VMware, dentro de um contentor Docker 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.

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.

Os nós executados nas plataformas VMware e nos dispositivos StorageGRID usam um firewall interno gerenciado automaticamente. 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, consulte o guia de instalação da sua plataforma.

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.

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 configurar o acesso de cliente aos compartilhamentos de auditoria para CIFS ou NFS, bloqueie ou desative o acesso a esses serviços.

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 as etapas para criar um proxy de administrador nas instruções de administração do StorageGRID.
- 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 administrar 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 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 as etapas para criar uma conta de locatário nas instruções de administração do StorageGRID.
- 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 as etapas para criar um proxy de armazenamento nas instruções de administração do StorageGRID.
- Opcionalmente, conete-se a serviços externos usando a rede do cliente. Em seguida, selecione **Configuração** > **Configurações de rede** > **rede cliente não confiável** e indique que a rede 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 em vez de usar o serviço CLB nos nós do Gateway. Consulte as etapas para gerenciar o balanceamento de carga nas instruções de administração do StorageGRID.

  O serviço CLB está obsoleto.

- 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 **Configuração** > **Configurações de rede** > **rede de cliente não confiável** e indique que a rede de cliente no nó de gateway 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.
- Se o controlador de armazenamento no dispositivo incluir unidades FDE ou FIPS e o recurso Segurança da unidade estiver ativado, use o SANtricity para configurar as chaves de segurança da unidade.
- Para dispositivos sem unidades FDE ou FIPS, habilite a criptografia de nós usando um KMS (Key Management Server).

Consulte as instruções de instalação e manutenção do seu dispositivo de hardware StorageGRID.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Administrar o StorageGRID"

"Use uma conta de locatário"

"Aparelhos de serviços SG100 SG1000"

"SG5600 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG6000 dispositivos de armazenamento"

Diretrizes de fortalecimento para certificados de servidor

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 do servidor 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 de locatário.
- **Object Storage API Service Endpoints Server Certificate**: Usado para proteger o acesso a nós de armazenamento e nós de Gateway, que os aplicativos clientes S3 e Swift usam para carregar e baixar dados de objetos.

> ⓘ O StorageGRID gerencia os certificados usados para pontos de extremidade do balanceador de carga separadamente. Para configurar os certificados do balanceador de carga, consulte as etapas para configurar os pontos de extremidade do balanceador de carga nas instruções de administração do StorageGRID.

Ao usar certificados de servidor personalizados, siga estas diretrizes:

- Os certificados devem ter um `subjectAltName` que corresponda às entradas de DNS para StorageGRID. Para mais informações, ver secção 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.

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.

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.

Consulte as instruções para monitoramento e solução de problemas para obter mais informações sobre logs do StorageGRID. Consulte as instruções para mensagens de auditoria 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 sistema e envie mensagens e detalhes automaticamente para o suporte técnico da NetApp, para a equipe de suporte interna da organização ou para um parceiro de suporte. Por padrão, as mensagens AutoSupport para o suporte técnico do NetApp são ativadas 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 das mensagens AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar mensagens AutoSupport para o suporte ao NetApp.

Opcionalmente, você pode configurar um proxy de administrador para obter mais controle sobre a comunicação do AutoSupport de nós de administração para o suporte técnico do NetApp. Consulte as etapas para criar um proxy de administrador nas instruções de administração do StorageGRID.

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 as etapas para configurar o Compartilhamento de recursos entre origens (CORS) nas instruções para usar contas de locatário.

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.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Rever registos de auditoria"

"Use uma conta de locatário"

"Administrar o StorageGRID"

Configurar o StorageGRID para FabricPool

Saiba como configurar o StorageGRID como um nível de nuvem do NetApp FabricPool.

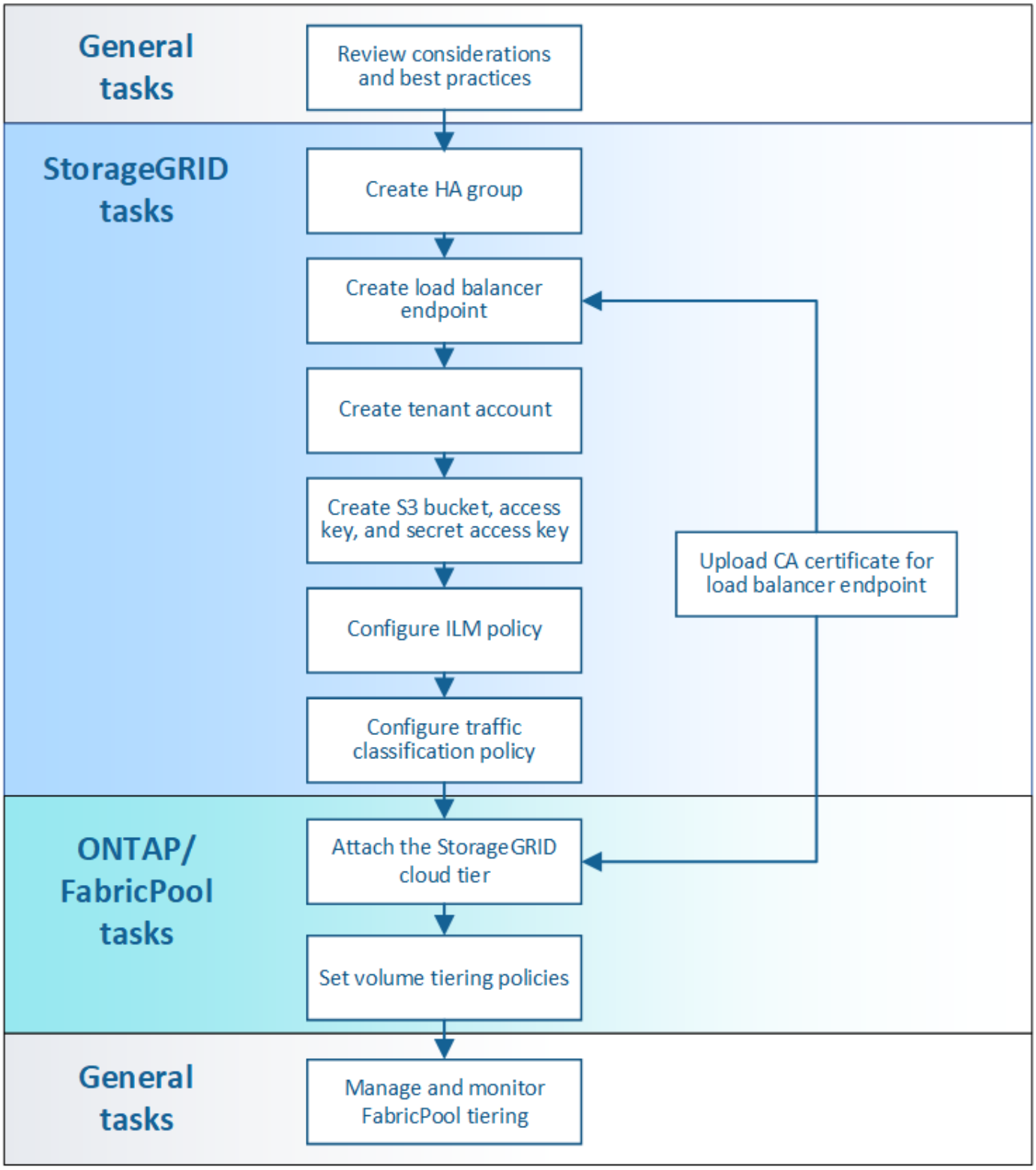
- "Configurando o StorageGRID para FabricPool"
- "Informações necessárias para anexar o StorageGRID como uma categoria de nuvem"
- "Uso do gerenciamento do ciclo de vida das informações do StorageGRID com dados do FabricPool"
- "Criando uma política de classificação de tráfego para o FabricPool"
- "Outras práticas recomendadas para StorageGRID e FabricPool"

Configurando o StorageGRID para FabricPool

Se você usar o software NetApp ONTAP, poderá usar o NetApp FabricPool para categorizar dados inativos ou inativos em um sistema de storage de objetos NetApp StorageGRID.

Use estas instruções para:

- Obtenha uma visão geral da configuração de um sistema de storage de objetos StorageGRID para uso com o FabricPool.
- Saiba como obter as informações que você fornece ao ONTAP ao anexar o StorageGRID como um nível de nuvem do FabricPool.
- Conheça as práticas recomendadas para configurar a política de gerenciamento de ciclo de vida de informações (ILM) do StorageGRID, uma política de classificação de tráfego do StorageGRID e outras opções do StorageGRID para uma carga de trabalho do FabricPool.



O que você vai precisar

Antes de usar estas instruções:

- 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 Gerenciador de Locatário.

Informações relacionadas

- "TR-4598: Melhores práticas da FabricPool para ONTAP 9.8"
- "Centro de Documentação do ONTAP 9"

O que é 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. Os dados em um FabricPool são armazenados em um nível com base se eles são acessados com frequência ou não. O uso de um FabricPool ajuda a reduzir os custos de storage sem comprometer a performance, a eficiência ou a proteção.

Nenhuma alteração de arquitetura é necessária. Você ainda pode continuar gerenciando o ambiente do aplicativo e banco de dados a partir do sistema de storage central da ONTAP.

O que é storage de objetos

Storage de objetos 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.

Usando o StorageGRID como uma categoria de nuvem do FabricPool

O FabricPool pode categorizar dados do ONTAP em vários fornecedores de armazenamento 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.

Usando vários clusters ONTAP com o StorageGRID

Estas instruções descrevem como conetar o StorageGRID a um único cluster ONTAP. No entanto, talvez você queira conectar o mesmo sistema StorageGRID a vários clusters do ONTAP.

O único requisito para separar os dados de vários clusters do ONTAP em um único sistema StorageGRID é que você precisa usar um bucket do S3 diferente em cada cluster. Com base nos seus requisitos, você pode usar o mesmo grupo de alta disponibilidade (HA), ponto de extremidade do balanceador de carga e conta de locatário para todos os clusters ou configurar cada um desses itens para cada cluster.

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 algumas etapas de configuração no StorageGRID e obter certos valores.

Sobre esta tarefa

A tabela a seguir lista as informações que você deve fornecer ao ONTAP ao anexar o StorageGRID como uma categoria de nuvem para o FabricPool. Os tópicos nesta seção explicam como usar o Gerenciador de Grade e o Gerenciador de Locatário do StorageGRID para obter as informações de que você precisa.

> Os nomes de campo exatos listados e o processo que você usa para inserir os valores necessários no ONTAP dependem se você está usando a CLI do ONTAP (storage agregado object-store config create) ou o Gerenciador de sistema do ONTAP (**armazenamento** > **agregados e discos** > **nível de nuvem**).

Para obter mais informações, consulte o seguinte:

- "TR-4598: Melhores práticas da FabricPool para ONTAP 9.8"
- "Centro de Documentação do ONTAP 9"

Campo ONTAP	Descrição
Nome do armazenamento de objetos	Qualquer nome único e descritivo. Por exemplo, `StorageGRID_Cloud_Tier`.
Tipo de fornecedor	StorageGRID (Gerenciador do sistema) ou `SGWS` (CLI).
Porta	A porta que o FabricPool usará quando se conetar ao StorageGRID. Você determina qual número de porta usar ao definir o ponto de extremidade do balanceador de carga do StorageGRID. "Criando um ponto de extremidade do balanceador de carga para FabricPool"
Nome do servidor	O nome de domínio totalmente qualificado (FQDN) para o ponto de extremidade do balanceador de carga StorageGRID. Por exemplo, `s3.storagegrid.company.com`. Observe o seguinte: • O nome de domínio que você especificar aqui deve corresponder ao nome de domínio no certificado de CA que você carrega para o endpoint do balanceador de carga do StorageGRID. • O Registro DNS para este nome de domínio deve ser mapeado para cada endereço IP que você usará para se conetar ao StorageGRID. "Configurando o servidor DNS para endereços IP StorageGRID"

Campo ONTAP	Descrição
Nome do contentor	O nome do bucket do StorageGRID que você usará com este cluster do ONTAP. Por exemplo, `fabricpool-bucket`. Você cria esse bucket no Gerenciador do Locatário. Observe o seguinte: • O nome do bucket não pode ser alterado quando a configuração for criada. • O bucket não pode ter o controle de versão ativado. • Você precisa usar um bucket diferente para cada cluster do ONTAP que categorize os dados no StorageGRID. "Criando um bucket do S3 e obtendo uma chave de acesso"
Chave de acesso e senha secreta	A chave de acesso e a chave de acesso secreta para a conta de locatário do StorageGRID. Você gera esses valores no Gerenciador do Locatário. "Criando um bucket do S3 e obtendo uma chave de acesso"
SSL	Tem de estar ativado.
Certificado de armazenamento de objetos	O certificado da CA que você carregou quando criou o ponto de extremidade do balanceador de carga do StorageGRID. **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. "Criando um ponto de extremidade do balanceador de carga para FabricPool"

Depois de terminar

Depois de obter as informações StorageGRID necessárias, acesse o ONTAP para adicionar StorageGRID como uma categoria de nuvem, adicionar a categoria de nuvem como agregado e definir políticas de disposição em categorias de volumes.

Práticas recomendadas para balanceamento de carga

Antes de anexar o StorageGRID como uma camada de nuvem do FabricPool, use o Gerenciador de Grade do StorageGRID para configurar pelo menos um ponto de extremidade do balanceador de carga.

O que é balanceamento de carga

Quando os dados são categorizados de FabricPool para um sistema StorageGRID, o StorageGRID usa um balanceador de carga para gerenciar o workload de ingestão e recuperação. O balanceamento de carga

maximiza a velocidade e a capacidade de conexão distribuindo o workload do FabricPool 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, entre em Contato com o representante da sua conta NetApp ou consulte o seguinte relatório técnico:

"Opções de balanceador de carga do StorageGRID"

> O serviço CLB (Connection Load Balancer) separado nos nós de gateway está obsoleto e não é mais recomendado para uso com o FabricPool.

Práticas recomendadas para balanceamento de carga StorageGRID

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 um nó de administrador e um nó de gateway ou até dois nós de administrador. Verifique se há infraestrutura adequada de rede, hardware ou virtualização para cada nó de balanceamento de carga, esteja você usando dispositivos de serviços SG100 ou SG1000, nós bare metal ou nós baseados em máquina virtual (VM).

Você deve configurar um ponto de extremidade do balanceador de carga do StorageGRID para definir a porta que os nós de gateway e os nós de administrador usarão para solicitações de FabricPool de entrada e saída.

Práticas recomendadas para o certificado de endpoint do balanceador de carga

Ao criar um ponto de extremidade do balanceador de carga para uso com o FabricPool, você deve usar o HTTPS como protocolo. Em seguida, você pode carregar um certificado assinado por uma autoridade de certificação (CA) publicamente confiável ou privada, ou gerar um certificado autoassinado. O certificado permite que o ONTAP se autentique com o StorageGRID.

Como prática recomendada, você deve usar um certificado de servidor CA para proteger a conexão. Os certificados assinados por uma CA podem ser girados sem interrupções.

Ao solicitar um certificado de CA para uso com o endpoint do balanceador de carga, verifique se o nome de domínio no certificado corresponde ao nome de servidor inserido no ONTAP para esse endpoint do balanceador de carga. Se possível, use um caractere curinga (*) para permitir URLs de estilo host virtual. Por exemplo:

```
*.s3.storagegrid.company.com
```

Ao adicionar o StorageGRID como um nível de nuvem do FabricPool, você deve instalar o mesmo certificado no cluster do ONTAP, bem como os certificados raiz e de autoridade de certificação (CA) subordinada.

O StorageGRID usa certificados de servidor para vários fins. Se você estiver se conetando ao serviço Load Balancer, não será necessário fazer o upload do certificado do servidor de Endpoints do Object Storage API Service.

Para saber mais sobre o certificado do servidor para um endpoint de balanceamento de carga:

- "Gerenciamento do balanceamento de carga"
- "Diretrizes de fortalecimento para certificados de servidor"

Práticas recomendadas para grupos de alta disponibilidade

Antes de anexar o StorageGRID como uma camada de nuvem do FabricPool, use o Gerenciador de Grade do StorageGRID para configurar um grupo de alta disponibilidade (HA).

O que é um grupo de alta disponibilidade (HA)

Para garantir que o serviço de balanceamento de carga esteja sempre disponível para gerenciar dados do FabricPool, você pode agrupar as interfaces de rede de vários nós de administrador e gateway em uma única entidade, conhecida como um grupo de alta disponibilidade (HA). Se o nó ativo no grupo de HA falhar, outro nó no grupo poderá continuar a gerenciar a carga de trabalho.

Cada grupo de HA fornece acesso altamente disponível aos serviços compartilhados nos nós associados. Por exemplo, um grupo de HA composto por todos os nós de administração fornece acesso altamente disponível a alguns serviços de gerenciamento do nó de administração e ao serviço do Load Balancer. Um grupo de HA que consiste apenas em nós de Gateway ou de nós de administração e de Gateway fornece acesso altamente disponível ao serviço de balanceador de carga compartilhado.

Ao criar um grupo HA, você seleciona interfaces de rede pertencentes à rede Grid (eth0) ou à rede Client (eth2). Todas as interfaces de um grupo HA devem estar dentro da mesma sub-rede de rede.

Um grupo de HA mantém um ou mais endereços IP virtuais que são adicionados à interface ativa no grupo. Se a interface ativa ficar indisponível, os endereços IP virtuais serão movidos para outra interface. Esse 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.

Se você configurar um grupo de HA de nós de balanceamento de carga, o FabricPool se conetará aos endereços IP virtuais desse grupo de HA.

Práticas recomendadas para grupos de alta disponibilidade (HA)

As práticas recomendadas para a criação de um grupo de HA do StorageGRID para FabricPool dependem do workload, como a seguir:

- 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 .

Configurando o servidor DNS para endereços IP StorageGRID

Depois de configurar grupos de alta disponibilidade e pontos de extremidade do balanceador de carga, você deve garantir que o sistema de nomes de domínio (DNS) do sistema ONTAP inclua um Registro para associar o nome do servidor StorageGRID (nome de domínio totalmente qualificado) ao endereço IP que o FabricPool usará 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 de HA, o FabricPool se conetará aos endereços IP virtuais desse grupo de HA.
- Se você não estiver usando um grupo de HA, o FabricPool poderá se conetar ao serviço do balanceador de carga do StorageGRID usando o endereço IP de qualquer 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.

Criação de 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 consiste em uma ou mais interfaces de rede em nós de administração, nós de gateway ou ambos.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

Cada grupo de HA usa endereços IP virtuais (VIPs) para fornecer acesso altamente disponível aos serviços compartilhados nos nós associados.

Para obter detalhes sobre esta tarefa. "Gerenciamento de grupos de alta disponibilidade"Consulte .

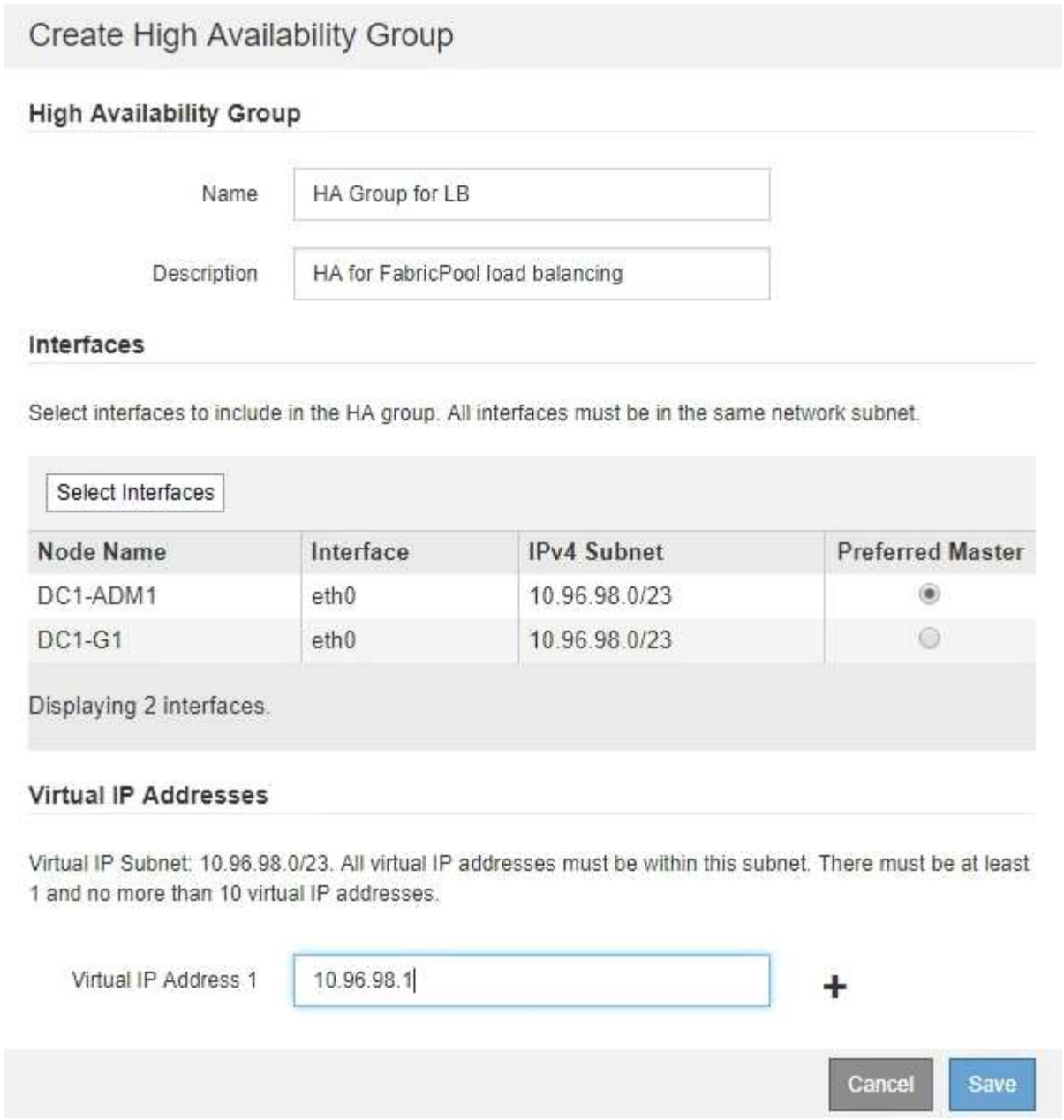
Passos

1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.
2. Selecione uma ou mais interfaces de rede. As interfaces de rede devem pertencer à mesma sub-rede na rede de Grade (eth0) ou na rede de Cliente (eth2).
3. Atribua um nó para ser o mestre preferido.

   O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup.

4. Introduza até dez endereços IPv4 para o grupo HA.

   Os endereços devem estar dentro da sub-rede IPv4 compartilhada por todas as interfaces membros.



Criando um ponto de extremidade do balanceador de carga para FabricPool

Ao configurar o StorageGRID para uso com o FabricPool, você configura um ponto de extremidade do balanceador de carga e carrega o certificado de ponto de extremidade do balanceador de carga, que é usado para proteger a conexão entre o ONTAP e o StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.
- Você tem os seguintes arquivos:
  - Certificado do servidor: O arquivo de certificado do servidor personalizado.
  - Chave privada do certificado do servidor: O arquivo de chave privada do certificado do servidor

personalizado.

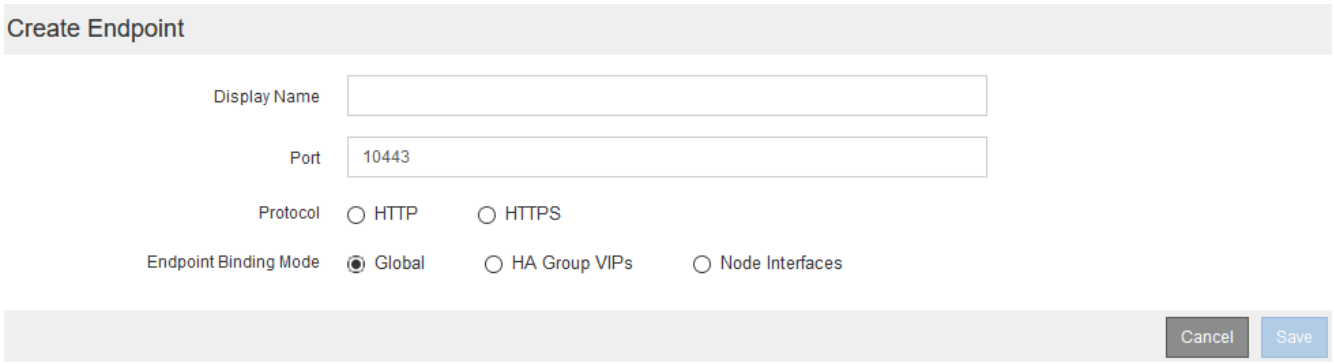
- Pacote CA: Um único arquivo contendo os certificados de cada autoridade de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

Sobre esta tarefa

Para obter detalhes sobre esta tarefa, "Configuração dos pontos de extremidade do balanceador de carga"consulte .

Passos

1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.



2. Selecione **Adicionar endpoint**.
3. Introduza as seguintes informações.

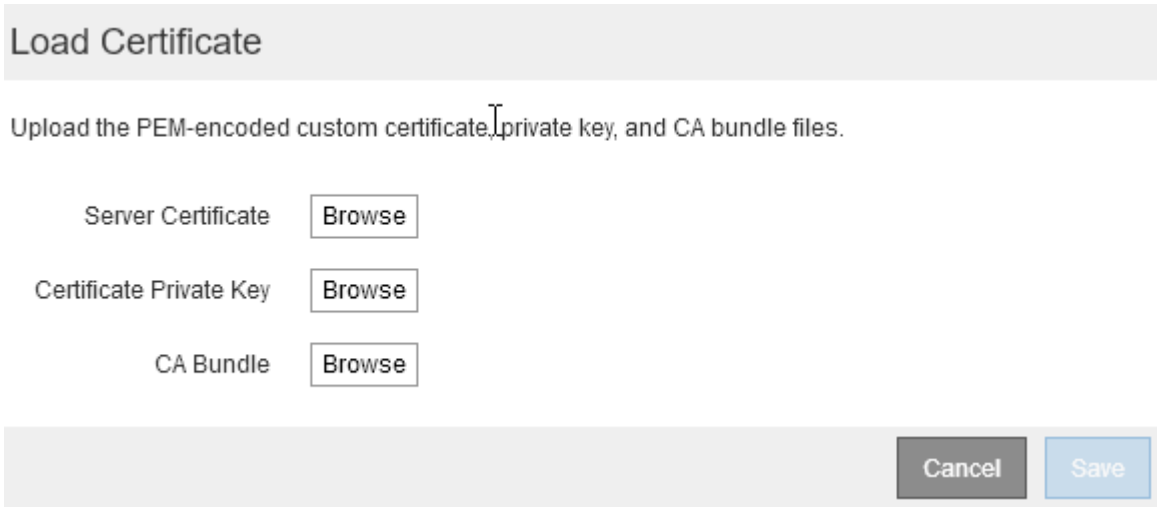
Campo	Descrição
Nome do visor	Um nome descritivo para o endpoint
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Esse campo é padrão para 10433, mas você pode inserir qualquer porta externa não utilizada. Se você inserir 80 ou 443, o endpoint será configurado apenas em nós de Gateway, uma vez que essas portas são reservadas em nós de administração. **Observação:** as portas usadas por outros serviços de grade não são permitidas. Consulte a lista de portas usadas para comunicações internas e externas: "Referência da porta de rede" Forneça esse mesmo número de porta ao ONTAP ao anexar o StorageGRID como uma categoria de nuvem do FabricPool.
Protocolo	Deve ser **HTTPS**.

Campo	Descrição
Modo de encadernação de endpoint	Use a configuração **Global** (recomendado) ou restrinja a acessibilidade deste ponto final a um dos seguintes: • Endereços IP virtuais (VIPs) específicos de alta disponibilidade (HA). Use essa seleção somente se você precisar de níveis muito mais altos de isolamento de workloads. • Interfaces de rede específicas de nós específicos.

4. Selecione **Guardar**.

   A caixa de diálogo Editar ponto final é exibida.

5. Para **Endpoint Service Type**, selecione **S3**.
6. Selecione **carregar certificado** (recomendado) e navegue até o certificado do servidor, a chave privada do certificado e o pacote CA.



7. Selecione **Guardar**.

Criando uma conta de locatário para o FabricPool

Você deve criar uma conta de locatário no Gerenciador de Grade para uso do FabricPool.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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.

Você pode usar a mesma conta de locatário para vários clusters do ONTAP. Ou você pode criar uma conta de locatário dedicada para cada cluster do ONTAP, conforme necessário.

> Essas instruções assumem que você configurou logon único (SSO) para o Gerenciador de Grade. Se você não estiver usando SSO, use as instruções para "Criando uma conta de locatário se o StorageGRID não estiver usando SSO".

Passos

1. Selecione **tenants**.
2. Selecione **criar**.
3. Insira um nome de exibição para a conta de locatário do FabricPool.
4. Selecione **S3**.
5. Deixe a caixa de seleção **permitir Serviços de Plataforma** selecionada para habilitar o uso de serviços de plataforma.

   Se os serviços de plataforma estiverem ativados, um locatário poderá usar recursos, como a replicação do CloudMirror, que acessam serviços externos.
6. Deixe o campo **cota de armazenamento** em branco.
7. No campo **Root Access Group**, selecione um grupo federado existente no Gerenciador de Grade para ter a permissão de acesso raiz inicial para o locatário.
8. Selecione **Guardar**.

Criando um bucket do S3 e obtendo uma chave 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.

O que você vai precisar

- Você deve ter criado uma conta de locatário para uso do FabricPool.

Sobre esta tarefa

Estas instruções descrevem como usar o Gerenciador de Locatário do StorageGRID para criar um bucket e obter chaves de acesso. Você também pode executar essas tarefas usando a API de gerenciamento do locatário ou a API REST do StorageGRID S3.

Para saber mais:

- "Use uma conta de locatário"
- "Use S3"

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 **STORAGE (S3)** > **Buckets**.

   b. Selecione **criar bucket**.

   c. Introduza o nome do bucket do StorageGRID que irá utilizar com o FabricPool. Por exemplo, `fabricpool-bucket`.

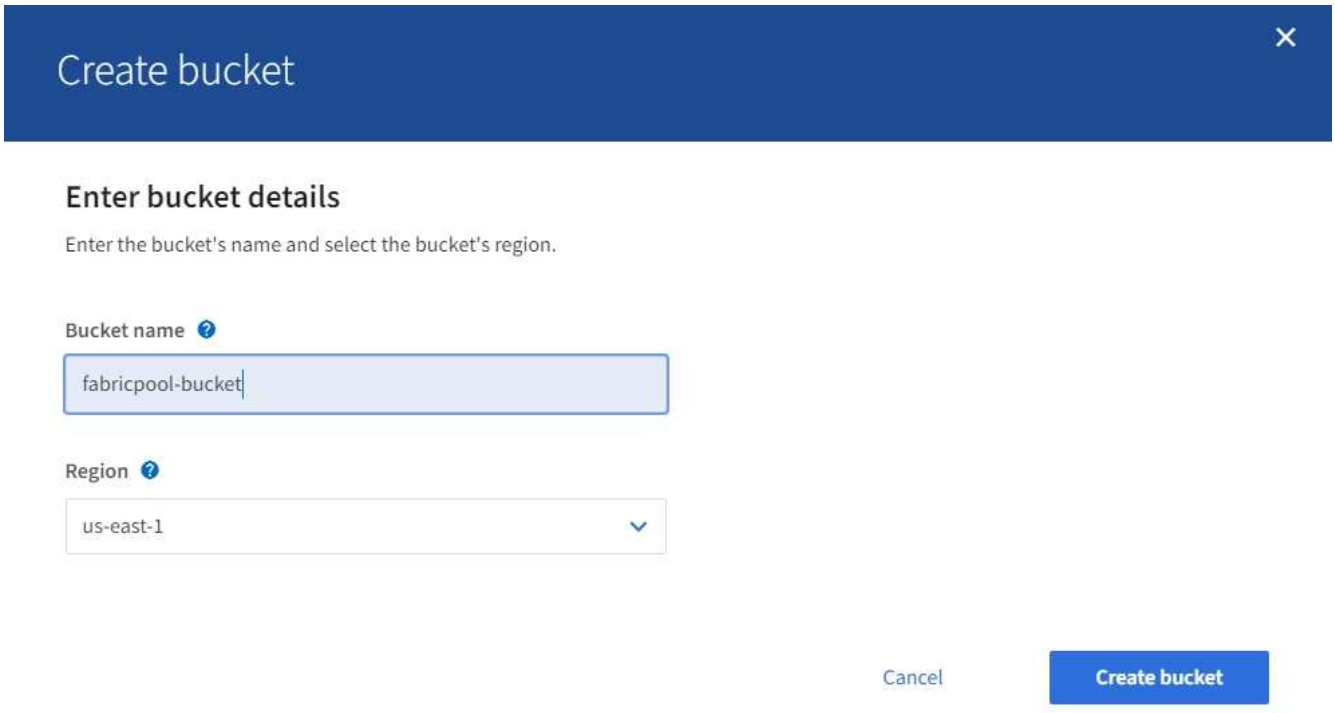
      > Não é possível alterar o nome do bucket depois de criar o bucket.

      Os nomes dos buckets devem cumprir 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.
      - 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.

   d. Selecione a região para este intervalo.

      Por padrão, todos os buckets são criados na `us-east-1` região.



a. Selecione **criar 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 criar uma nova chave de acesso e chave de acesso secreta no futuro, lembre-se de atualizar os valores correspondentes no ONTAP imediatamente para garantir que o ONTAP possa armazenar e recuperar dados no StorageGRID sem interrupção.

Uso do gerenciamento do ciclo de vida das informações do StorageGRID com dados do FabricPool

Se você estiver usando o FabricPool para categorizar dados no StorageGRID, entenda os requisitos para criar regras de gerenciamento do ciclo de vida das informações (ILM) do StorageGRID e uma política de ILM para gerenciar dados do FabricPool. Você deve garantir que as regras de ILM que se aplicam aos dados do FabricPool não sejam disruptivas.

> 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 saber mais: "Gerenciar objetos com ILM"

Diretrizes de ILM para dados FabricPool

Revise essas diretrizes para garantir que suas regras de ILM e sua política de ILM sejam adequadas para dados do FabricPool e seus requisitos de negócios. Se você já estiver usando o StorageGRID ILM, talvez seja necessário atualizar sua política ILM ativa 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 significativamente menos capacidade de storage, do que a replicação. Os esquemas 4-1 e 6-1 usam menos capacidade do que 2-1, mas ao custo de menor taxa de transferência e menos flexibilidade quando você adiciona nós de storage durante a expansão da grade.

- 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.

- Não use uma regra de ILM que expirará ou excluirá dados de nível 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. Você não pode usar regras de ILM para arquivar dados do FabricPool em fita usando um nó de arquivamento ou usar um pool de armazenamento em nuvem para mover dados do FabricPool para o Glacier.

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.

Exemplo de política de ILM para dados do FabricPool

Use esta 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 política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Para saber mais: "Gerenciar objetos com ILM"

Passos

1. Crie um pool de armazenamento chamado **DEN**. Selecione o site de Denver.
2. Crie um perfil de codificação de apagamento chamado **2 plus 1**. Selecione o esquema de codificação de apagamento 2-1 e o pool de armazenamento **DEN**.
3. 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

Definição de regra	Exemplo de valor
Nome do balde	`fabricpool-bucket` Você também pode filtrar na conta de locatário do FabricPool.
Filtragem avançada	Tamanho do objeto (MB) 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
Colocação	Desde o dia 0 loja para sempre
Tipo	Codificar para apagamento
Localização	DEN (2 mais 1)
Comportamento de ingestão	Equilibrado

4. Crie uma regra ILM 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
Nome do balde	*none*
Filtragem avançada	*none*
Tempo de referência	Tempo de ingestão
Colocação	Desde o dia 0 loja para sempre
Tipo	Replicado
Localização	DEN
Cópias	2
Comportamento de ingestão	Equilibrado

5. Crie uma política de ILM proposta e selecione as duas regras. Como a regra de replicação não usa filtros, ela pode ser a regra padrão (última) para a política.
6. Ingira objetos de teste na grade.
7. Simule a política com os objetos de teste para verificar o comportamento.
8. 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 codificadas por apagamento e replicadas serão mantidas no StorageGRID até que sejam excluídas pelo cliente S3. StorageGRID ILM nunca excluirá esses itens.

Criando 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

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.

- Como regra geral, você não deve impor limites de qualidade de serviço a qualquer workload do FabricPool; apenas limitar os outros workloads.
- Os limites colocados em outras cargas de trabalho podem precisar ser amplos para considerar o comportamento desconhecido 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.

Para saber mais: "Gerir políticas de classificação de tráfego"

Passos

1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.
2. Introduza um nome e uma descrição.
3. Na seção regras correspondentes, crie pelo menos uma regra.
   a. Selecione **criar**.
   b. Selecione **ponto final** e selecione o ponto final do balanceador de carga que você criou para o FabricPool.

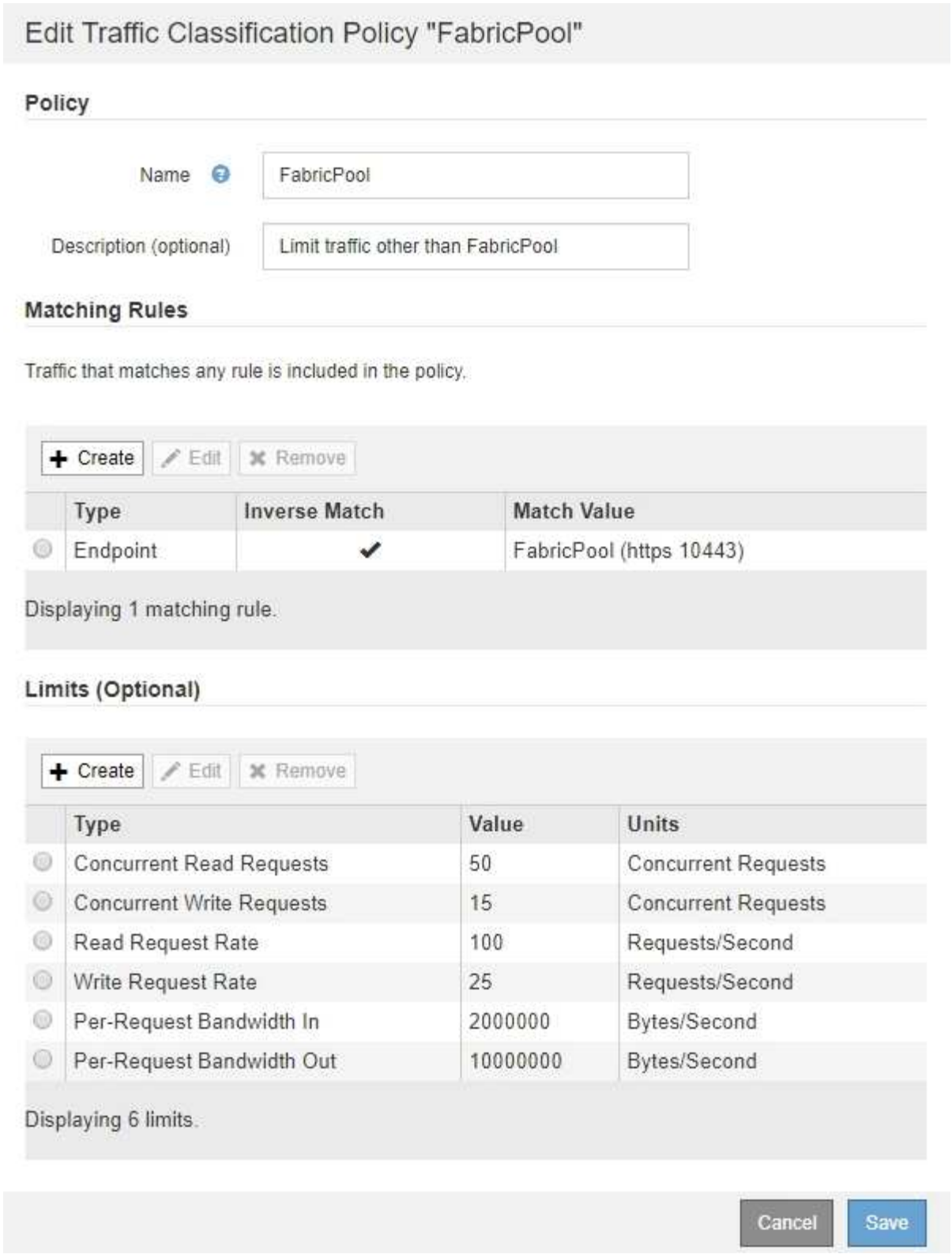
      Você também pode selecionar a conta de locatário ou o intervalo do FabricPool.

   c. Se você quiser que essa política de tráfego limite o tráfego para os outros endpoints, selecione **correspondência inversa**.
4. Opcionalmente, crie um ou mais limites.

   Mesmo que nenhum limite seja definido para uma política de classificação de tráfego, as métricas são coletadas para que você possa entender as tendências de tráfego.

   a. Selecione **criar**.
   b. Selecione o tipo de tráfego que pretende limitar e o limite a aplicar.

      Este exemplo de classificação de tráfego FabricPool lista os tipos de tráfego de rede que você pode limitar e os tipos de valores que você pode selecionar. Os tipos de tráfego e valores de uma política real seriam baseados em seus requisitos específicos.



5. Depois de criar a política de classificação de tráfego, selecione a política e, em seguida, selecione **Metrics** para determinar se a política está limitando o tráfego conforme esperado.

Outras práticas recomendadas para StorageGRID e FabricPool

Ao configurar um sistema StorageGRID para uso com o FabricPool, você deve evitar definir opções globais que possam afetar a forma como seus dados são salvos.

Criptografia de objetos

Ao configurar o StorageGRID, você pode opcionalmente ativar a configuração global **criptografia de objeto armazenado** se a criptografia de dados for necessária para outros clientes StorageGRID (**Configuração** > **Configurações do sistema** > **Opções de grade**). 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 a configuração global **Compress Stored Objects** (**Configuration** > **System Settings** > **Grid Options**). Os dados dispostos em camadas de FabricPool para StorageGRID já estão compatados. Ativar **Compress Stored Objects** não reduzirá ainda mais o tamanho de um objeto.

Nível de consistência

Para buckets do FabricPool, o nível de consistência de bucket recomendado é **leitura após nova gravação**, que é a configuração padrão para um novo bucket. Não edite buckets do FabricPool para usar **Available** ou qualquer outro nível de consistência.

Disposição em camadas do FabricPool

Se o nó StorageGRID usar o storage atribuído a partir de um sistema NetApp AFF, 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.

Use o StorageGRID

Use uma conta de locatário

Saiba como usar uma conta de locatário do StorageGRID.

- "Usando o Gerenciador do Locatário"
- "Gerenciamento do acesso do sistema para usuários de locatários"
- "Gerenciamento de contas de locatários do S3"
- "Gerenciamento de serviços da plataforma S3"

Usando o Gerenciador do Locatário

O Gerenciador do Locatário permite gerenciar todos os aspetos de uma conta de locatário do StorageGRID.

Você pode usar o Gerenciador do locatário para monitorar o uso do armazenamento de uma conta de locatário e gerenciar usuários com federação de identidade ou criando grupos e usuários locais. Para contas de locatários do S3, você também pode gerenciar chaves do S3, gerenciar buckets do S3 e configurar serviços de plataforma.

Usando uma conta de locatário do StorageGRID

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.

Cada conta de locatário tem seus próprios grupos federados ou locais, usuários, buckets do S3 ou contentores Swift e objetos.

Opcionalmente, 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 para a implementação de aplicativos cliente S3.

- * 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.

Criando contas de inquilino

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 as seguintes informações:

- Nome de exibição para o locatário (o ID da conta do locatário é atribuído automaticamente e não pode ser alterado).
- Se a conta de locatário usará o S3 ou Swift.
- Para contas de inquilino S3: Se a conta de inquilino tem permissão para usar serviços de plataforma. Se o uso de serviços de plataforma for permitido, a grade deve ser configurada para suportar seu uso.
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).
- Se a federação de identidade estiver ativada para o sistema StorageGRID, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.
- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.

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.

Configurando S3 locatários

Depois que uma conta de locatário do S3 for criada, você poderá acessar o Gerenciador do Locatário para executar tarefas como as seguintes:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) ou criando grupos e usuários locais
- Gerenciando chaves de acesso S3
- Criação e gerenciamento de buckets do S3, incluindo buckets em conformidade
- Usando serviços de plataforma (se ativado)
- Monitoramento do uso do storage

> Embora você possa criar e gerenciar buckets do S3 com o Gerenciador do locatário, você precisa ter S3 chaves de acesso e usar a API REST do S3 para ingerir e gerenciar objetos.

Configurando os locatários Swift

Depois que uma conta de locatário Swift for criada, os usuários com a permissão de acesso root podem acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e criando grupos e usuários locais
- Monitoramento do uso do storage

> Os usuários Swift devem ter a permissão de acesso root para acessar o Gerenciador do locatário. No entanto, a permissão de acesso root não permite que os usuários se autentiquem na API REST do Swift para criar contentores e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

Informações relacionadas

"Administrar o StorageGRID"

"Use S3"

"Use Swift"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Iniciar sessão no Gestor do Locatário

Você acessa o Gerenciador do Locatário inserindo o URL do locatário na barra de endereços de um navegador da Web compatível.

O que você vai precisar

- Tem de ter as suas credenciais de início de sessão.
- Você deve ter 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 contém o nome de domínio totalmente qualificado (FQDN) ou o endereço IP usado para acessar um nó de administração e, opcionalmente, também pode incluir um número de porta, o ID da conta de locatário de 20 dígitos ou ambos.

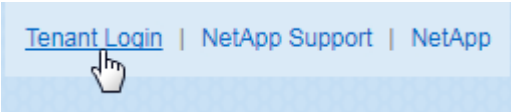
- Se o URL não incluir o ID de conta de 20 dígitos do locatário, você deve ter esse ID de conta.
- Você deve estar usando um navegador da Web compatível.
- Os cookies devem estar ativados no seu navegador.
- Você deve ter permissões de acesso específicas.

Passos

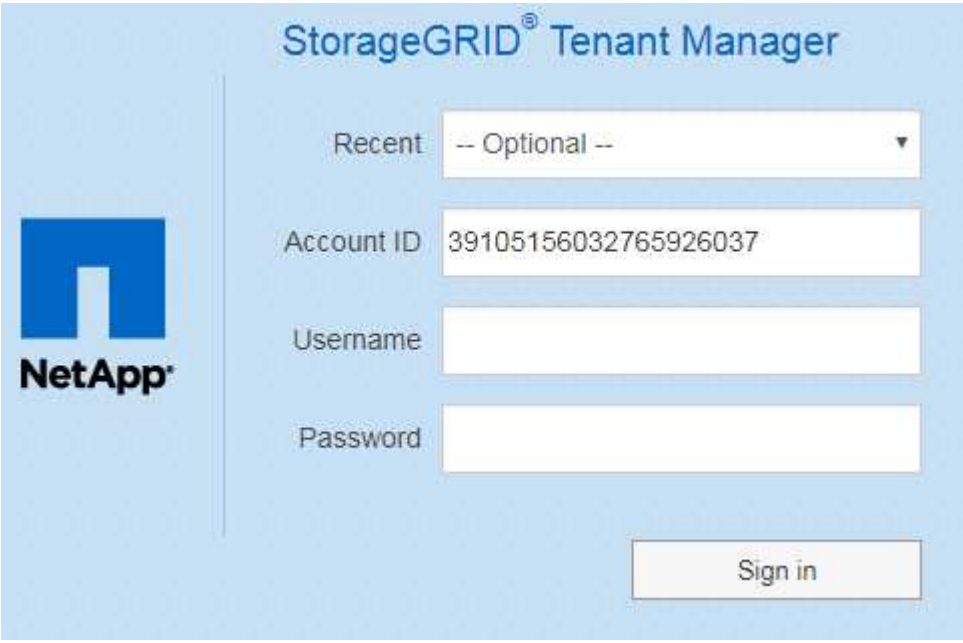
1. Inicie um navegador da Web compatível.
2. Na barra de endereços do navegador, insira o URL para acessar o Gerenciador de locatários.
3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Inicie sessão no Gestor do Locatário.

   A tela de login que você vê depende do URL digitado e se sua organização está usando o logon único (SSO). Você verá uma das seguintes telas:

   - A página de login do Gerenciador de Grade. Clique no link **Login do locatário** no canto superior direito.

   - A página de início de sessão do Tenant Manager. O campo **ID da conta** pode já estar concluído, como mostrado abaixo.

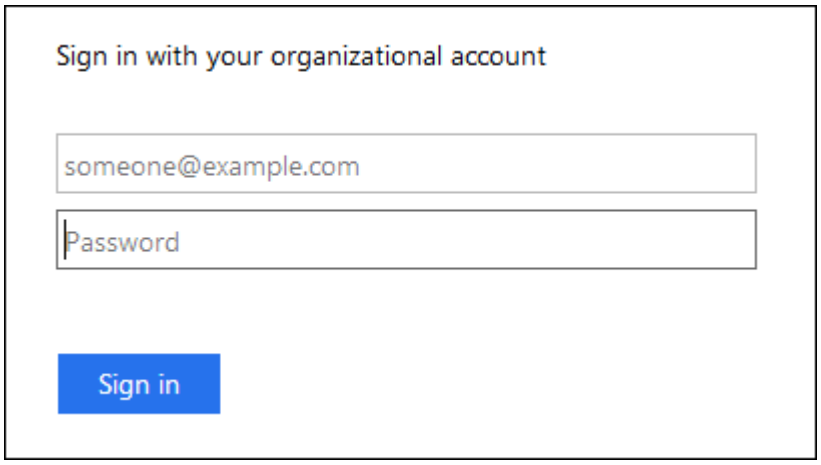
     i. Se o ID da conta de 20 dígitos do locatário não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.

ii. Introduza o seu nome de utilizador e palavra-passe.

iii. Clique em **entrar**.

É apresentado o Painel do Gestor do Locatário.

- A página SSO da sua organização, se o SSO estiver ativado na grade. Por exemplo:



Insira suas credenciais SSO padrão e clique em **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. Clique em **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 Gestor do Locatário.

5. Se você recebeu uma senha inicial de outra pessoa, altere sua senha para proteger sua conta. Selecione ***username*** **alterar senha**.

> Se o SSO estiver ativado para o sistema StorageGRID, você não poderá alterar sua senha do Gerenciador do Locatário.

Informações relacionadas

"Administrar o StorageGRID"

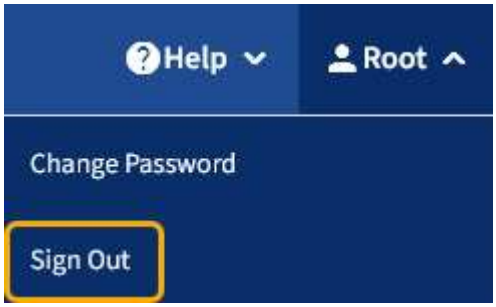
"Requisitos do navegador da Web"

Sair do gerente do locatário

Quando terminar de trabalhar com o Gestor do Locatário, tem de terminar sessão para garantir que os utilizadores não autorizados não conseguem 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**.

Opção	Descrição
SSO não em uso	Você está desconetado do Admin Node. É apresentada a página de início de sessão do Gestor do Locatário. **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. 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. **Observação:** se o SSO estiver ativado e você também estiver conetado ao Gerenciador de Grade, você também deve sair do Gerenciador de Grade para sair do SSO.

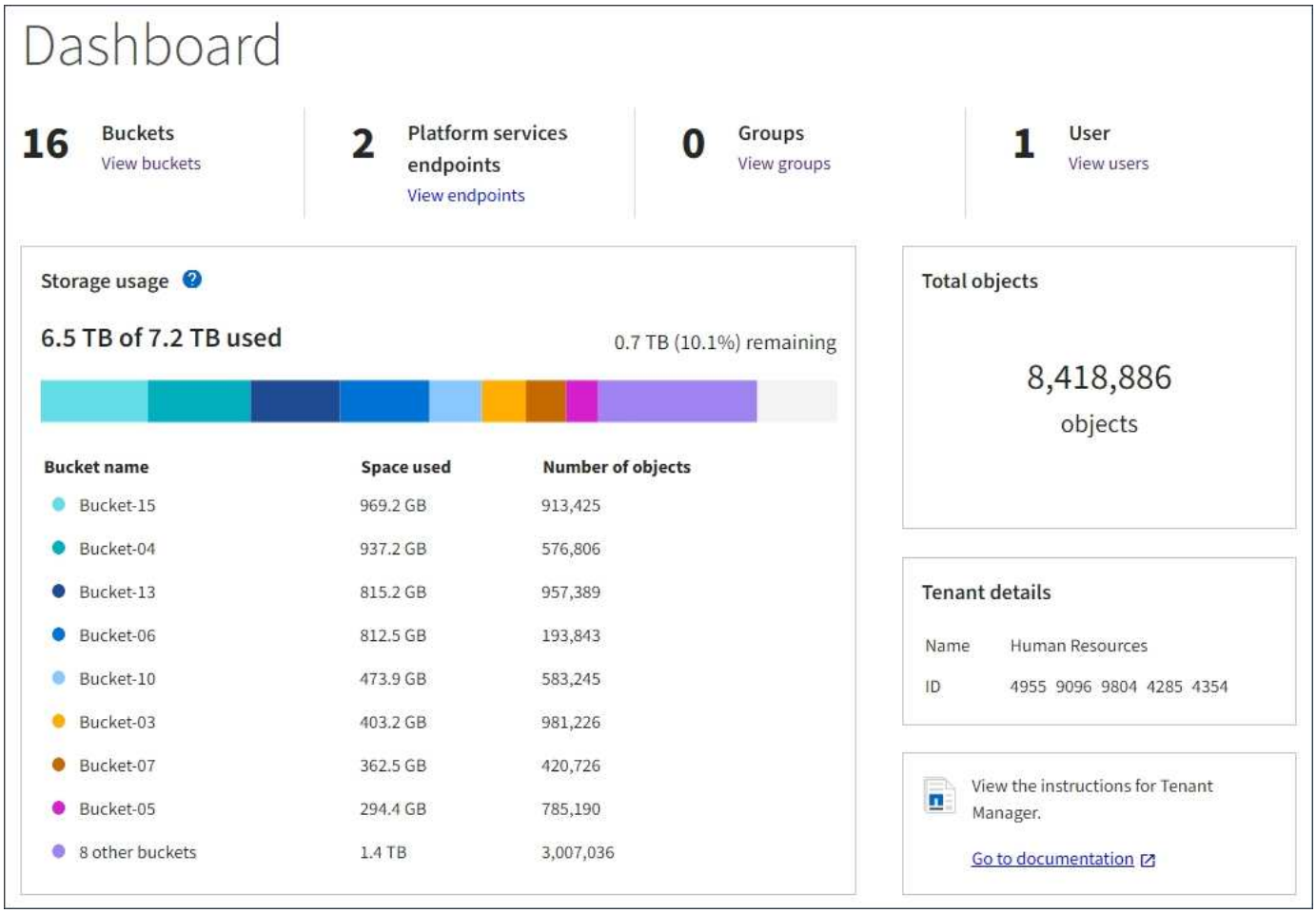
Compreender o Painel do Gestor do Locatário

O Painel do Gerenciador do Tenant 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 em contentores (Swift). Se o locatário tiver uma cota, o Dashboard mostrará quanto da cota é usada e quanto resta. Se houver algum erro relacionado à conta de

locatário, os erros serão exibidos no Painel de Controle.

> 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 de Controle se parece com o seguinte exemplo:



Resumo da conta do locatário

A parte superior do Painel contém as seguintes informações:

- O número de buckets ou contêineres configurados, grupos e usuários
- O número de endpoints de serviços de plataforma, se algum tiver sido configurado

Pode selecionar as ligações para ver os detalhes.

O lado direito do painel contém as seguintes informações:

- O número total de objetos para o locatário.

  Para uma conta do S3, se nenhum objeto tiver sido ingerido e você tiver a permissão de acesso root, as diretrizes de introdução aparecerão em vez do número total de objetos.

- O nome e o ID da conta do locatário.
- Um link para a documentação do StorageGRID.

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.

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

- 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.

Alertas de uso de cota

Se os alertas de uso de cota tiverem sido ativados no Gerenciador de Grade, eles aparecerão no Gerenciador de Locatário quando a cota for baixa ou excedida, da seguinte forma:

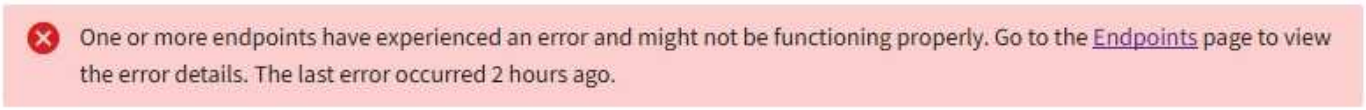
Se 90% ou mais da cota de um locatário tiver sido usada, o alerta **uso de cota de locatário alto** será acionado. Para obter mais informações, consulte a referência de alertas nas instruções para monitoramento e solução de problemas do StorageGRID.

Se você exceder sua cota, não poderá carregar novos objetos.

Para exibir detalhes adicionais e gerenciar regras e notificações para alertas, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

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 um erro de endpoint, selecione Endpoints para exibir a página Endpoints.

Informações relacionadas

"Solução de problemas de erros de endpoint de serviços de plataforma"

"Monitorizar Resolução de problemas"

Entendendo 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 Tenant usa a plataforma de API de código aberto Swagger. 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.

Para acessar a documentação do Swagger para a API de gerenciamento do locatário:

Passos

1. Inicie sessão no Gestor do Locatário.
2. Selecione **Ajuda Documentação da API** no cabeçalho do Gerenciador do Locatário.

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").

  Consulte ""proteção contra falsificação de solicitação entre sites"" para obter informações sobre como melhorar a segurança de autenticação.

  > Se o logon único (SSO) estiver ativado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte ""autenticar na API se o logon único estiver ativado"" nas instruções de administração do StorageGRID.

- **Config** — operações relacionadas à versão do produto e versões da API de Gerenciamento do locatário. 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, como segue:

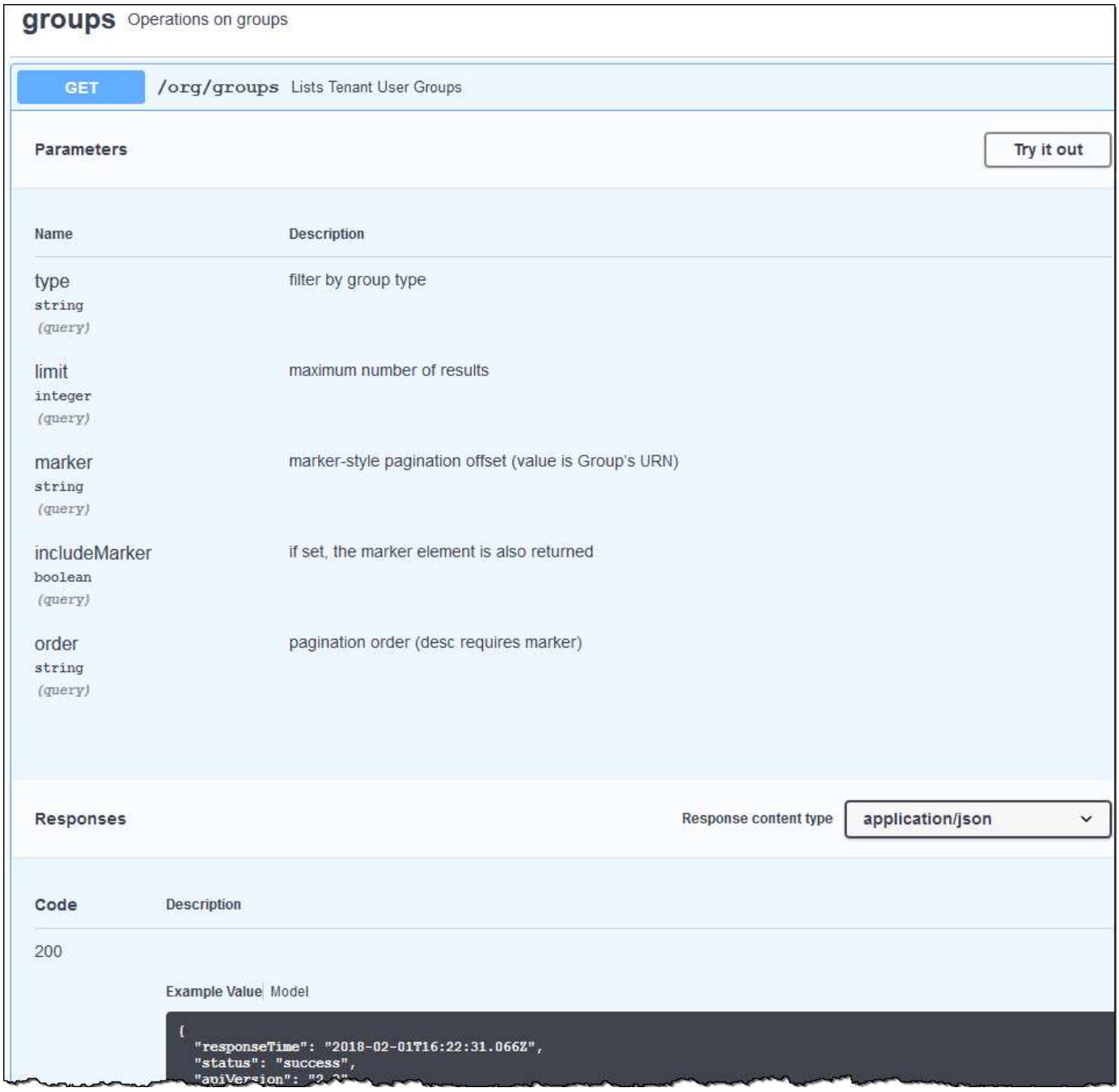
Protocolo	Permissão permite
S3	• Criação de buckets compatíveis e não compatíveis • Modificação das configurações de conformidade legadas • Definir o controle de consistência para operações executadas em objetos • Criando, atualizando e excluindo a configuração CORS de um bucket • Ativar e desativar as atualizações da última hora de acesso para objetos • Gerenciamento das configurações dos serviços da plataforma, incluindo replicação do CloudMirror, notificações e integração de pesquisa (notificação de metadados) • Eliminar buckets vazios
Rápido	Definir o nível de consistência usado para contentores

- **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.

- **Groups** — operações para gerenciar grupos de locatários locais e recuperar grupos de locatários federados de uma origem de identidade externa.
- **Identity-source** — operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **Regions** — operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **S3** — operações para gerenciar chaves de acesso S3 para usuários arrendatários.
- **S3-object-lock** — operações para determinar como o bloqueio global de objetos S3 (conformidade) é configurado para o sistema StorageGRID.
- **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.



Emissão de solicitações de API

Todas as operações de API que você executa usando a página da Web do API Docs são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. Clique na 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 clicar em **modelo** para aprender os requisitos para cada campo.

4. Clique em **Experimente**.
5. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
6. Clique em **Executar**.
7. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Informações relacionadas

"Proteção contra falsificação de solicitação entre sites (CSRF)"

"Administrar o StorageGRID"

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 3 da API.

```
https://hostname_or_ip_address/api/v3/authorize
```

A versão principal da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que são ***not compatible*** com versões mais antigas. A versão menor da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que ***are 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 o software StorageGRID é instalado pela primeira vez, apenas a versão mais recente da API de gerenciamento de locatário é ativada. No entanto, quando o StorageGRID é atualizado para uma nova versão de recurso, você continua a ter acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.

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

Determinando quais versões de API são suportadas na versão atual

Use a seguinte solicitação de API para retornar uma lista das principais versões da API suportada:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especificando uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v3`) ou um cabeçalho (`Api-Version: 3`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Proteção contra falsificação de solicitação entre sites (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 `"Content-Type: application/json"` cabeçalho para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

Gerenciamento do acesso do sistema para usuários de locatários

Você concede aos usuários acesso a uma conta de locatário importando grupos de uma origem de identidade federada e atribuindo permissões de gerenciamento. Você também pode criar grupos de locatários locais e usuários, a menos que o logon único (SSO) esteja em vigor para todo o sistema StorageGRID.

- "Usando a federação de identidade"
- "Gerenciando grupos"
- "Gerenciamento de usuários locais"

Usando 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.

- "Configurando uma fonte de identidade federada"
- "Forçando a sincronização com a fonte de identidade"
- "Desativando a federação de identidade"

Configurando uma fonte de identidade federada

Você pode configurar a federação de identidade se quiser que grupos de locatários e usuários sejam gerenciados em outro sistema, como ative Directory, OpenLDAP ou Oracle Directory Server.

O que você vai precisar

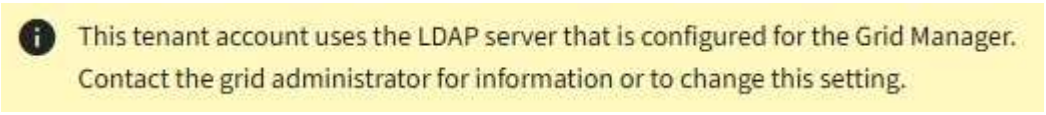
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve estar usando o ative Directory, OpenLDAP ou Oracle Directory Server como o provedor de

identidade. Se pretender utilizar um serviço LDAP v3 que não esteja listado, tem de contactar o suporte técnico.

- 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.

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.



Passos

1. Selecione **GERENCIAMENTO DE ACESSO federação de identidade**.
2. Selecione **Ativar federação de identidade**.
3. Na seção tipo de serviço LDAP, selecione **ative Directory**, **OpenLDAP** ou **Other**.

   Se selecionar **OpenLDAP**, configure o servidor OpenLDAP. Consulte as diretrizes para configurar um servidor OpenLDAP.

   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.
   - **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. Na secção Configurar servidor LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias.
   - **Nome do host**: O nome do host do servidor 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`
- **Senha**: A senha associada ao nome de usuário.
- **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 base do usuário** a que pertencem.

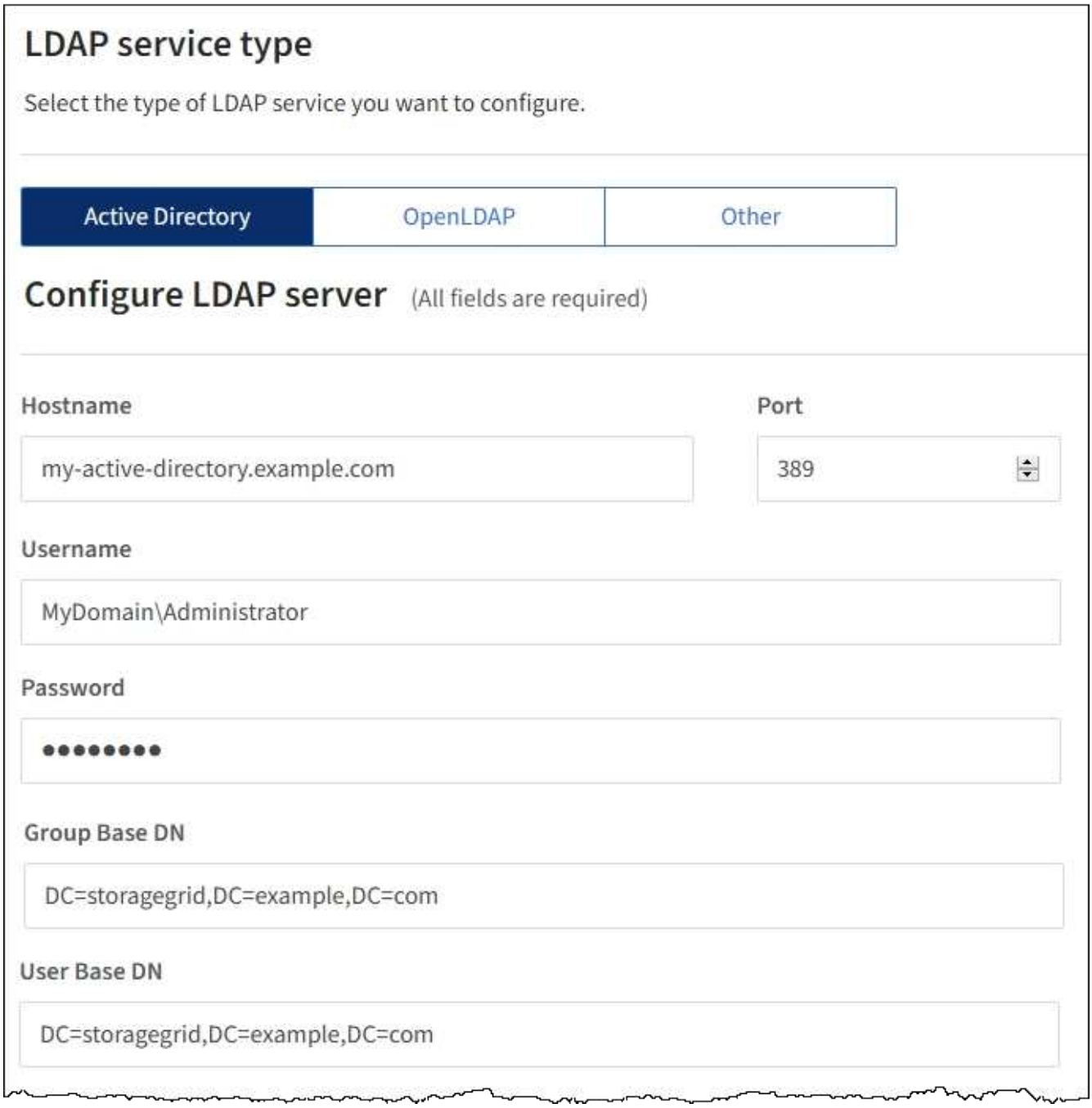
6. Na seção **Transport Layer Security (TLS)**, selecione uma configuração de segurança.
   - **Use STARTTLS (recomendado)**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada.
   - **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Esta opção é suportada por razões de compatibilidade.
   - **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido.

     Esta opção não é suportada 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 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.
8. Selecione **testar ligação** para validar as definições de ligação para o servidor LDAP.

   Uma mensagem de confirmação aparece no canto superior direito da página se a conexão for válida.
9. Se a conexão for válida, selecione **Salvar**.

   A captura de tela a seguir mostra valores de configuração de exemplo para um servidor LDAP que usa o ative Directory.



Informações relacionadas

"Permissões de gerenciamento do locatário"

"Diretrizes para configurar um servidor OpenLDAP"

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.

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as

instruções para manutenção de associação reversa em grupo no Guia do Administrador para OpenLDAP.

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 Guia do Administrador para OpenLDAP.

Forçando 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- A origem de identidade guardada tem de estar ativada.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO federação de identidade**.

   A página de federação de identidade é exibida. O botão **servidor de sincronização** está no canto superior direito da página.

   > ⓘ Se a origem de identidade salva não estiver ativada, o botão **servidor de sincronização** não estará ativo.

2. Selecione **servidor de sincronização**.

   É apresentada uma mensagem de confirmação a indicar que a sincronização foi iniciada com êxito.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Desativando a federação de identidade

Se você tiver configurado um serviço de federação de identidade para esse locatário, poderá desativar temporariamente ou permanentemente a federação de identidade para grupos de locatários e usuários. Quando a federação de identidade está desativada, não

há comunicação entre o sistema StorageGRID e a origem da identidade. No entanto, todas as configurações que você configurou são mantidas, permitindo que você reative facilmente a federação de identidade no futuro.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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 à conta do locatário até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a fonte de identidade não ocorrerá.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO federação de identidade**.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.
3. Selecione **Guardar**.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Gerenciando grupos

Você atribui permissões a grupos de usuários para controlar quais tarefas os usuários do locatário podem executar. Você pode importar grupos federados de uma origem de identidade, como o ative Directory ou o OpenLDAP, ou criar grupos locais.

> Se o logon único (SSO) estiver habilitado para o seu sistema StorageGRID, os usuários locais não poderão fazer login no Gerenciador do locatário, embora possam acessar os recursos S3 e Swift, com base nas permissões de grupo.

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. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Permissão	Descrição
Acesso à raiz	Fornece acesso total ao Gerenciador do Locatário e à API de Gerenciamento do Locatário. **Observação:** os usuários do 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 **Observação:** os usuários do Swift devem ter a permissão Swift Administrator para executar qualquer operação com a Swift REST API.
Gerencie suas próprias credenciais S3	Apenas S3 inquilinos. Permite que os usuários criem e removam suas próprias chaves de acesso S3. Os usuários que não têm essa permissão não veem a opção de menu **ARMAZENAMENTO (S3) My S3 Access Keys**.
Gerenciar todos os baldes	• S3 locatários: 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. Os usuários que não têm essa permissão não veem a opção de menu **Buckets**. • Swift tenants: Permite que usuários Swift controlem o nível de consistência para contentores Swift usando a API de Gerenciamento do locatário. **Observação:** você só pode atribuir a permissão Gerenciar todos os buckets a grupos Swift a partir da API de Gerenciamento de locatário. Você não pode atribuir essa permissão a grupos Swift usando o Gerenciador de inquilinos.
Gerir pontos finais	Apenas S3 inquilinos. Permite que os usuários usem o Gerenciador do Locatário ou a API de Gerenciamento do Locatário para criar ou editar endpoints, que são usados como o destino para os serviços da plataforma StorageGRID. Os usuários que não têm essa permissão não veem a opção de menu **endpoints de serviços da plataforma**.

Informações relacionadas

"Use S3"

"Use Swift"

Criando grupos para um locatário S3

Você pode gerenciar permissões para S3 grupos de usuários importando grupos federados ou criando grupos locais.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.

2. Selecione **criar grupo**.
3. 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.

4. 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.

5. Selecione **continuar**.
6. Selecione um modo de acesso. 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.
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do Tenant e gerenciar a configuração do locatário.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações nem 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.
7. Selecione as permissões de grupo para este grupo.

   Consulte as informações sobre permissões de gerenciamento de locatários.
8. Selecione **continuar**.
9. Selecione uma política de grupo para determinar quais permissões de acesso S3 os membros deste grupo terão.
   - **No S3 Access**: 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.
   - **Custom**: Os usuários do grupo recebem as permissões que você especificar na caixa de texto. Consulte as instruções para implementar um aplicativo cliente S3 para obter informações detalhadas sobre políticas de grupo, incluindo sintaxe de linguagem e exemplos.
10. 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.

    Neste exemplo, os membros do grupo só podem listar e acessar uma pasta que corresponda ao nome de usuário (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.

11. Selecione o botão que aparece, dependendo se você está criando um grupo federado ou um grupo local:

    - Grupo federado: **Criar grupo**
    - Grupo local: **Continuar**

    Se você estiver criando um grupo local, a etapa 4 (Adicionar usuários) será exibida após selecionar **continuar**. Esta etapa não aparece para grupos federados.

12. Marque a caixa de seleção para cada usuário que deseja adicionar ao grupo e selecione **criar grupo**.

    Opcionalmente, você pode salvar o grupo sem adicionar usuários. Você pode adicionar usuários ao grupo mais tarde ou selecionar o grupo quando adicionar novos usuários.

13. Selecione **Finish**.

    O grupo criado aparece na lista de grupos. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

"Use S3"

Criando 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 que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.

2. Selecione **criar grupo**.
3. 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.

4. 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.
5. Selecione **continuar**.
6. Selecione um modo de acesso. 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.

- **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do Tenant e gerenciar a configuração do locatário.
- **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações nem 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.

7. Defina a permissão Grupo.
   - Marque a caixa de seleção **Root Access** se os usuários precisarem fazer login na API de Gerenciamento de Tenant ou Tenant Manager. (Predefinição)
   - Desmarque a caixa de seleção **Root Access** se os usuários não precisarem de acesso ao Gerenciador do locatário ou à API de Gerenciamento do locatário. Por exemplo, desmarque a caixa de seleção para aplicativos que não precisam acessar o locatário. Em seguida, atribua a permissão **Swift Administrator** para permitir que esses usuários gerenciem contentores e objetos.
8. Selecione **continuar**.
9. Marque a caixa de seleção **Swift administrator** se o usuário precisar usar a Swift REST API.

   Os usuários Swift devem ter a permissão de acesso root para acessar o Gerenciador do locatário. No entanto, a permissão de acesso root não permite que os usuários se autentiquem na API REST do Swift para criar contentores e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

10. Selecione o botão que aparece, dependendo se você está criando um grupo federado ou um grupo local:
    - Grupo federado: **Criar grupo**
    - Grupo local: **Continuar**

      Se você estiver criando um grupo local, a etapa 4 (Adicionar usuários) será exibida após selecionar **continuar**. Esta etapa não aparece para grupos federados.

11. Marque a caixa de seleção para cada usuário que deseja adicionar ao grupo e selecione **criar grupo**.

    Opcionalmente, você pode salvar o grupo sem adicionar usuários. Você pode adicionar usuários ao grupo mais tarde ou selecionar o grupo quando criar novos usuários.

12. Selecione **Finish**.

    O grupo criado aparece na lista de grupos. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

"Use Swift"

Visualização e edição de detalhes do grupo

Ao exibir os detalhes de um grupo, você pode alterar o nome de exibição, as permissões, as políticas e os usuários que pertencem ao grupo.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.

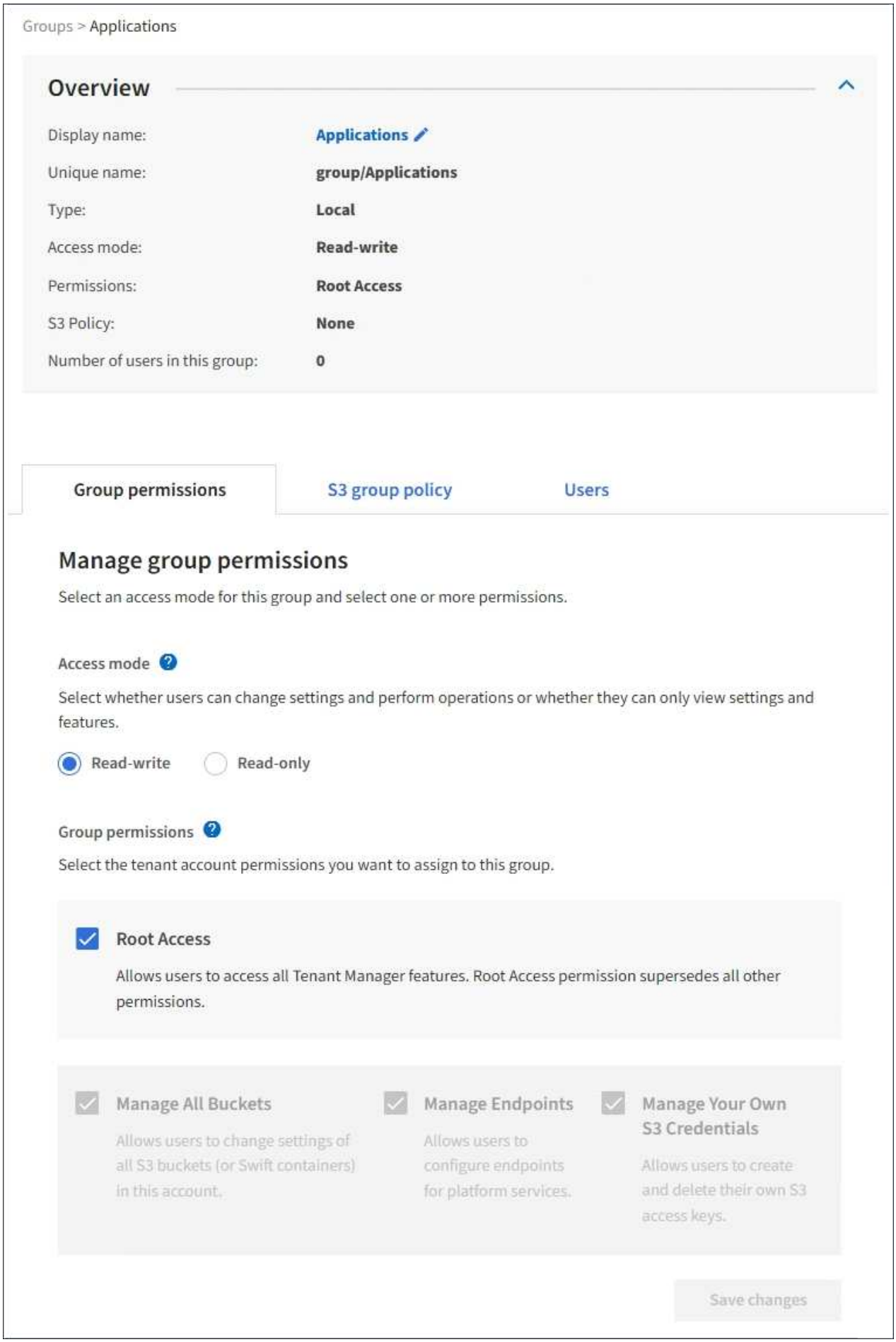
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Selecione o nome do grupo cujos detalhes deseja exibir ou editar.

   Alternativamente, você pode selecionar **ações Exibir detalhes do grupo**.

   A página de detalhes do grupo é exibida. O exemplo a seguir mostra a página de detalhes do grupo S3.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Faça alterações nas definições do grupo conforme necessário.

> Para garantir que suas alterações sejam salvas, selecione **Salvar alterações** depois de fazer alterações em cada seção. Quando as alterações são salvas, uma mensagem de confirmação aparece no canto superior direito da página.

   a. Opcionalmente, selecione o nome de exibição ou o ícone de edição para atualizar o nome de exibição.

      Não é possível alterar o nome exclusivo de um grupo. Não é possível editar o nome de exibição de um grupo federado.

   b. Opcionalmente, atualize as permissões.

   c. Para a política de grupo, faça as alterações apropriadas para o seu locatário S3 ou Swift.

      - Se você estiver editando um grupo para um locatário S3, opcionalmente, selecione uma política de grupo S3 diferente. Se você selecionar uma política S3 personalizada, atualize a cadeia de carateres JSON conforme necessário.
      - Se você estiver editando um grupo para um locatário Swift, opcionalmente selecione ou desmarque a caixa de seleção **Administrador Swift**.

        Para obter mais informações sobre a permissão Swift Administrator, consulte as instruções para criar grupos para um locatário Swift.

   d. Opcionalmente, adicione ou remova usuários.

4. Confirme que selecionou **Guardar alterações** para cada secção alterada.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Criando grupos para um locatário S3"

"Criando grupos para um locatário Swift"

Adicionando usuários a um grupo local

Você pode adicionar usuários a um grupo local conforme necessário.

O que você vai precisar

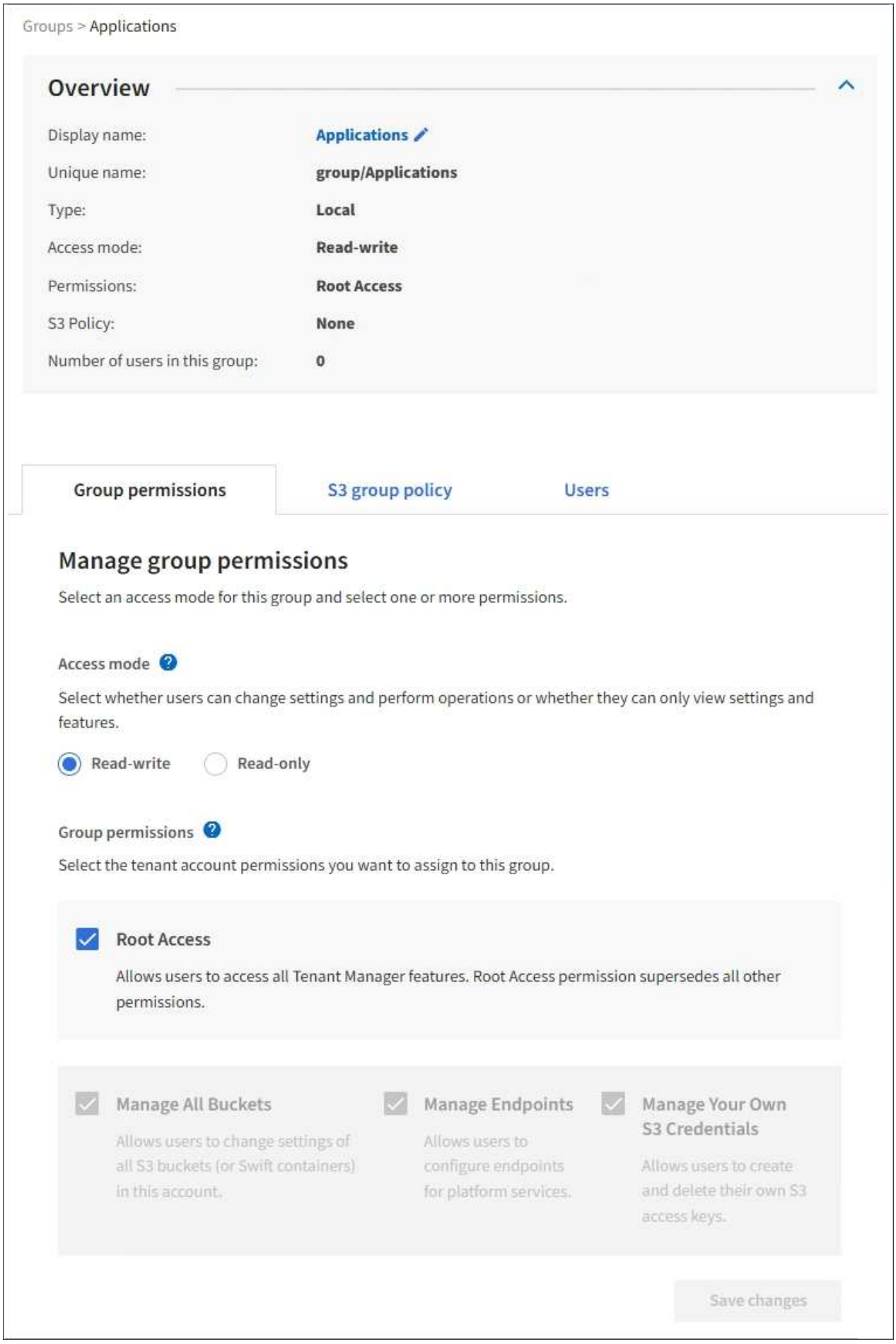
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

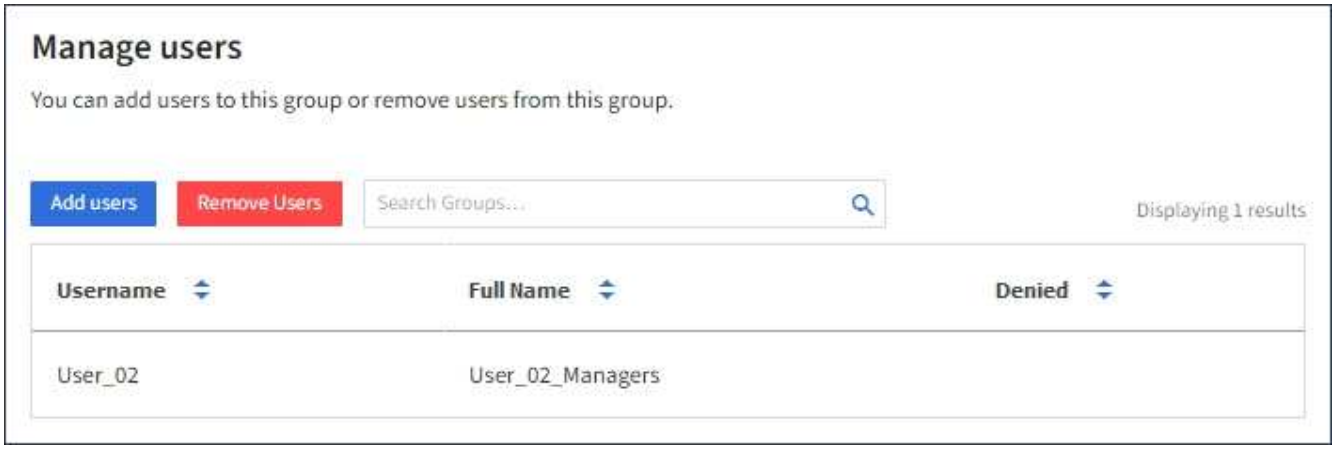
1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Selecione o nome do grupo local ao qual deseja adicionar usuários.

   Alternativamente, você pode selecionar **ações Exibir detalhes do grupo**.

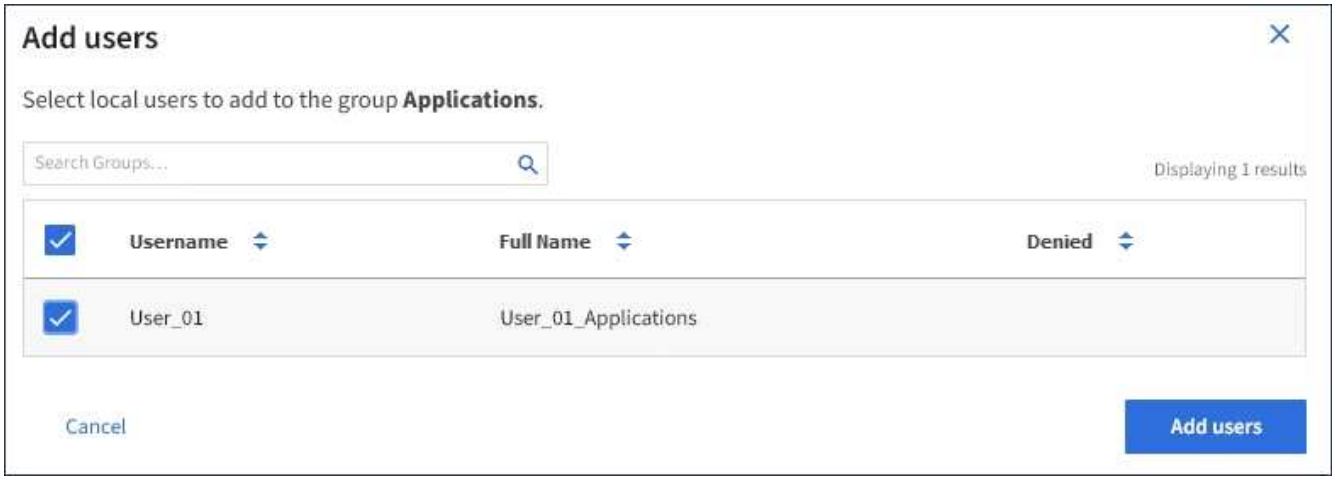
   A página de detalhes do grupo é exibida.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Selecione **Gerenciar usuários** e, em seguida, selecione **Adicionar usuários**.



4. Selecione os usuários que deseja adicionar ao grupo e selecione **Adicionar usuários**.



Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Editar um nome de grupo

Pode editar o nome de apresentação de um grupo. Não é possível editar o nome exclusivo de um grupo.

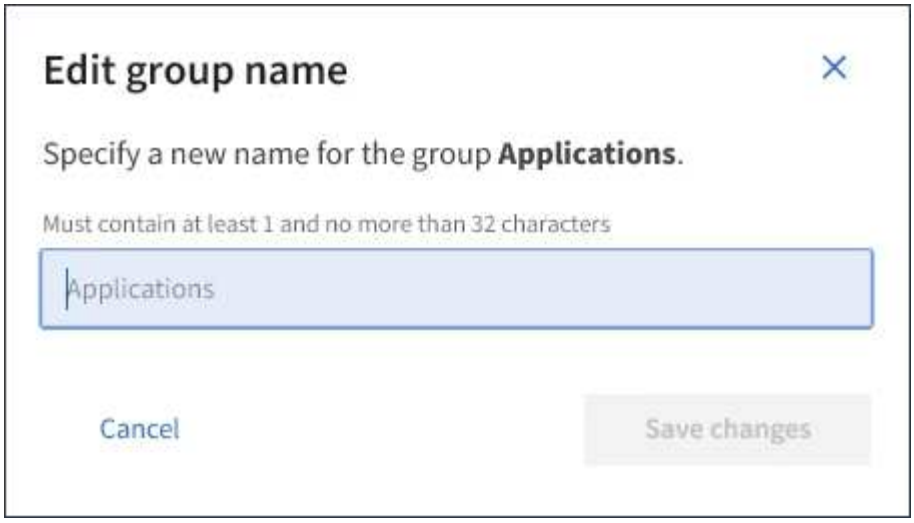
O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Marque a caixa de seleção do grupo cujo nome de exibição deseja editar.
3. Selecione **ações Editar nome do grupo**.

   A caixa de diálogo Editar nome do grupo é exibida.



4. Se estiver editando um grupo local, atualize o nome de exibição conforme necessário.

   Não é possível alterar o nome exclusivo de um grupo. Não é possível editar o nome de exibição de um grupo federado.

5. Selecione **Salvar alterações**.

   Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Duplicando um grupo

Você pode criar novos grupos mais rapidamente duplicando um grupo existente.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Marque a caixa de seleção do grupo que deseja duplicar.
3. Selecione **Duplicate group**. Para obter detalhes adicionais sobre a criação de um grupo, consulte as instruções para criar grupos para um locatário S3 ou para um locatário Swift.
4. 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.

5. 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.

6. Selecione **continuar**.
7. Conforme necessário, modifique as permissões para este grupo.
8. Selecione **continuar**.
9. Conforme necessário, se você estiver duplicando um grupo para um locatário S3, opcionalmente, selecione uma política diferente nos botões de opção **Adicionar política S3**. Se você selecionou uma política personalizada, atualize a cadeia de carateres JSON conforme necessário.
10. Selecione **criar grupo**.

Informações relacionadas

"Criando grupos para um locatário S3"

"Criando grupos para um locatário Swift"

"Permissões de gerenciamento do locatário"

Eliminar um grupo

Pode eliminar um grupo do sistema. Quaisquer usuários que pertençam apenas a esse grupo não poderão mais entrar no Gerenciador do Locatário ou usar a conta do locatário.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.

2. Marque as caixas de seleção dos grupos que deseja excluir.
3. Selecione **ações Excluir grupo**.

   É apresentada uma mensagem de confirmação.

4. Selecione **Excluir grupo** para confirmar que deseja excluir os grupos indicados na mensagem de confirmação.

   Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Gerenciamento de 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, não é possível remover o usuário root.

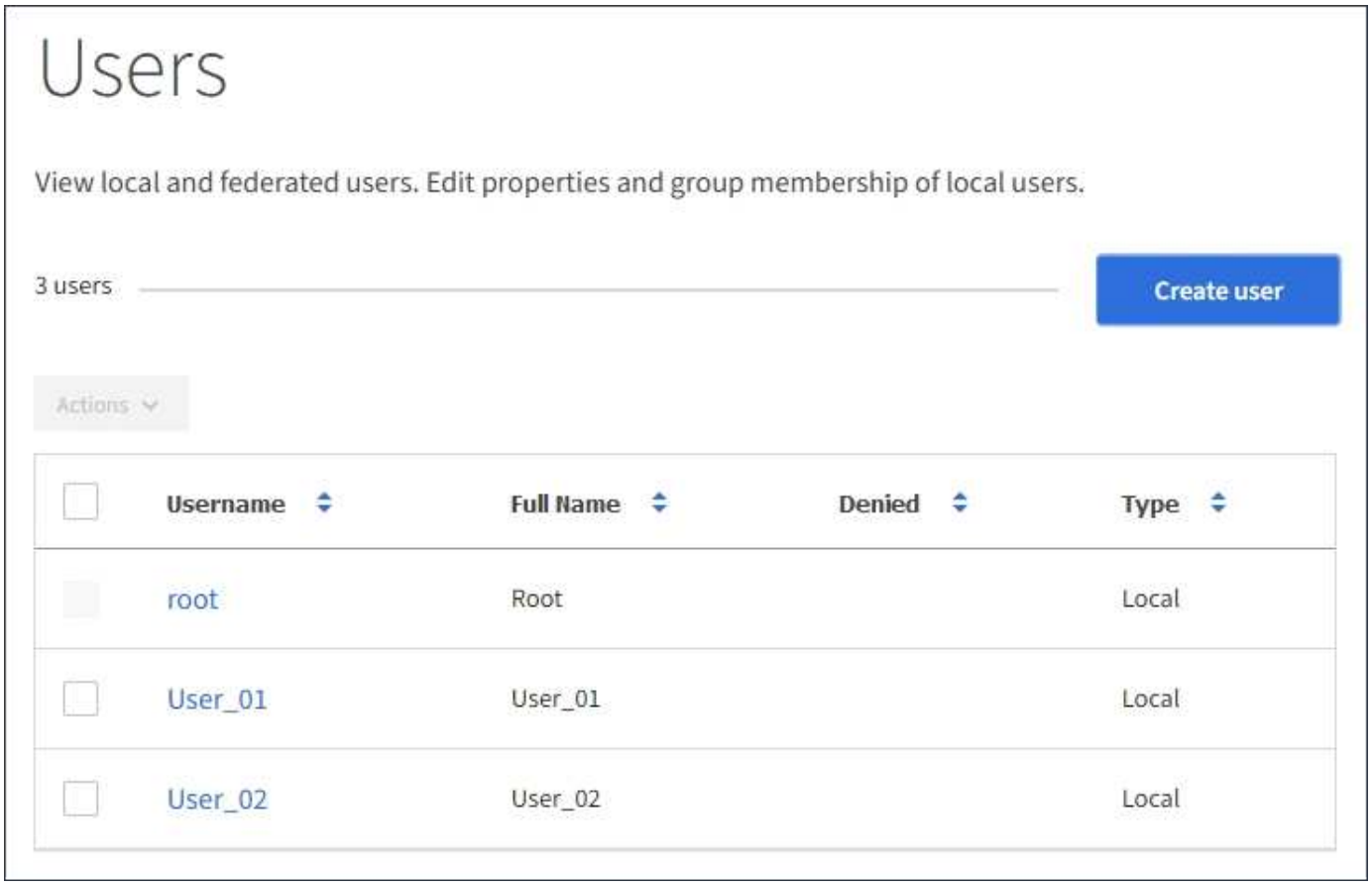
O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários de leitura e gravação que tenha a permissão de acesso root.

> Se o logon único (SSO) estiver habilitado para o seu 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 S3 ou Swift para acessar os recursos do locatário, com base nas permissões de grupo.

Acessando a página usuários

Selecione **GERENCIAMENTO DE ACESSO usuários**.



Criando usuários locais

Você pode criar usuários locais e atribuí-los 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.

Passos

1. Selecione **criar usuário**.
2. Preencha os campos a seguir.
   - **Nome completo**: O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo.
   - **Nome de usuário**: O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados.
   - * Senha*: Uma senha, que é usada quando o usuário entra.
   - **Confirm password**: Digite a mesma senha digitada no campo Senha.
   - **Negar acesso**: Se você selecionar **Sim**, esse usuário não poderá entrar na conta de locatário, mesmo que o usuário ainda possa pertencer a um ou mais grupos.

     Como exemplo, você pode usar esse recurso para suspender temporariamente a capacidade de um

usuário fazer login.

3. Selecione **continuar**.
4. Atribua o usuário a um ou mais grupos locais.

   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.

5. Selecione **criar usuário**.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Editando detalhes do usuário

Ao editar os detalhes de um usuário, você pode alterar o nome completo e a senha do usuário, adicionar o usuário a diferentes grupos e impedir que o usuário acesse o locatário.

Passos

1. Na lista Users (utilizadores), selecione o nome do utilizador cujos detalhes pretende ver ou editar.

   Alternativamente, você pode selecionar a caixa de seleção para o usuário e, em seguida, selecionar **ações Exibir detalhes do usuário**.

2. Faça alterações nas definições do utilizador, conforme necessário.
   a. Altere o nome completo do usuário conforme necessário selecionando o nome completo ou o ícone de edição na seção Visão geral.

      Você não pode alterar o nome de usuário.

   b. Na guia **Senha**, altere a senha do usuário conforme necessário.
   c. Na guia **Access**, permita que o usuário faça login (selecione **não**) ou impeça que o usuário faça login (selecione **Sim**) conforme necessário.
   d. Na guia **Groups**, adicione o usuário aos grupos ou remova o usuário dos grupos conforme necessário.
   e. Conforme necessário para cada seção, selecione **Salvar alterações**.

      As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Duplicação de usuários locais

Você pode duplicar um usuário local para criar um novo usuário mais rapidamente.

Passos

1. Na lista usuários, selecione o usuário que deseja duplicar.
2. Selecione **Duplicate user**.
3. Modifique os campos a seguir para o novo usuário.
   - **Nome completo**: O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo.
   - **Nome de usuário**: O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados.

- * Senha*: Uma senha, que é usada quando o usuário entra.
- **Confirm password**: Digite a mesma senha digitada no campo Senha.
- **Negar acesso**: Se você selecionar **Sim**, esse usuário não poderá entrar na conta de locatário, mesmo que o usuário ainda possa pertencer a um ou mais grupos.

  Como exemplo, você pode usar esse recurso para suspender temporariamente a capacidade de um usuário fazer login.

4. Selecione **continuar**.
5. Selecione um ou mais grupos locais.

   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.

6. Selecione **criar usuário**.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Eliminar utilizadores locais

Você pode excluir permanentemente usuários locais que não precisam mais acessar a conta de locatário do StorageGRID.

Usando o Gerenciador do Locatário, você pode excluir usuários locais, mas não usuários federados. Você deve usar a origem de identidade federada para excluir usuários federados.

Passos

1. Na lista Users (utilizadores), selecione a caixa de verificação para o utilizador local que pretende eliminar.
2. Selecione **ações Excluir usuário**.
3. Na caixa de diálogo de confirmação, selecione **Excluir usuário** para confirmar que deseja excluir o usuário do sistema.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Gerenciamento de contas de locatários do S3

Você pode usar o Gerenciador do Locatário para gerenciar chaves de acesso do S3 e criar e gerenciar buckets do S3.

- "Gerenciando chaves de acesso S3"
- "Gerenciamento de buckets do S3"

Gerenciando chaves de acesso S3

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.

Sobre esta tarefa

As chaves de acesso S3 podem ser gerenciadas 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 **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.

Criando 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 na conta de locatário do S3.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter a permissão Gerenciar suas próprias credenciais do S3.

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 novas chaves periodicamente, não será necessário definir um tempo de expiração para suas chaves. Se você decidir mais tarde criar novas chaves, exclua as chaves antigas manualmente.

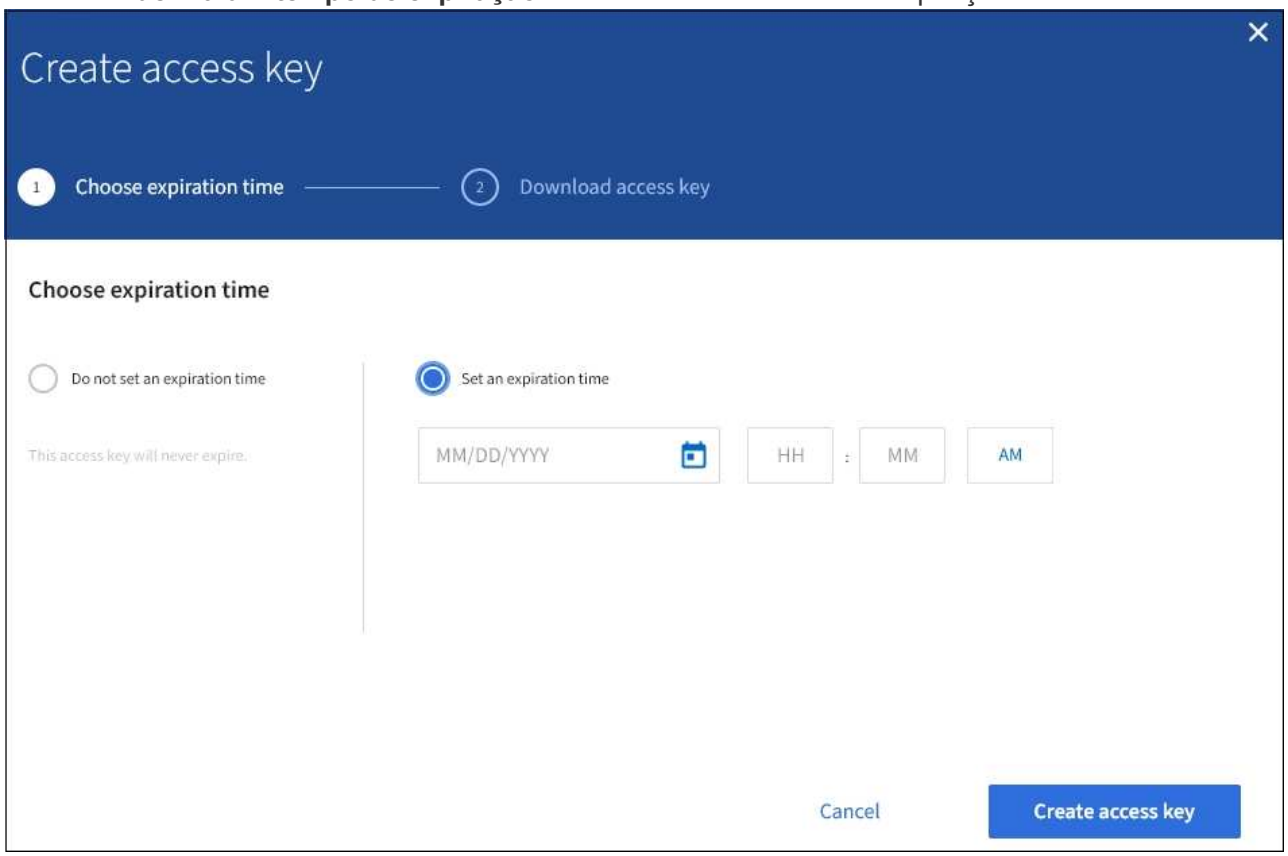
> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova 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.

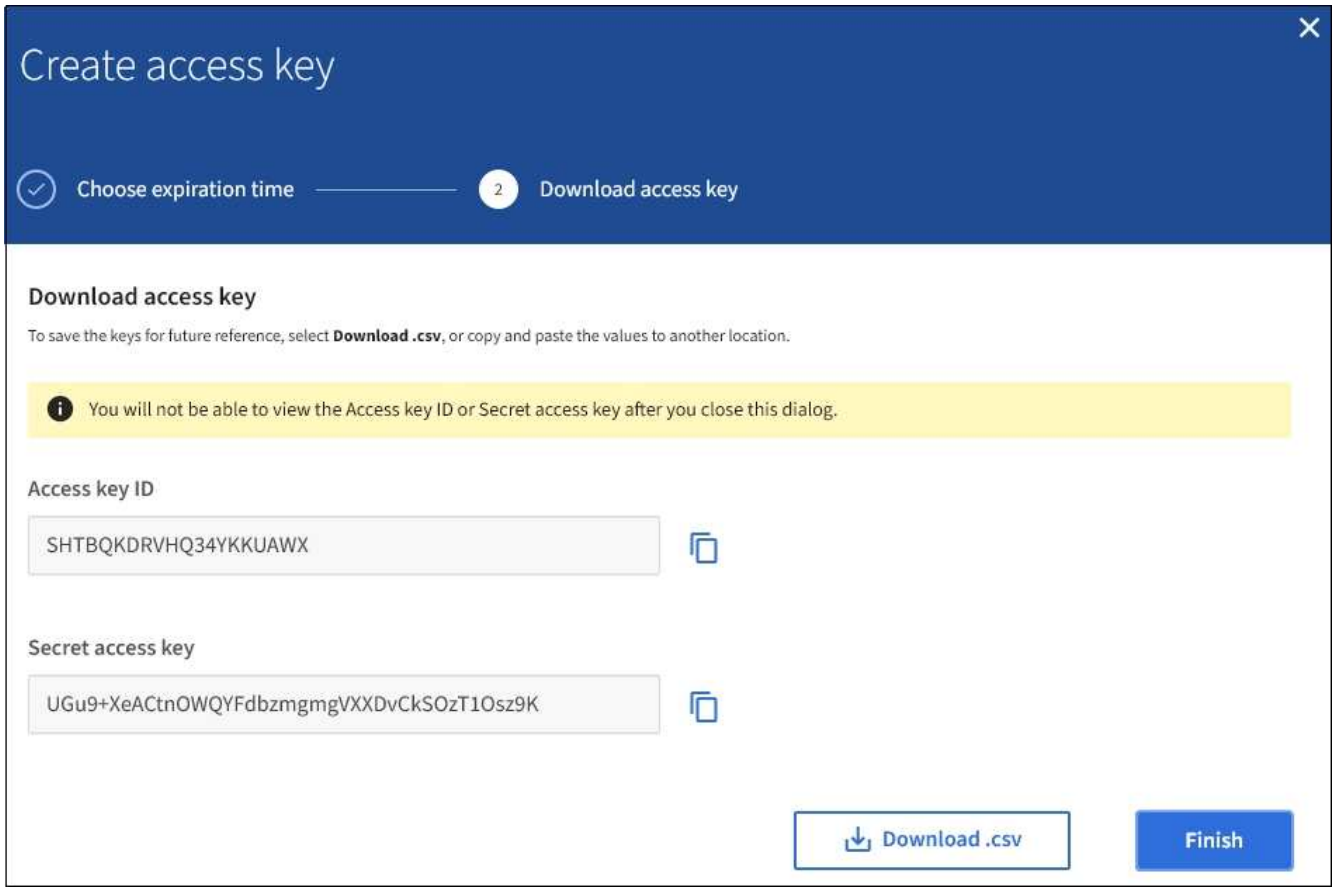


4. Selecione **criar chave de acesso**.

   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.



6. Selecione **Finish**.

   A nova chave está listada na página Minhas chaves de acesso. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Visualizar as suas teclas de acesso S3

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, você poderá exibir uma lista de suas 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 criar novas chaves ou excluir chaves que você não está mais usando.

O que você vai precisar

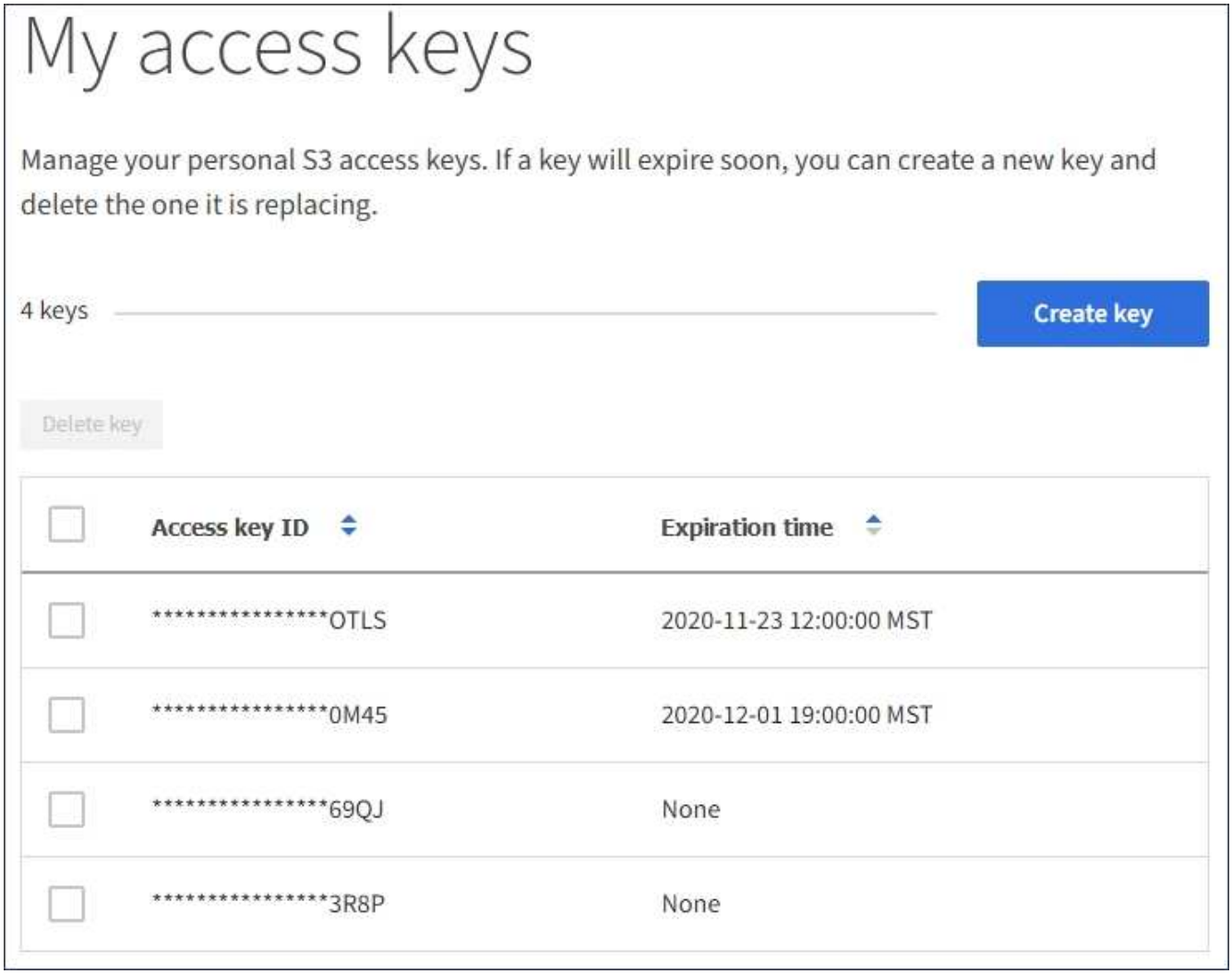
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter a permissão Gerenciar suas próprias credenciais do S3.

> 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**.

   A página Minhas chaves de acesso é exibida e lista todas as chaves de acesso existentes.



2. Classifique as chaves por **tempo de expiração** ou **ID da chave de acesso**.
3. Conforme necessário, crie novas chaves e exclua manualmente as chaves que você não está 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.

Informações relacionadas

"Criando suas próprias chaves de acesso S3"

"Eliminar as suas próprias chaves de acesso S3"

Eliminar 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter a permissão Gerenciar suas próprias credenciais do 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.

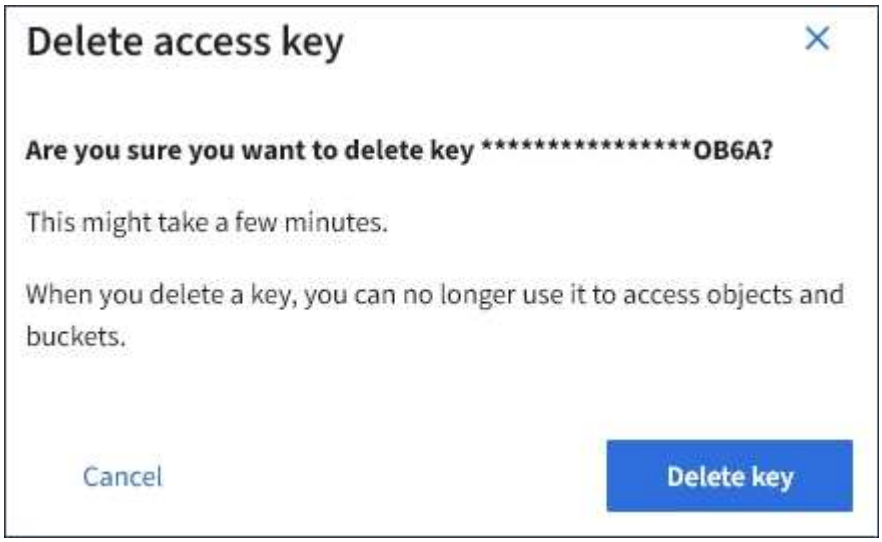
Passos

1. Selecione **ARMAZENAMENTO (S3)** > **as minhas chaves de acesso**.

   A página Minhas chaves de acesso é exibida e lista todas as chaves de acesso existentes.

2. Marque a caixa de seleção para cada chave de acesso que deseja remover.
3. Selecione **Delete key**.

   É apresentada uma caixa de diálogo de confirmação.



4. Selecione **Delete key**.

   Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Criando 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter a permissão de acesso root.

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, não será necessário definir um tempo de expiração para as chaves. Se você decidir mais tarde criar novas chaves, exclua as chaves antigas manualmente.

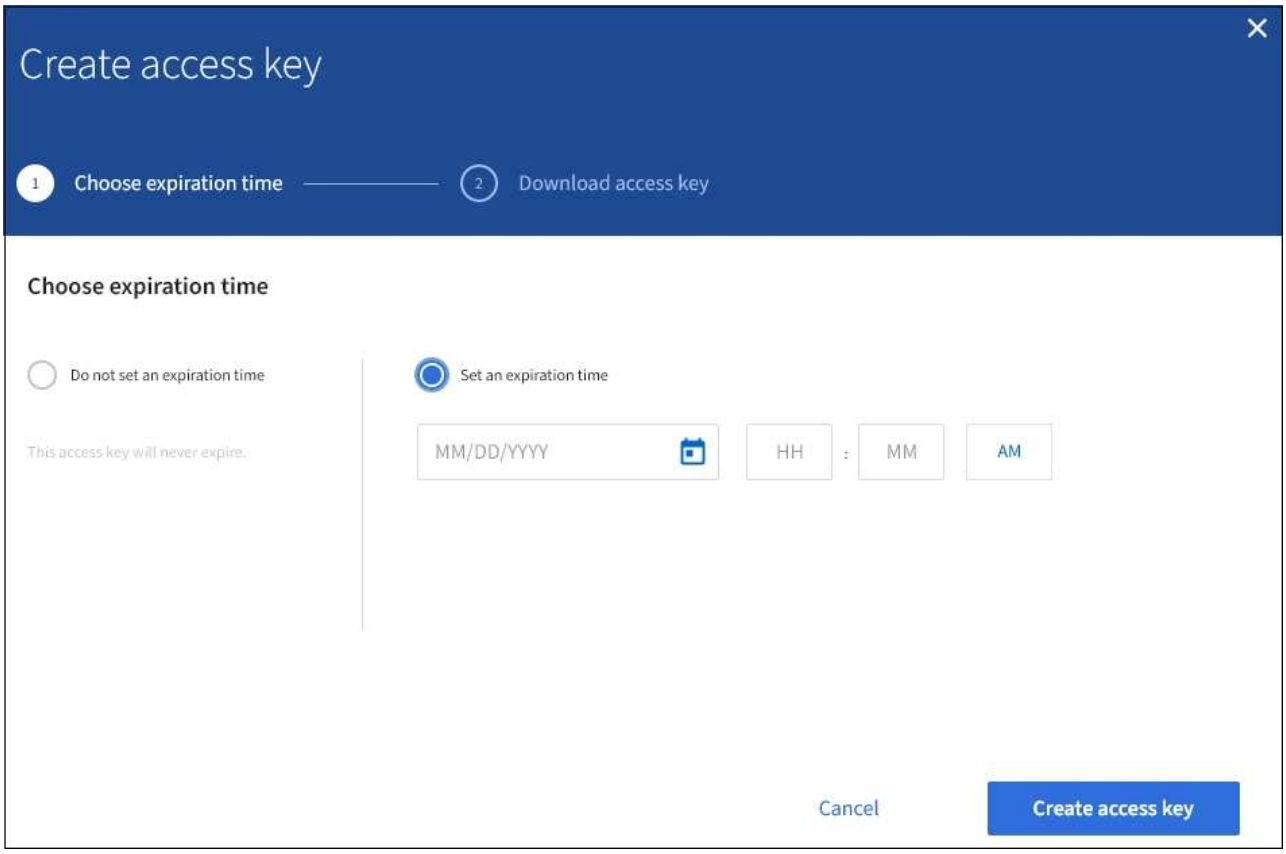
> Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para esse usuário no Gerenciador do locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova 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.

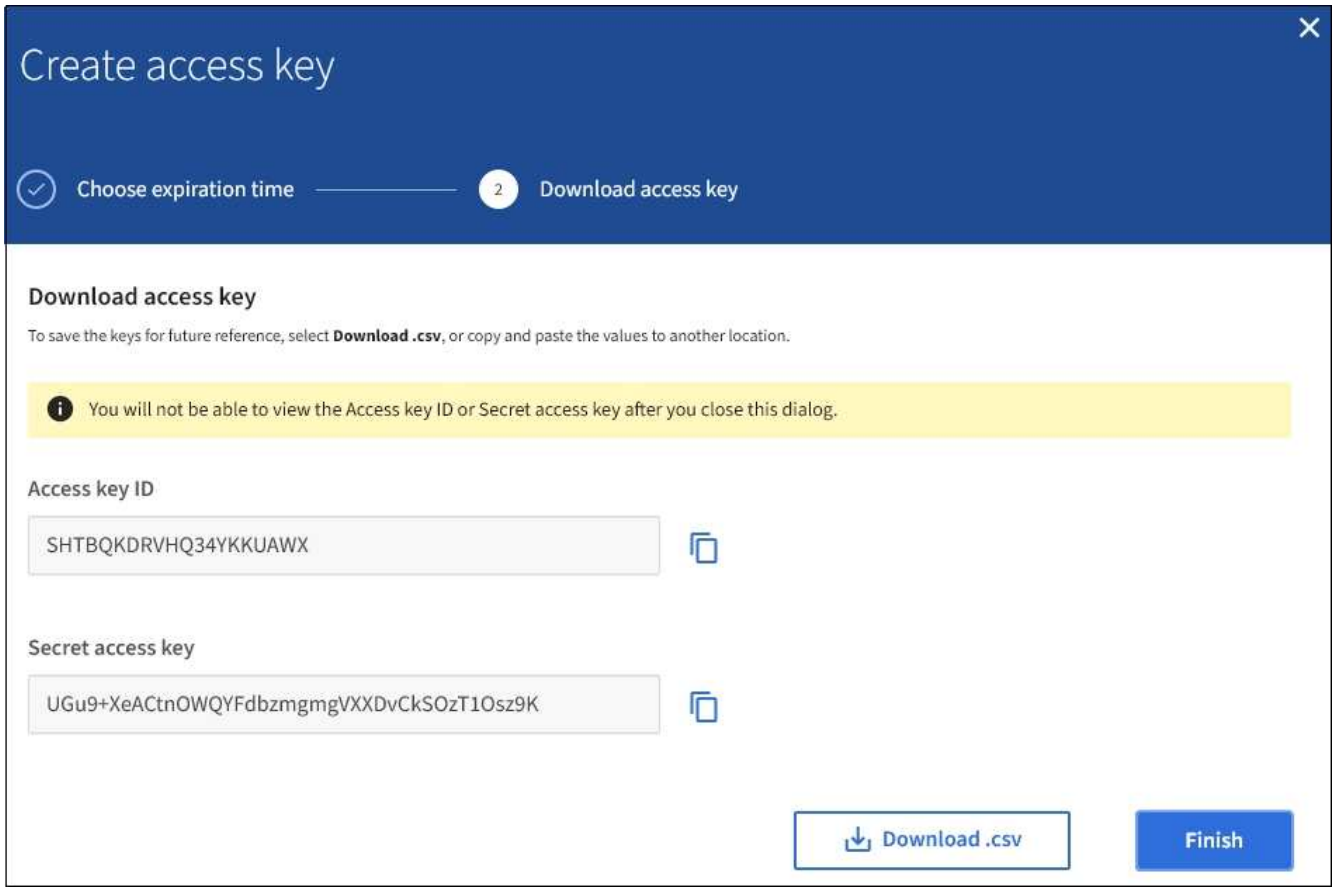


5. Selecione **criar chave de acesso**.

   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.



7. Selecione **Finish**.

   A nova chave está listada na guia teclas de acesso da página de detalhes do usuário. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Visualizar as teclas de acesso S3 de outro utilizador

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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter a permissão de acesso root.

> 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

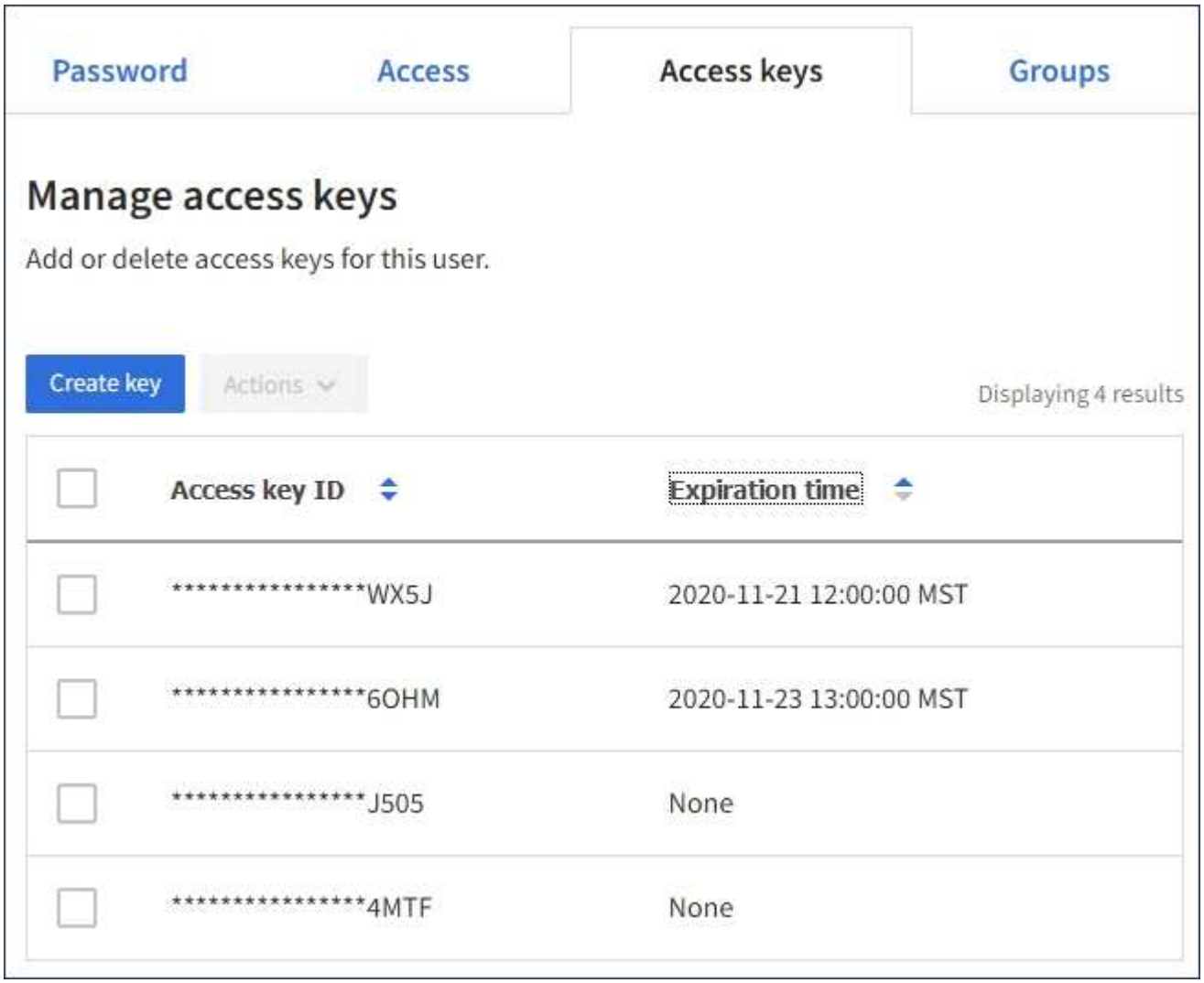
1. Selecione **GERENCIAMENTO DE ACESSO usuários**.

   A página usuários é exibida e lista os usuários existentes.

2. Selecione o utilizador cujas teclas de acesso S3 pretende visualizar.

   É apresentada a página Detalhes do utilizador.

3. 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

"Criando as chaves de acesso S3 de outro usuário"

"Eliminar as teclas de acesso S3 de outro utilizador"

Excluindo as chaves de acesso S3 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter a permissão de acesso root.

> 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**.

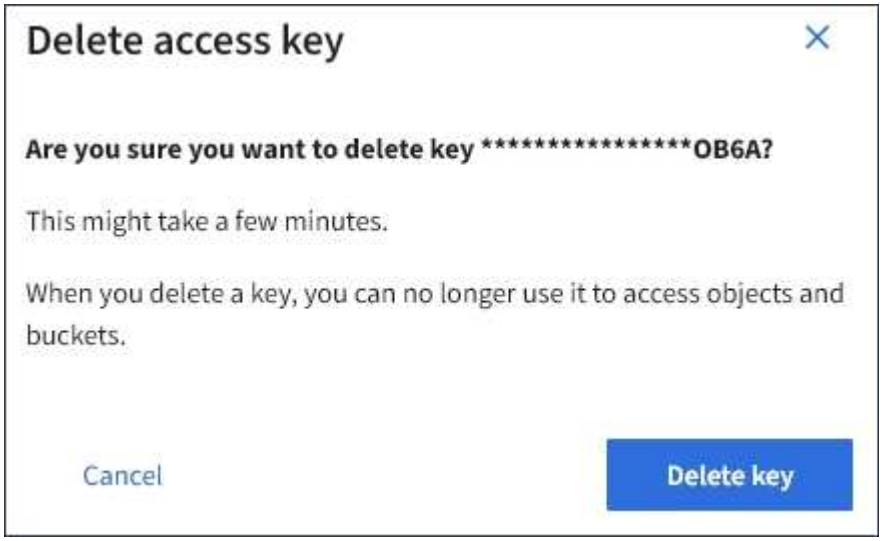
   A página usuários é exibida e lista os usuários existentes.

2. Selecione o usuário cujas chaves de acesso S3 você deseja gerenciar.

   É apresentada a página Detalhes do utilizador.

3. 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**.

   É apresentada uma caixa de diálogo de confirmação.



5. Selecione **Delete key**.

Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Gerenciamento de buckets do S3

Se você estiver usando um locatário S3 com as permissões apropriadas, você poderá criar, exibir e excluir buckets do S3, atualizar configurações de nível de consistência, configurar o Compartilhamento de recursos entre origens (CORS), ativar e desativar as configurações de atualização da última hora de acesso e gerenciar os serviços da plataforma S3.

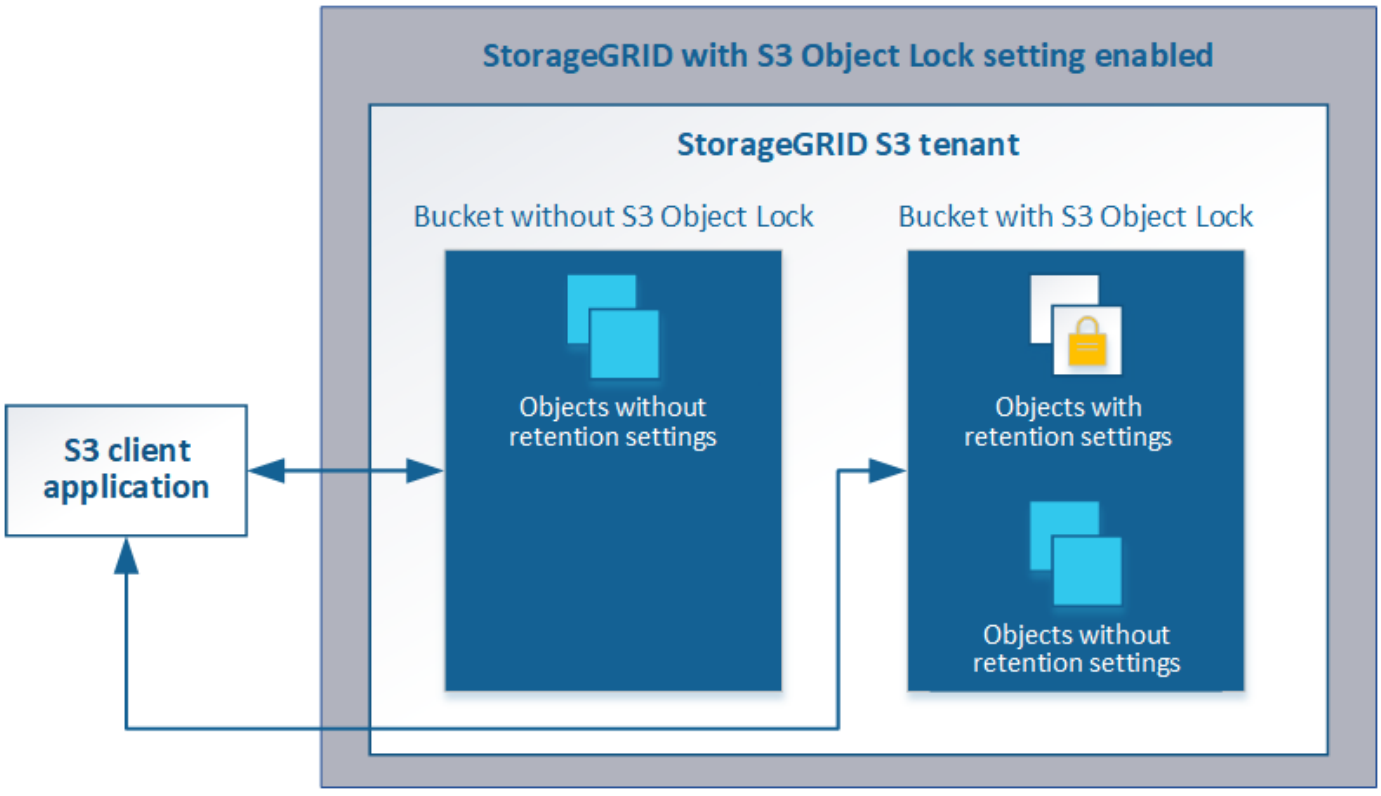
Usando S3 Object Lock

Você pode usar o recurso bloqueio de objetos S3 no StorageGRID se seus objetos precisarem cumprir com os requisitos regulamentares para retenção.

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).

Como mostrado na figura, quando a configuração global de bloqueio de objeto S3D está ativada para um sistema StorageGRID, uma conta de locatário S3D pode criar buckets com ou sem bloqueio de objeto S3D ativado. Se um bucket tiver o bloqueio de objeto S3 ativado, os aplicativos cliente S3 podem, opcionalmente, especificar configurações de retenção para qualquer versão de objeto nesse bucket. Uma versão de objeto deve ter configurações de retenção especificadas para ser protegida pelo bloqueio de objeto S3.



O recurso bloqueio de objetos do StorageGRID S3 fornece um modo de retenção único equivalente ao modo de conformidade do Amazon S3. Por padrão, uma versão de objeto protegido não pode ser substituída ou excluída por nenhum usuário. O recurso bloqueio de objetos do StorageGRID S3 não suporta um modo de governança e não permite que usuários com permissões especiais ignorem as configurações de retenção ou excluam objetos protegidos.

Se um bucket tiver o bloqueio de objeto S3 ativado, o aplicativo cliente S3 pode, opcionalmente, especificar uma ou ambas as seguintes configurações de retenção no nível do objeto ao criar ou atualizar um objeto:

- **Retent-until-date**: Se a data de retent-until de uma versão de objeto for no futuro, o objeto pode ser recuperado, mas não pode ser modificado ou excluído. Conforme necessário, a data de retenção até um objeto pode ser aumentada, mas essa data não pode ser diminuída.
- **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.

Para obter detalhes sobre essas configurações, vá para ""usando o bloqueio de objetos S3"" em "S3 operações e limitações suportadas pela API REST".

Gerenciamento de 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, consulte o artigo da base de dados de Conhecimento da NetApp.

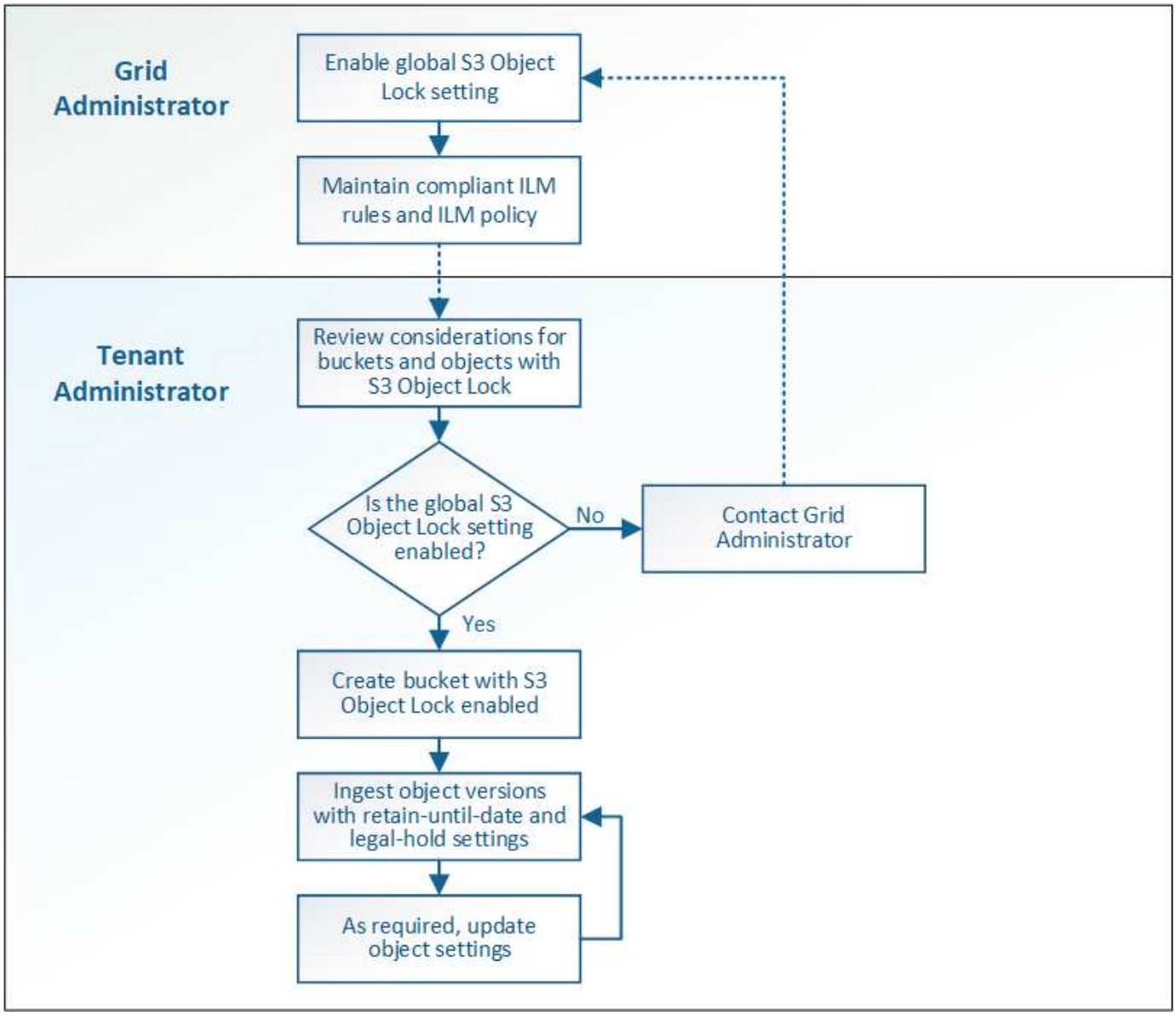
"Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

S3 fluxo de trabalho Object Lock

O diagrama de fluxo de trabalho mostra as etapas de alto nível para usar o recurso bloqueio de objetos S3 no StorageGRID.

Antes de criar buckets com o bloqueio de objeto S3 ativado, o administrador de grade deve ativar a configuração global de bloqueio de objeto S3 para todo o sistema StorageGRID. O administrador da grade também deve garantir que a política de gerenciamento do ciclo de vida das informações (ILM) seja "compatível"; ela deve atender aos requisitos dos buckets com o bloqueio de objetos S3 ativado. Para obter detalhes, entre em Contato com o administrador da grade ou consulte as instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

Depois que a configuração global S3 Object Lock for ativada, você poderá criar buckets com o S3 Object Lock ativado. Em seguida, você pode usar o aplicativo cliente S3 para especificar opcionalmente as configurações de retenção para cada versão do objeto.



Informações relacionadas

"Gerenciar objetos com ILM"

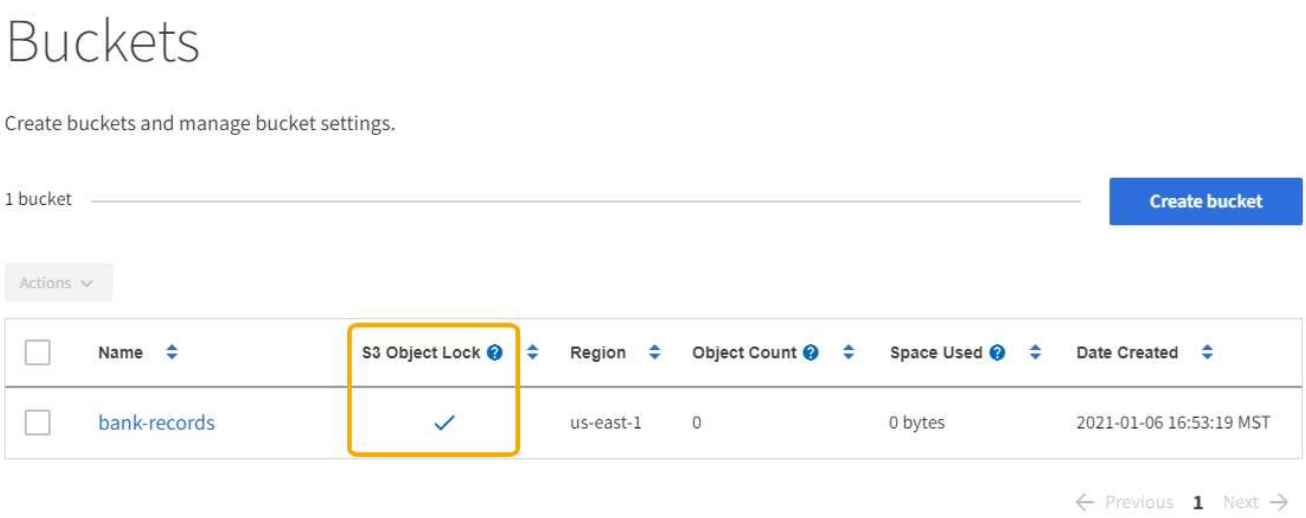
Requisitos para o bloqueio de objetos S3

Antes de ativar o bloqueio de objeto S3 para um bucket, revise os requisitos para buckets e objetos do bloqueio de objeto S3 e o ciclo de vida dos objetos em buckets com o bloqueio de objeto S3 ativado.

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.

  Este exemplo do Gerenciador do Locatário mostra um bucket 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 S3D para um bucket existente.
- O controle de versão do bucket é necessário com o S3 Object Lock. Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket.
- Depois de criar um bucket com o bloqueio de objetos S3 ativado, não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão desse bucket.
- Um bucket do StorageGRID que tenha o bloqueio de objetos S3 ativado não tem um período de retenção padrão. Em vez disso, o aplicativo cliente S3 pode, opcionalmente, especificar uma data de retenção e uma configuração de retenção legal para cada versão de objeto adicionada a esse bucket.
- A configuração do ciclo de vida do bucket é compatível com buckets do ciclo de vida do objeto do S3.
- 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

- O aplicativo cliente S3 deve especificar configurações de retenção para cada objeto que precisa ser protegido pelo bloqueio de objetos S3.
- Você pode aumentar a data de retenção até uma versão de objeto, mas nunca pode diminuir esse valor.
- Se você for notificado de uma ação legal pendente ou investigação regulatória, poderá preservar informações relevantes colocando uma retenção legal em uma versão de objeto. Quando uma versão de objeto está sob uma retenção legal, esse objeto não pode ser excluído do StorageGRID, mesmo que tenha atingido sua data de retenção até. Assim que a retenção legal for levantada, a versão do objeto pode ser excluída se a data de retenção for atingida.
- S3 Object Lock requer o uso de buckets versionados. 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 três estágios:

1. * Ingestão de objetos*
    - Ao adicionar uma versão de objeto a um bucket com o bloqueio de objeto S3 ativado, o aplicativo

cliente S3 pode, opcionalmente, especificar configurações de retenção para o objeto (reter até a data, retenção legal ou ambos). Em seguida, o StorageGRID gera metadados para esse objeto, que inclui um identificador de objeto exclusivo (UUID) e a data e hora de ingestão.

- Depois que uma versão de objeto com configurações de retenção é ingerida, seus dados e metadados S3 definidos pelo usuário não podem ser modificados.
- O StorageGRID armazena os metadados do objeto independentemente dos dados do objeto. Ele mantém três cópias de todos os metadados de objetos em cada local.

2. **Retenção de objetos**
   - Várias cópias do objeto são armazenadas pelo StorageGRID. O número exato e o tipo de cópias e os locais de storage são determinados pelas regras em conformidade na política de ILM ativa.
3. **Exclusão de objeto**
   - Um objeto pode ser excluído quando sua data de retenção é alcançada.
   - Não é possível eliminar um objeto que esteja sob uma guarda legal.

Criando um bucket S3

Você pode usar o Gerenciador do locatário para criar buckets do S3 para dados de objetos. Ao criar um intervalo, você deve especificar o nome e a região do intervalo. Se a configuração global de bloqueio de objetos S3D estiver ativada para o sistema StorageGRID, você poderá ativar opcionalmente o bloqueio de objetos S3D para o bucket.

O que você vai precisar

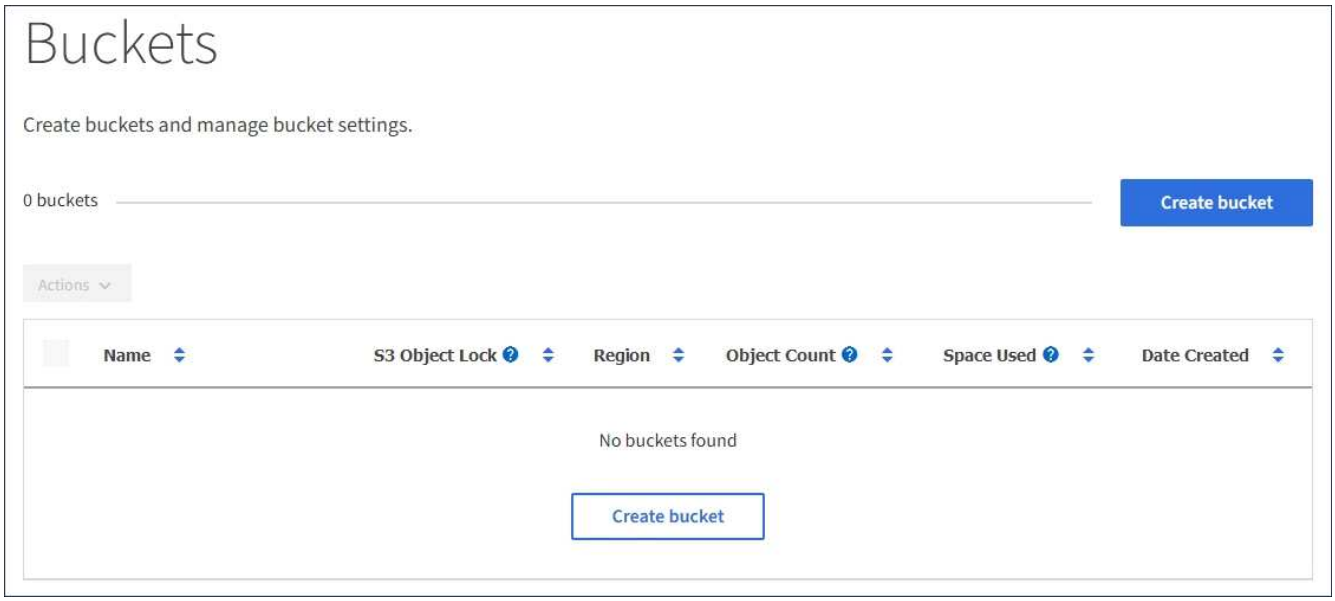
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Se você planeja criar um bucket com o bloqueio de objeto S3, a configuração global bloqueio de objeto S3 deve ter sido ativada para o sistema StorageGRID e você deve ter revisado os requisitos para buckets e objetos do bloqueio de objeto S3.

  "Usando S3 Object Lock"

Passos

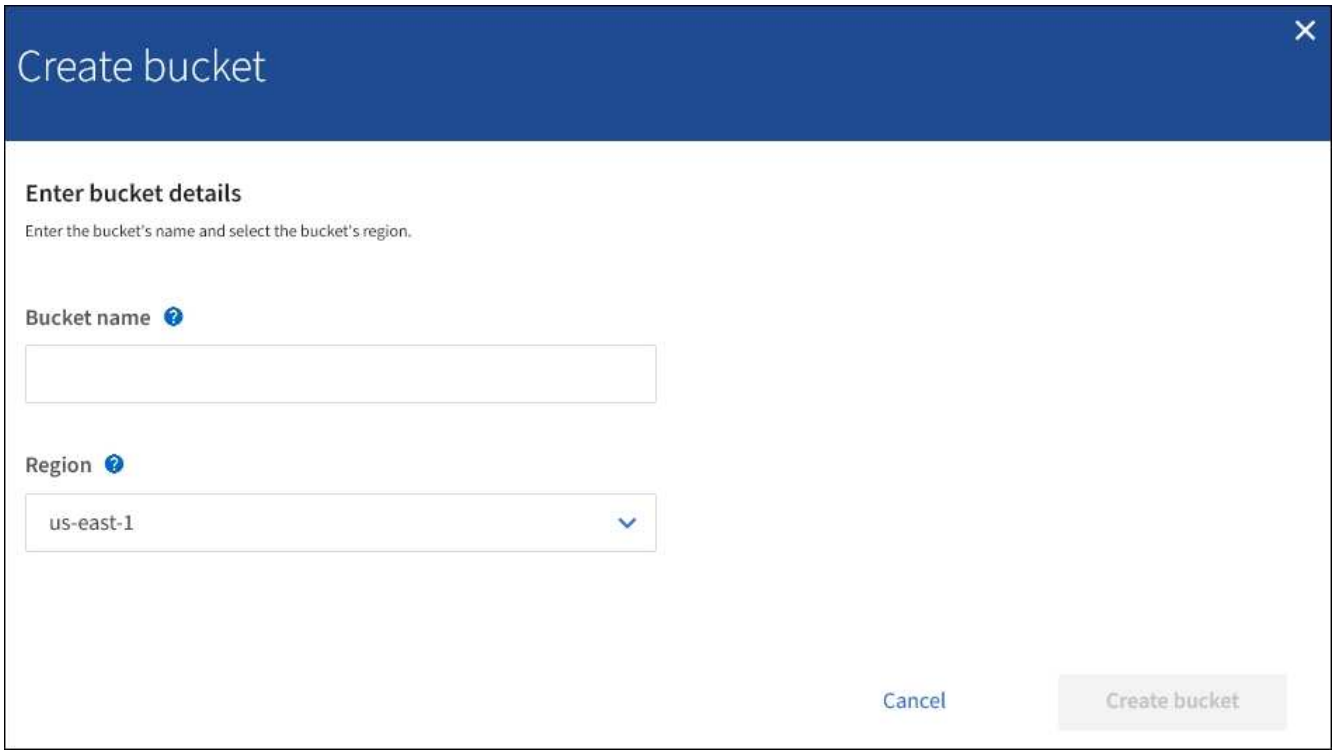
1. Selecione **STORAGE (S3)** > **Buckets**.

   A página Buckets é exibida e lista todos os buckets que já foram criados.



2. Selecione **criar bucket**.

   O assistente criar bucket é exibido.



> Se a configuração global S3 Object Lock estiver ativada, Create bucket inclui uma segunda etapa para gerenciar o S3 Object Lock para o bucket.

3. Introduza um nome exclusivo para o intervalo.

> Não é possível alterar o nome do bucket depois de criar o bucket.

   Os nomes dos buckets devem cumprir 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.
- 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.

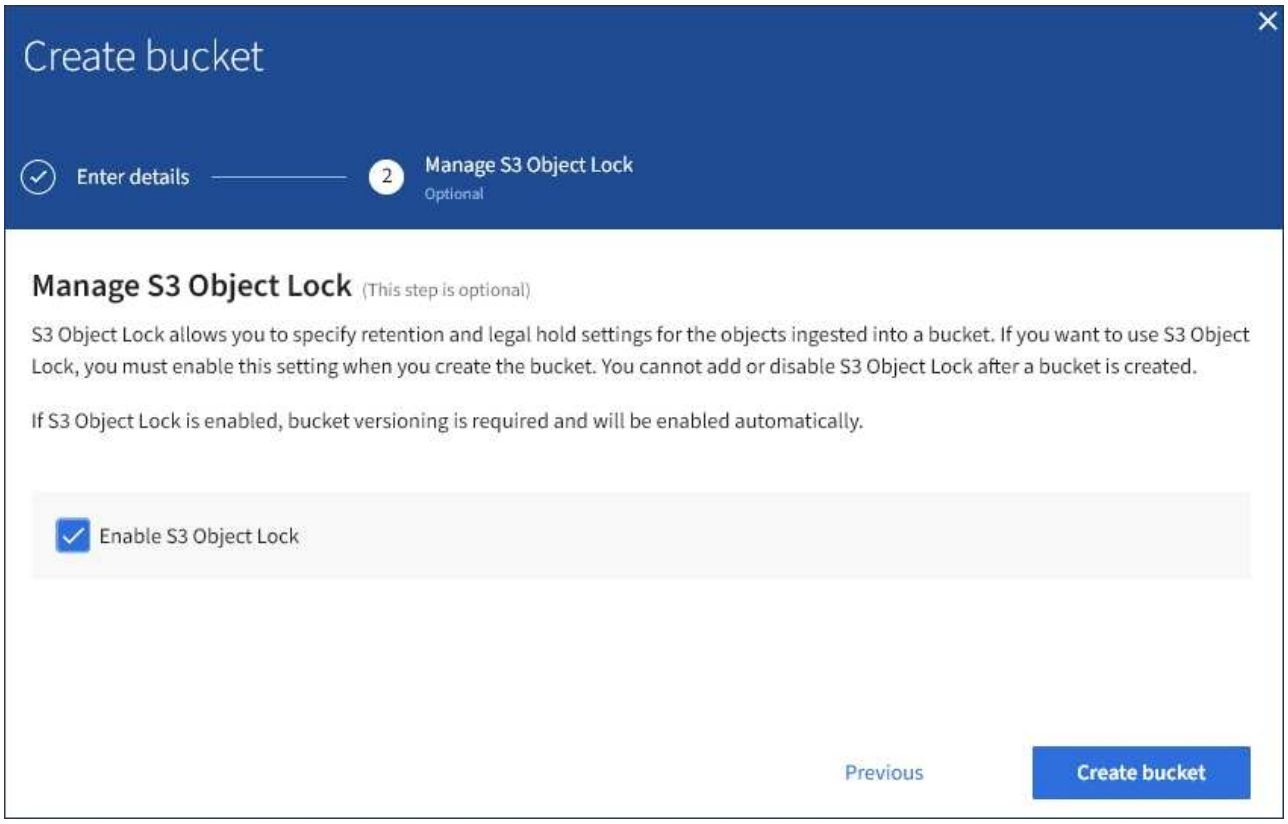
Consulte a documentação do Amazon Web Services (AWS) para obter mais informações.

4. Selecione a região para este intervalo.

   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.

   Não é possível alterar a região depois de criar o intervalo.

5. Selecione **criar bucket** ou **continuar**.
   - Se a configuração global S3 Object Lock não estiver ativada, selecione **Create bucket**. O bucket é criado e adicionado à tabela na página Buckets.
   - Se a configuração global S3 Object Lock estiver ativada, selecione **Continue**. O passo 2, Gerenciar bloqueio de objetos S3, aparece.



6. Opcionalmente, marque a caixa de seleção para ativar o bloqueio de objetos S3D para este bucket.

   O bloqueio de objetos S3 deve ser ativado para o bucket antes que um aplicativo cliente S3 possa especificar as configurações de retenção legal e de retenção para os objetos adicionados ao bucket.

   > Não é possível ativar ou desativar o bloqueio de objetos S3 depois de criar o bucket.

   > Se você ativar o bloqueio de objeto S3 para um bucket, o controle de versão do bucket será ativado automaticamente.

7. Selecione **criar bucket**.

   O bucket é criado e adicionado à tabela na página Buckets.

Informações relacionadas

"Gerenciar objetos com ILM"

"Entendendo a API de gerenciamento do locatário"

"Use S3"

Visualização dos detalhes do balde S3

Você pode exibir uma lista dos buckets e configurações do bucket em sua conta de locatário.

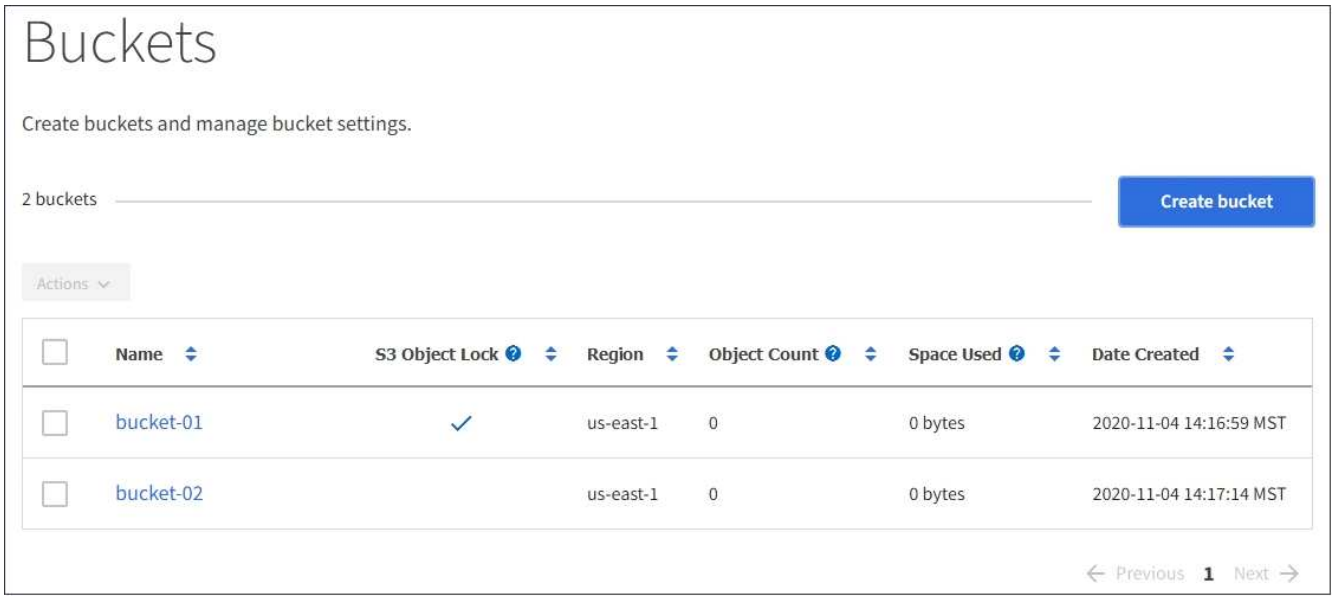
O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.

Passos

1. Selecione **STORAGE (S3)** > **Buckets**.

   A página Buckets é exibida e lista todos os buckets da conta de locatário.



2. Reveja as informações de cada balde.

   Conforme necessário, você pode classificar as informações por qualquer coluna, ou pode encaminhar e voltar a página através da lista.

   - Nome: O nome exclusivo do bucket, que não pode ser alterado.
   - S3 Object Lock: Se o S3 Object Lock está ativado para este bucket.

     Esta coluna não será exibida se a configuração global de bloqueio de objetos S3D estiver desativada. Esta coluna também mostra informações para quaisquer buckets em conformidade com o legado.

   - Região: A região do balde, que não pode ser alterada.
   - Contagem de objetos: O número de objetos neste intervalo.
   - Espaço usado: O tamanho lógico de todos os objetos neste intervalo. O tamanho lógico não inclui o espaço real necessário para cópias replicadas ou codificadas para apagamento ou metadados de objetos.
   - Data de criação: A data e a hora em que o intervalo foi criado.

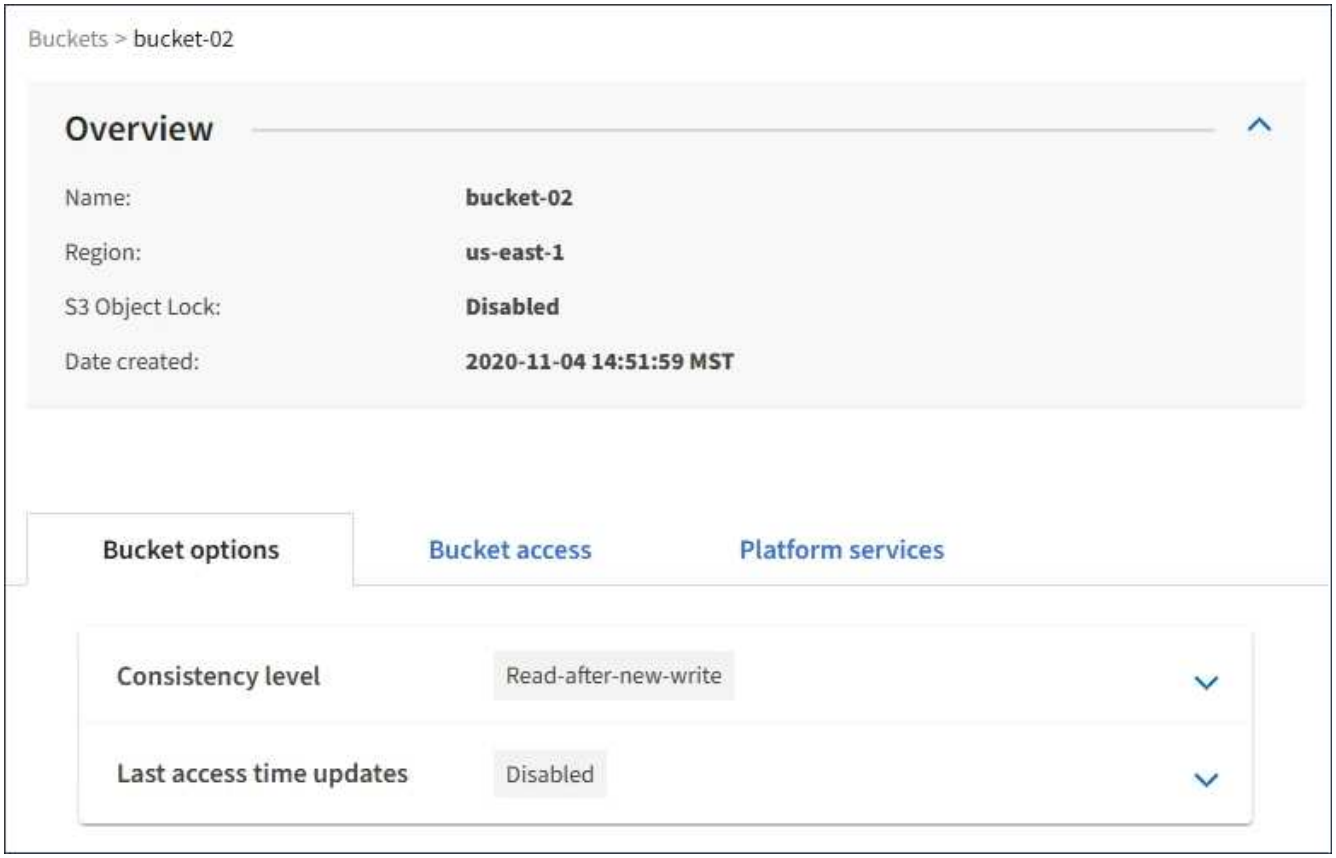
   > Os valores contagem de objetos e espaço utilizados apresentados são estimativas. Essas estimativas são afetadas pelo timing de inests, conetividade de rede e status de nó.

3. Para ver e gerir as definições de um intervalo, selecione o nome do intervalo.

   É apresentada a página de detalhes do balde.

   Esta página permite visualizar e editar as definições de opções de intervalo, acesso a intervalos e serviços de plataforma.

   Consulte as instruções para configurar cada configuração ou serviço de plataforma.



Informações relacionadas

"Alterar o nível de consistência"

"Ativar ou desativar as atualizações da última hora de acesso"

"Configurando o compartilhamento de recursos entre origens (CORS)"

"Configurando a replicação do CloudMirror"

"Configurando notificações de eventos"

"Configurando o serviço de integração de pesquisa"

Alterar o nível de consistência

Se você estiver usando um locatário do S3, poderá usar o Gerenciador do Locatário ou a API de Gerenciamento do Locatário para alterar o controle de consistência para operações executadas nos objetos nos buckets do S3.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Sobre esta tarefa

O nível de consistência faz uma troca entre a disponibilidade dos objetos e a consistência desses objetos em

diferentes nós e sites de storage. Em geral, você deve usar o nível de consistência **Read-after-novo-write** para seus buckets. Se o nível de consistência **Read-after-new-write** não atender aos requisitos do aplicativo cliente, você pode alterar o nível de consistência definindo o nível de consistência do bucket ou usando o `Consistency-Control` cabeçalho. O `Consistency-Control` colhedor substitui o nível de consistência do balde.

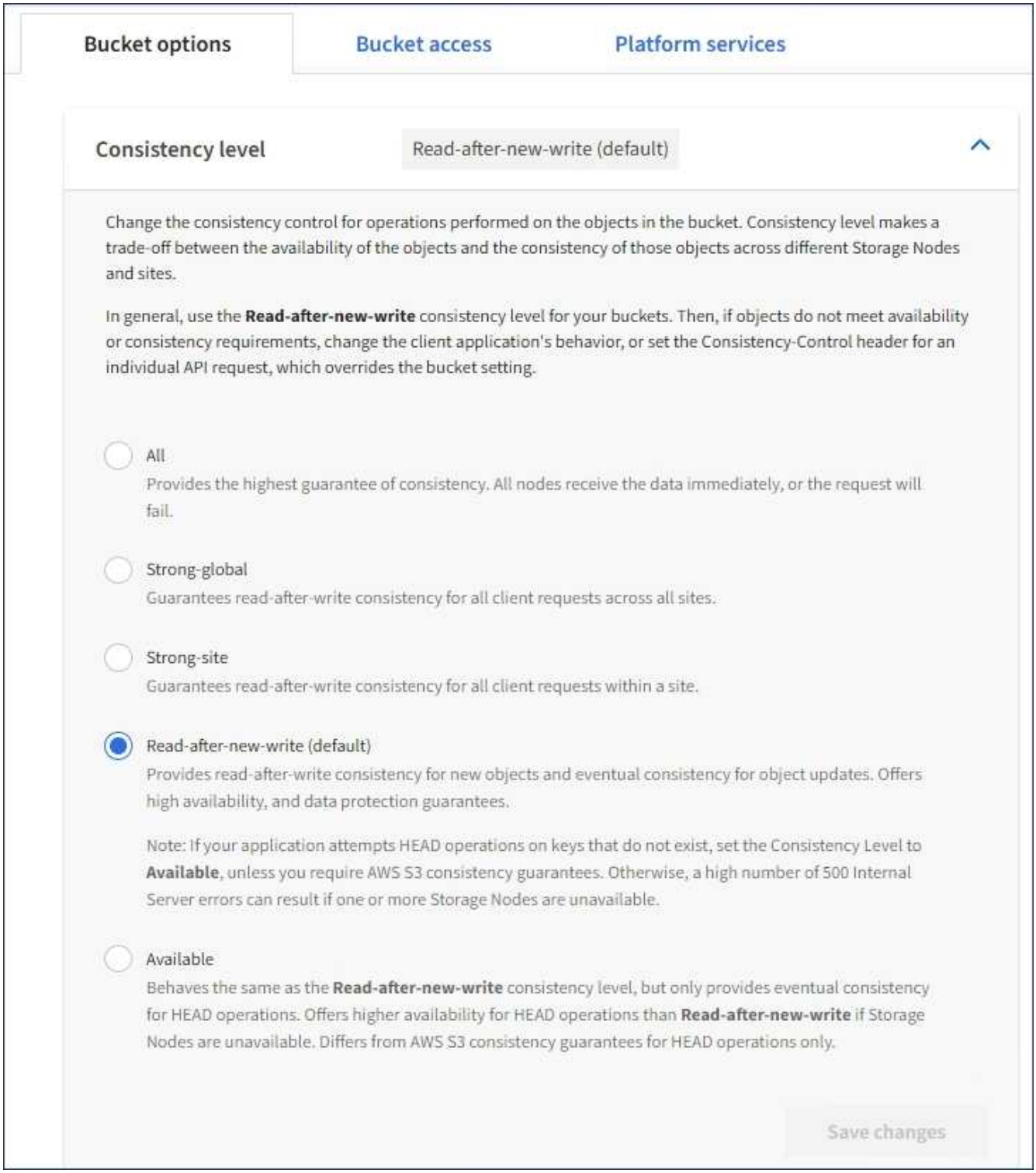
> Quando você altera o nível de consistência de um balde, apenas os objetos que são ingeridos após a alteração são garantidos para atender ao nível revisado.

Passos

1. Selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na lista.

   É apresentada a página de detalhes do balde.

3. Selecione **Opções de balde nível de consistência**.



4. Selecione um nível de consistência para as operações realizadas nos objetos neste intervalo.

Nível de 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.

Nível de consistência	Descrição
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 consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Corresponde às garantias de consistência do Amazon S3. **Observação:** se o aplicativo tentar operações DE CABEÇA em chaves que não existem, defina o nível de consistência como **disponível**, a menos que você exija garantias de consistência do Amazon S3. Caso contrário, um grande número de erros de servidor interno do 500 pode resultar se um ou mais nós de storage não estiverem disponíveis.
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência **Read-after-new-write**, mas fornece apenas consistência para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES PRINCIPAIS do que **leitura após nova gravação** se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

5. Selecione **Salvar alterações**.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Ativar ou desativar 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** nas instruções de colocação. Você pode ignorar essas instruções se o seu sistema StorageGRID não incluir essa regra.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

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.

> Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

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

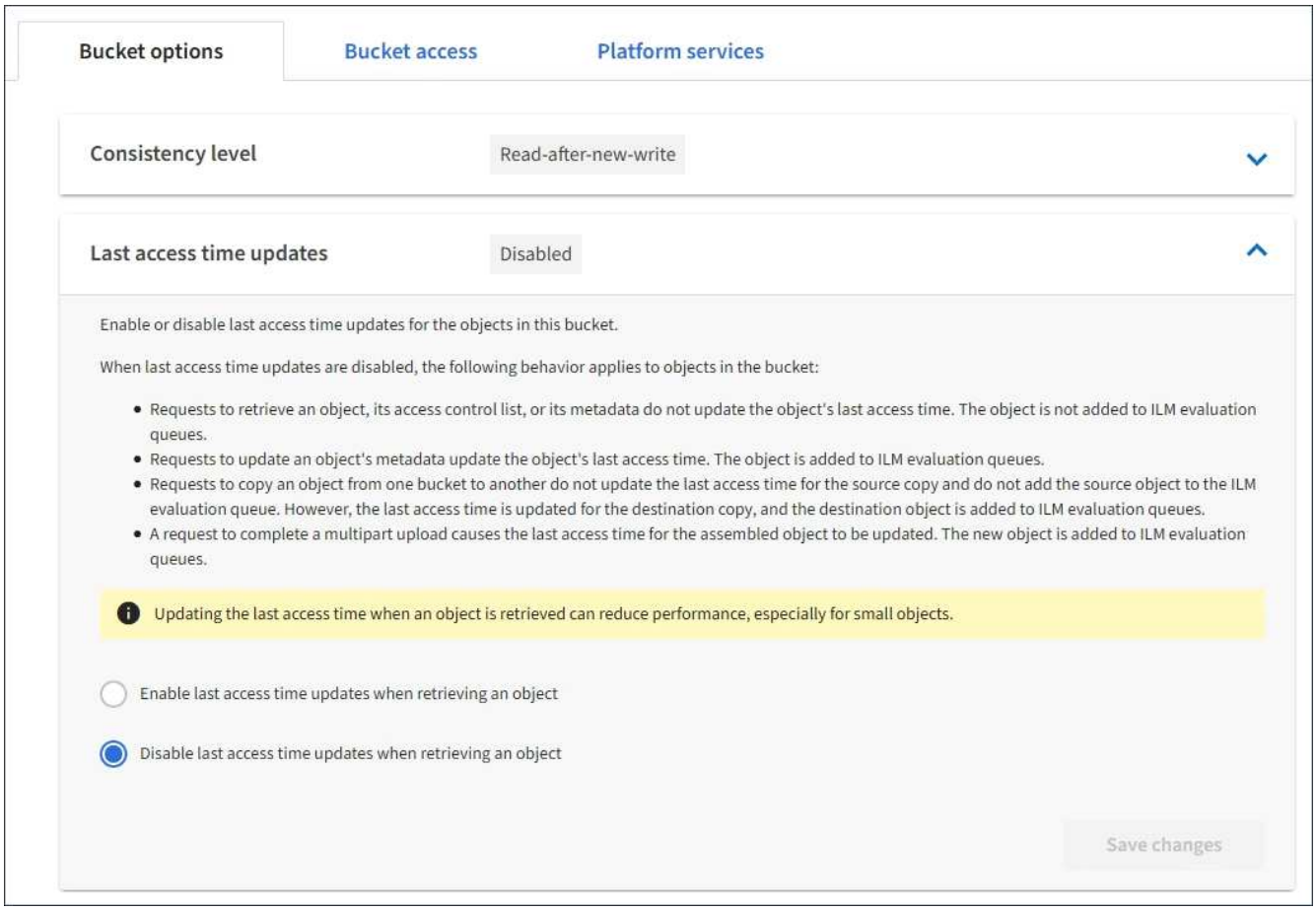
Solicitação para copiar um objeto de um bucket para outro	• Não, para a cópia de origem • Sim, para a cópia de destino	• Não, para a cópia de origem • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino
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 **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na lista.

   É apresentada a página de detalhes do balde.

3. Selecione **Opções de intervalo atualizações do último tempo de acesso**.
4. Selecione o botão de opção apropriado para ativar ou desativar as atualizações da última hora de acesso.



5. Selecione **Salvar alterações**.

Informações relacionadas

"Permissões de gerenciamento do locatário"

"Gerenciar objetos com ILM"

Configurando 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Sobre esta tarefa

O Compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos da Web de 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`.

Passos

1. Use um editor de texto para criar o XML necessário para ativar o CORS.

   Este exemplo mostra o XML usado para ativar o CORS para um bucket S3. Esse XML permite que qualquer domínio envie SOLICITAÇÕES GET para o bucket, mas só permite que o `http://www.example.com` domínio envie SOLICITAÇÕES POST e EXCLUA. Todos os cabeçalhos de solicitação são permitidos.

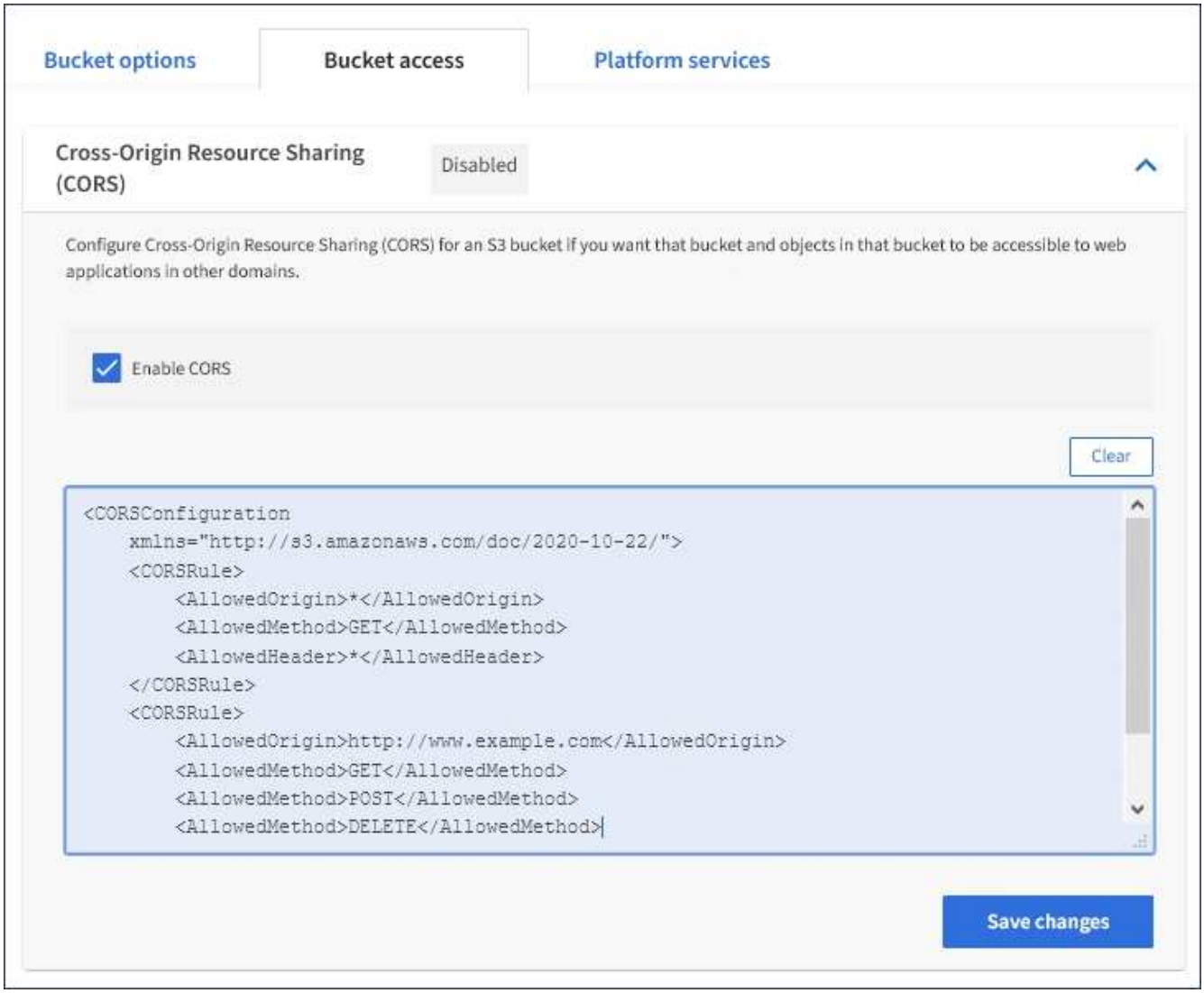
   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</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 desenvolvedor do Amazon Simple Storage Service" consulte .

2. No Gerenciador do Locatário, selecione **STORAGE (S3) Buckets**.
3. Selecione o nome do intervalo na lista.

É apresentada a página de detalhes do balde.

4. Selecione **Bucket Access Cross-Origin Resource Sharing (CORS)**.
5. Marque a caixa de seleção **Enable CORS** (Ativar VRF*).
6. Cole o XML de configuração do CORS na caixa de texto e selecione **Salvar alterações**.



7. Para modificar a configuração CORS para o bucket, atualize o XML de configuração do CORS na caixa de texto ou selecione **Limpar** para recomeçar. Em seguida, selecione **Salvar alterações**.
8. Para desativar o CORS para o bucket, desmarque a caixa de seleção **Ativar CORS** e selecione **Salvar alterações**.

Eliminar um bucket do S3

Você pode usar o Gerenciador do Locatário para excluir um bucket do S3 vazio.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Sobre esta tarefa

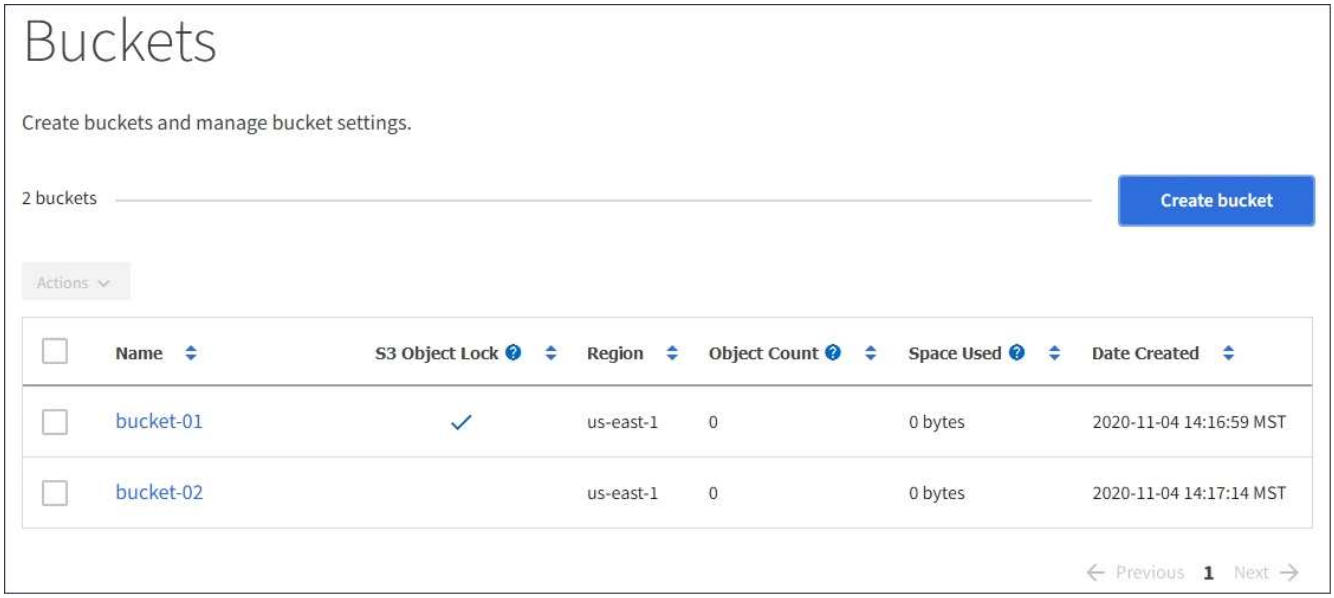
Estas instruções descrevem como excluir um bucket do S3 usando o Gerenciador do locatário. Você também pode excluir buckets do S3 usando a API de gerenciamento do locatário ou a API REST do S3.

Não é possível excluir um bucket do S3 se ele contiver objetos ou versões de objetos não atuais. Para obter informações sobre como objetos com versão S3 são excluídos, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Passos

1. Selecione **STORAGE (S3)** > **Buckets**.

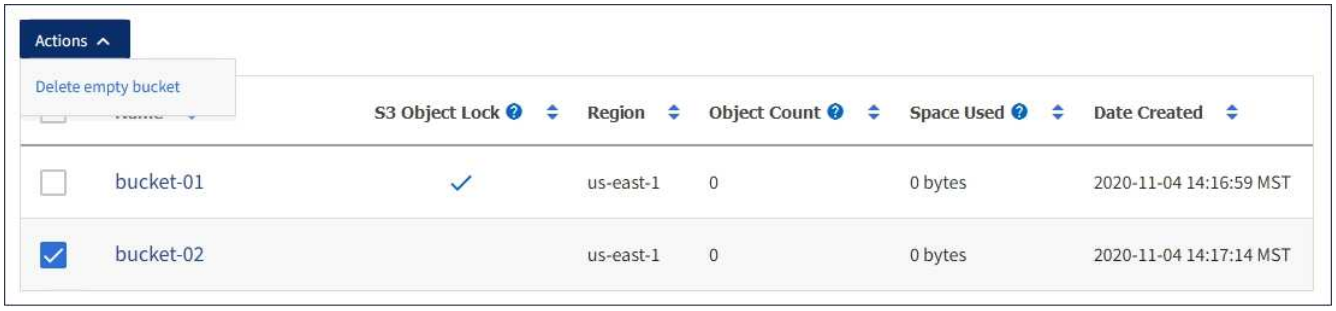
   A página baldes é exibida e mostra todos os baldes S3 existentes.



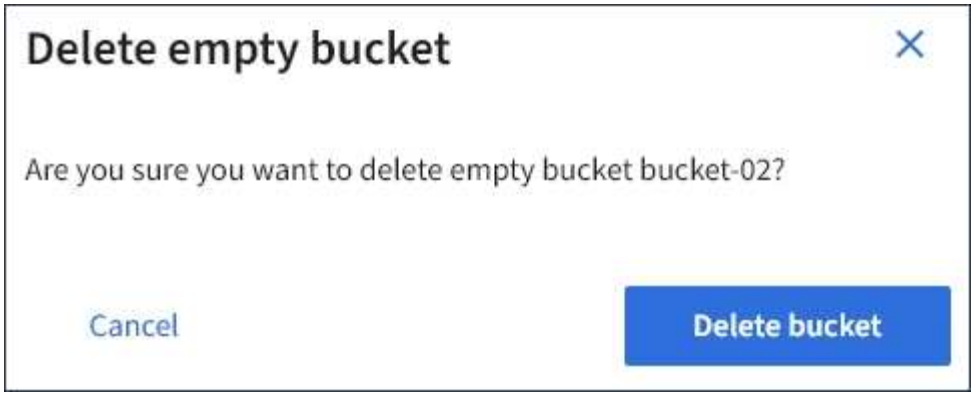
2. Marque a caixa de seleção do intervalo vazio que deseja excluir.

   O menu ações está ativado.

3. No menu ações, selecione **Excluir bucket vazio**.



   É apresentada uma mensagem de confirmação.



4. Se tiver certeza de que deseja excluir o intervalo, selecione **Excluir intervalo**.

   O StorageGRID confirma que o balde está vazio e, em seguida, elimina o balde. Esta operação pode demorar alguns minutos.

   Se o balde não estiver vazio, é apresentada uma mensagem de erro. Você deve excluir todos os objetos antes de excluir o bucket.

Informações relacionadas

"Gerenciar objetos com ILM"

Gerenciamento de serviços da plataforma S3

Se o uso de serviços de plataforma for permitido para sua conta de locatário do S3, você poderá usar os serviços de plataforma para aproveitar os serviços externos e configurar a replicação, notificações e integração de pesquisa do CloudMirror para buckets do S3.

- "Quais são os serviços de plataforma"
- "Considerações sobre o uso de serviços de plataforma"
- "Configurando endpoints de serviços de plataforma"
- "Configurando a replicação do CloudMirror"
- "Configurando notificações de eventos"
- "Usando o serviço de integração de pesquisa"

Quais são os serviços de plataforma

Os serviços de plataforma da StorageGRID podem ajudar você a implementar uma estratégia de nuvem híbrida.

Se o uso de serviços de plataforma for permitido para sua conta de locatário, você poderá configurar os seguintes serviços para qualquer bucket do S3:

- **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 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 Amazon Simple Notification Service (SNS) externo especificado.

  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 objetos 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.

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 as notificações em um bucket do StorageGRID S3 para que você possa espelhar objetos específicos para o Amazon Simple Storage Service, 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 Gerenciador do locatário ou a 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 serviço de notificação simples

(SNS) ou um cluster do Elasticsearch hospedado localmente, na AWS ou em outro lugar.

Depois de criar um endpoint, 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:

1. 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.
2. Se você também quiser enviar notificações quando esses objetos estiverem armazenados no bucket, adicione uma configuração de notificações.
3. Finalmente, 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
Replicação do CloudMirror	• OBTER replicação do bucket • COLOQUE a replicação do balde
Notificações	• OBTER notificação Bucket • COLOCAR notificação de balde
Integração de pesquisa	• OBTER configuração de notificação de metadados do bucket • COLOQUE a configuração de notificação de metadados do bucket Essas operações são personalizadas para o StorageGRID.

Consulte as instruções para implementar aplicativos cliente S3 para obter detalhes sobre como o StorageGRID implementa essas APIs.

Informações relacionadas

"Use S3"

"Entendendo o serviço de replicação do CloudMirror"

"Entendendo as notificações para buckets"

"Compreender o serviço de integração de pesquisa"

"Considerações sobre o uso de serviços de plataforma"

Entendendo 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.

A replicação do CloudMirror opera independentemente da política de ILM ativa 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.

Se você habilitar a replicação do CloudMirror para um bucket existente, somente os novos objetos adicionados a esse bucket serão 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 AWS 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.

No StorageGRID, é possível replicar os objetos em um único bucket em vários buckets do destino. Para fazer isso, especifique o destino para cada regra no XML de configuração de replicação. Você não pode replicar um objeto para mais de um bucket ao mesmo tempo.

Além disso, você pode configurar a replicação do CloudMirror em buckets com controle de versão ou não versionados e especificar um bucket com controle de versão ou não versionado como destino. 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.

O comportamento de exclusão para o serviço de replicação do CloudMirror é o mesmo que o comportamento de exclusão do serviço CRR (Cross Region Replication) fornecido pelo Amazon S3 — excluir 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 nem exclui o objeto de destino.

À medida que os objetos são replicados para o bucket de destino, o StorageGRID os marca como "replicas". 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.

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.

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.

Informações relacionadas

"Configurando a replicação do CloudMirror"

Entendendo 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 SNS (Serviço de notificação simples) do Amazon de destino.

Você pode configurar 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 SNS de destino especificado como a URNA de um endpoint.

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.

Notificações e mensagens suportadas

A notificação de eventos do StorageGRID segue a API do Amazon S3 com as seguintes limitações:

- 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 tabela:

Nome da chave	Valor StorageGRID
EventSource	`sgws:s3`
AwsRegion	não incluído
x-amz-id-2	não incluído
arn	`urn:sgws:s3:::bucket_name`

Informações relacionadas

"Configurando notificações de eventos"

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 objetos S3 para um endpoint de destino sempre que um objeto ou seus metadados 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.

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 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.

As notificações são geradas e enfileiradas 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.

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 a *Interoperability Matrix Tool* para determinar as versões suportadas do Elasticsearch.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Configuração XML para integração de pesquisa"

"Metadados de objetos incluídos nas notificações de metadados"

"JSON gerado pelo serviço de integração de pesquisa"

"Configurando o serviço de integração de pesquisa"

Considerações sobre o uso de serviços de plataforma

Antes de implementar os serviços da plataforma, revise as recomendações e considerações sobre o uso desses serviços.

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.
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.

Consideração	Detalhes
Exclusões de objetos orientadas por ILM	Para corresponder ao comportamento de exclusão dos serviços AWS CRR e SNS, 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.

Considerações para usar o serviço de replicação do CloudMirror

Consideração	Detalhes
Estado da replicação	O StorageGRID não suporta o `x-amz-replication-status` colhedor.
Tamanho do objeto	O tamanho máximo para objetos que podem ser replicados para um bucket de destino pelo serviço de replicação do CloudMirror é de 5 TB, o que é o mesmo que o tamanho máximo de objeto suportado pelo StorageGRID.
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 de marcação PUT Object ou EXCLUI solicitações de marcação de objetos que forneçam um 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 de marcação DE objetos ou EXCLUI solicitações de marcação de objetos 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	Se o intervalo S3 de destino para replicação do CloudMirror tiver o bloqueio de objetos S3 ativado, a operação de replicação falhará com um erro AccessDenied.

Informações relacionadas

"Use S3"

Configurando 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 a permissão Gerenciar endpoints ou acesso root, em uma grade cuja rede foi configurada para permitir que os nós de armazenamento acessem recursos de endpoint externos. Contacte o administrador do StorageGRID para obter mais informações.

O que é um endpoint de serviços de plataforma

Ao criar um endpoint de serviços de plataforma, você 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 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 AWS.

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 um destino, o que permite que você faça coisas como enviar notificações sobre a criação de objetos para um tópico do SNS e notificações sobre a exclusão de objetos para um segundo tópico do 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 oferece suporte a pontos de extremidade do Serviço de notificação simples (SNS). Os endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.

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. Não é necessário 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"

Especificando a URNA para um 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 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 AWS, use `arn:aws`o .
- 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
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	nome do balde
Notificações	sns-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

Para entidades da AWS, 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:

```
urn:mysite:sns:optional:optional:sns-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.

Criando um endpoint de serviços de plataforma

Você deve criar pelo menos um endpoint do tipo correto antes de habilitar um serviço de plataforma.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar Endpoints.
- O recurso referenciado pelo endpoint de serviços da plataforma deve ter sido criado:
  - Replicação do CloudMirror: Bucket do S3
  - Notificação de evento: Tópico SNS
  - Notificação de pesquisa: Índice Elasticsearch, se o cluster de destino não estiver configurado para criar índices automaticamente.
- Você deve ter 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)

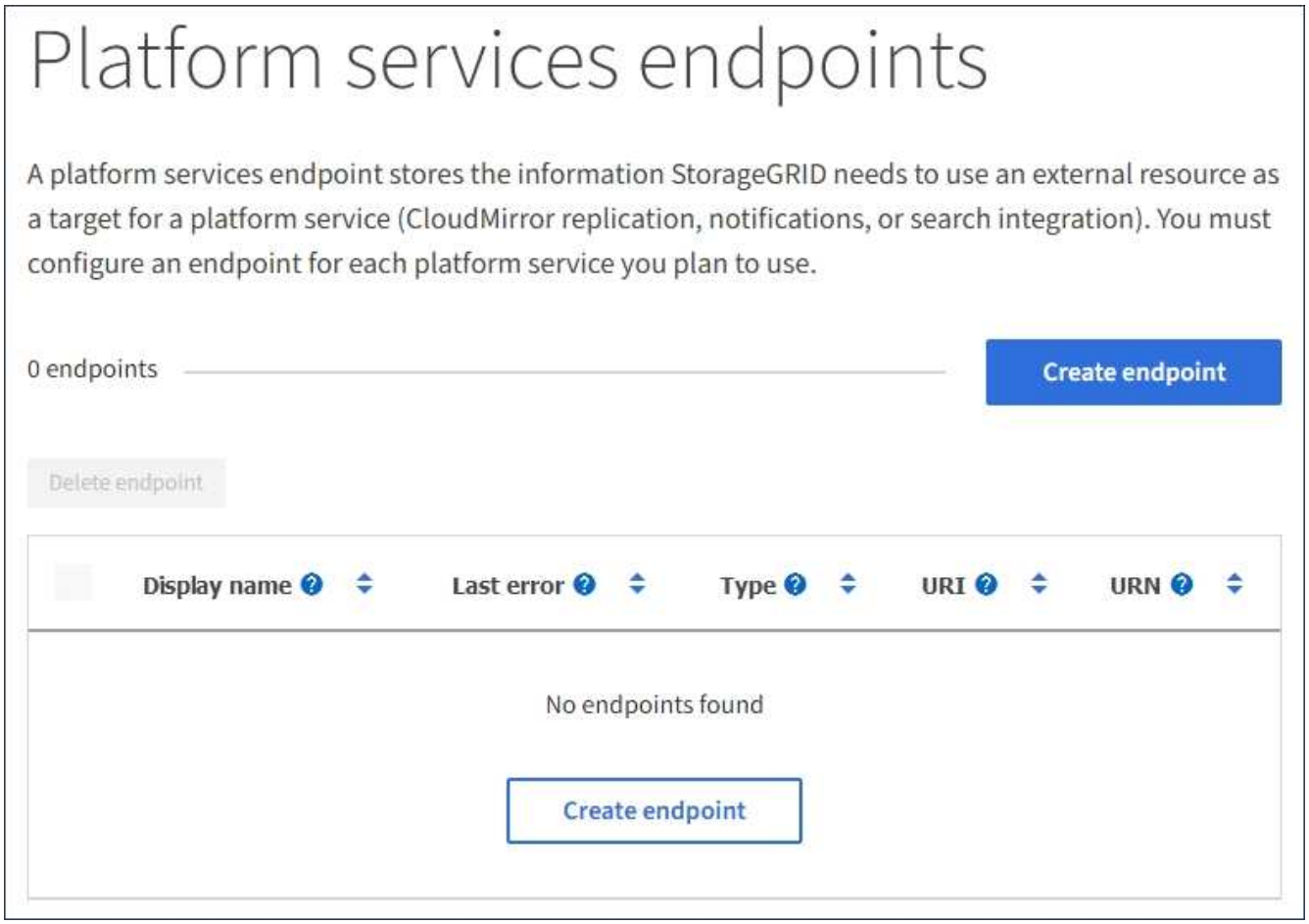
    "Especificando a URNA para um endpoint de serviços de plataforma"

  - Credenciais de autenticação (se necessário):
    - Chave de acesso: ID da chave de acesso e chave de acesso secreta
    - HTTP básico: Nome de usuário e senha
  - Certificado de segurança (se estiver usando um certificado de CA personalizado)

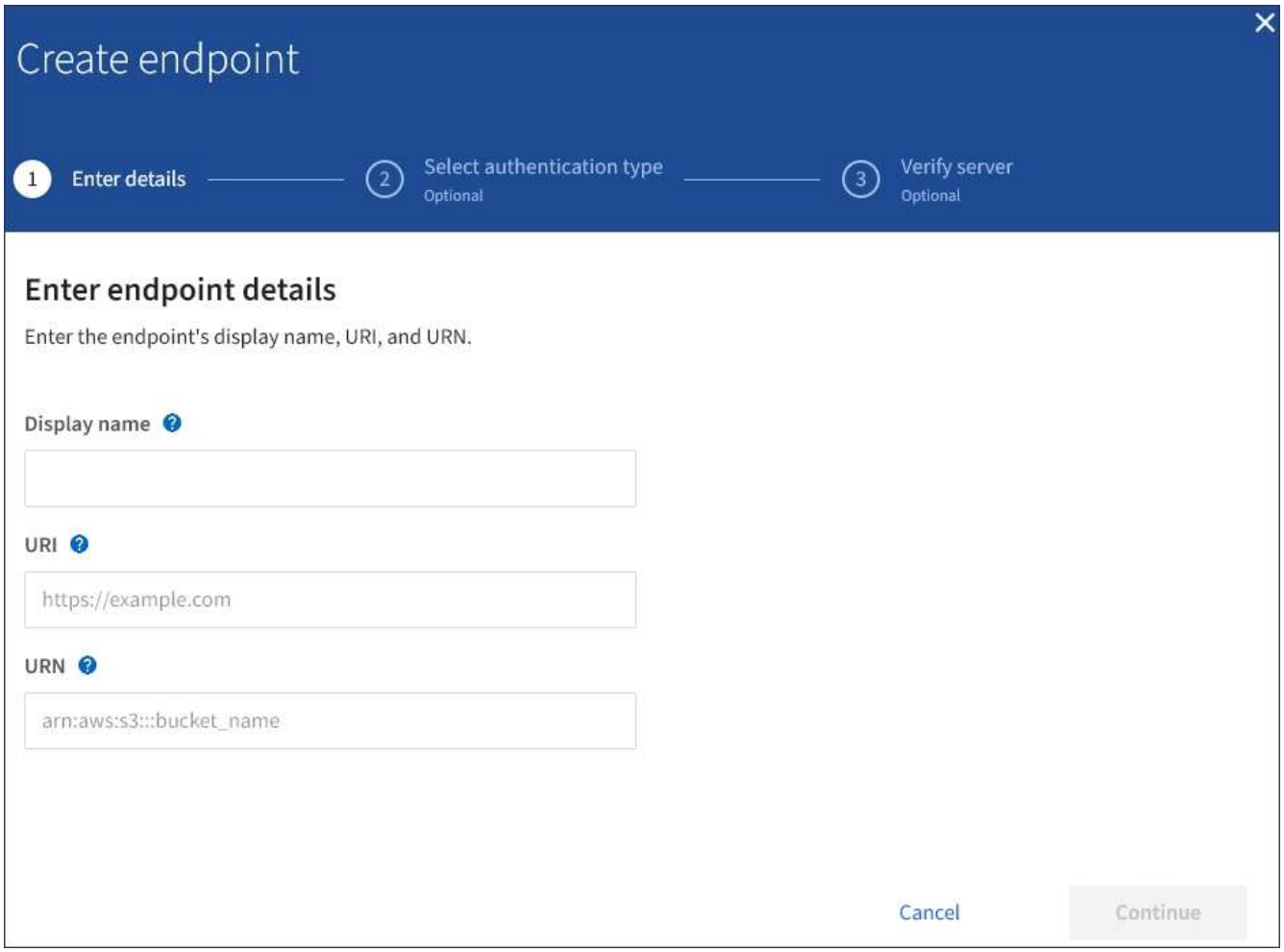
Passos

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, portanto, você não precisa 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, a porta 443 será usada para URIs HTTPS e a porta 80 será usada para URIs HTTP.

   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:

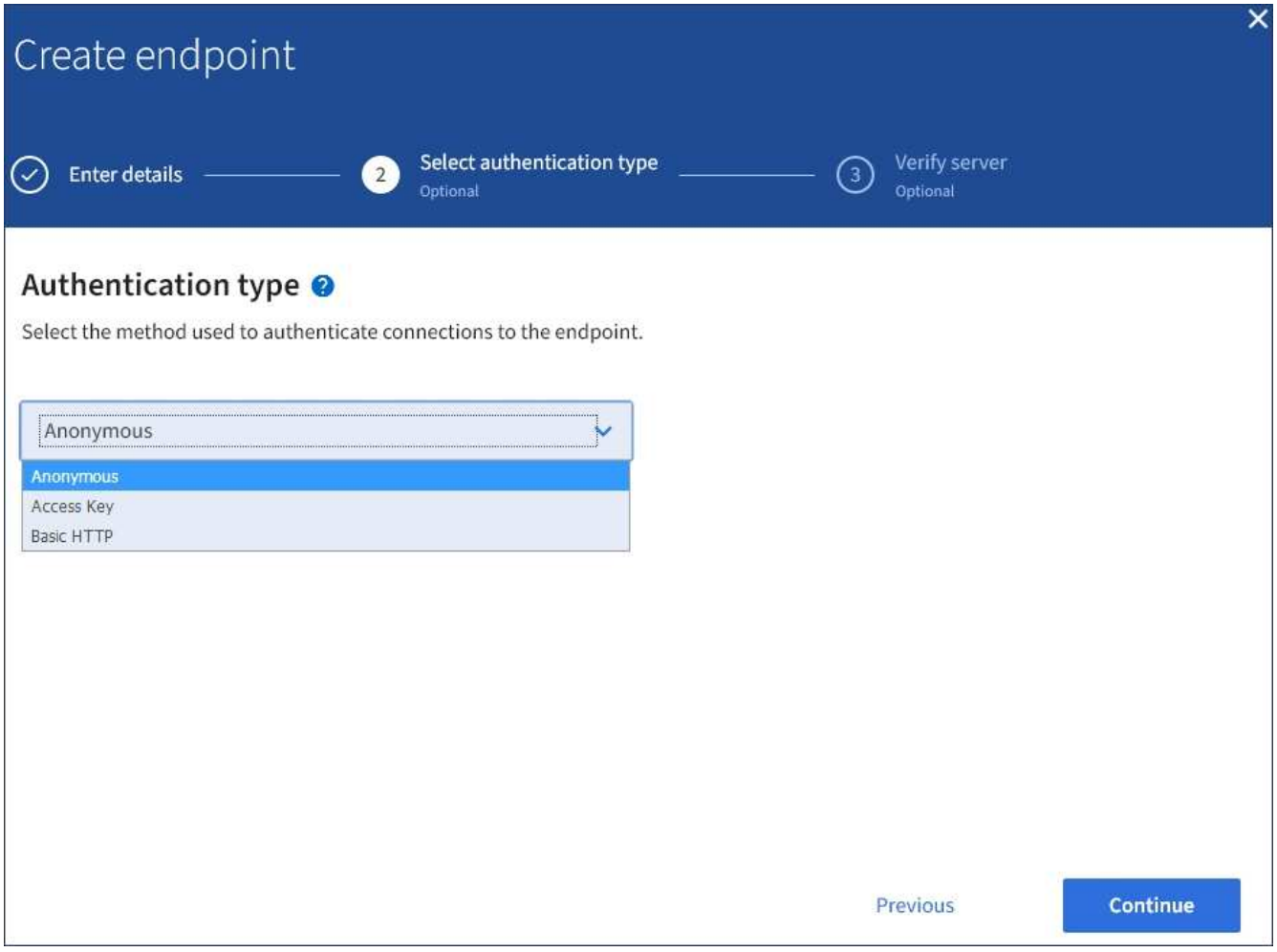
```
https://s3-aws-region.amazonaws.com
```

> 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.

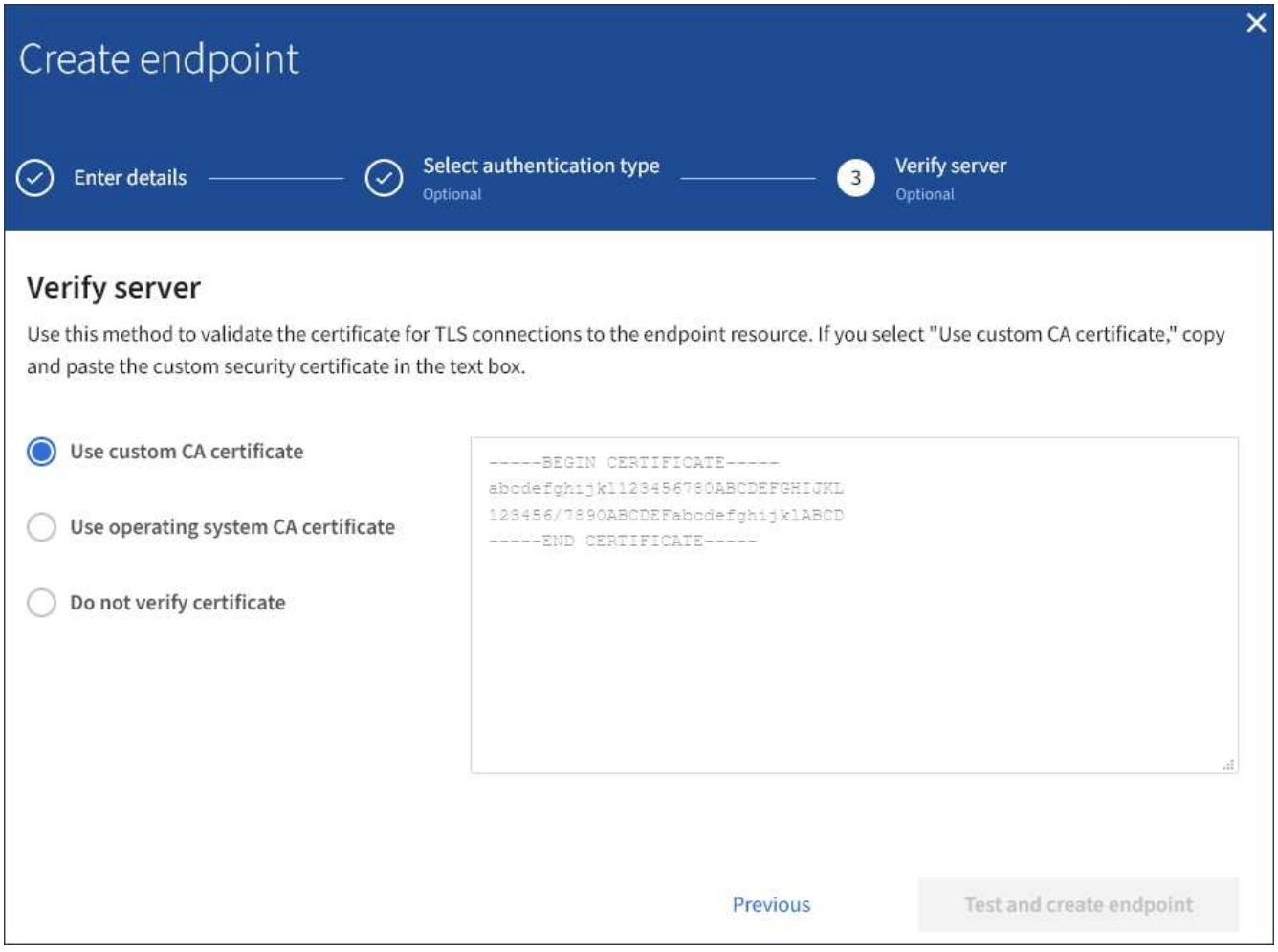
6. Selecione **continuar**.
7. Selecione um valor para **tipo de autenticação** e insira as credenciais necessárias.



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

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 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

"Especificando a URNA para um endpoint de serviços de plataforma"

"Configurando a replicação do CloudMirror"

"Configurando notificações de eventos"

"Configurando o serviço de integração de pesquisa"

Testando a conexão para um 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar Endpoints.

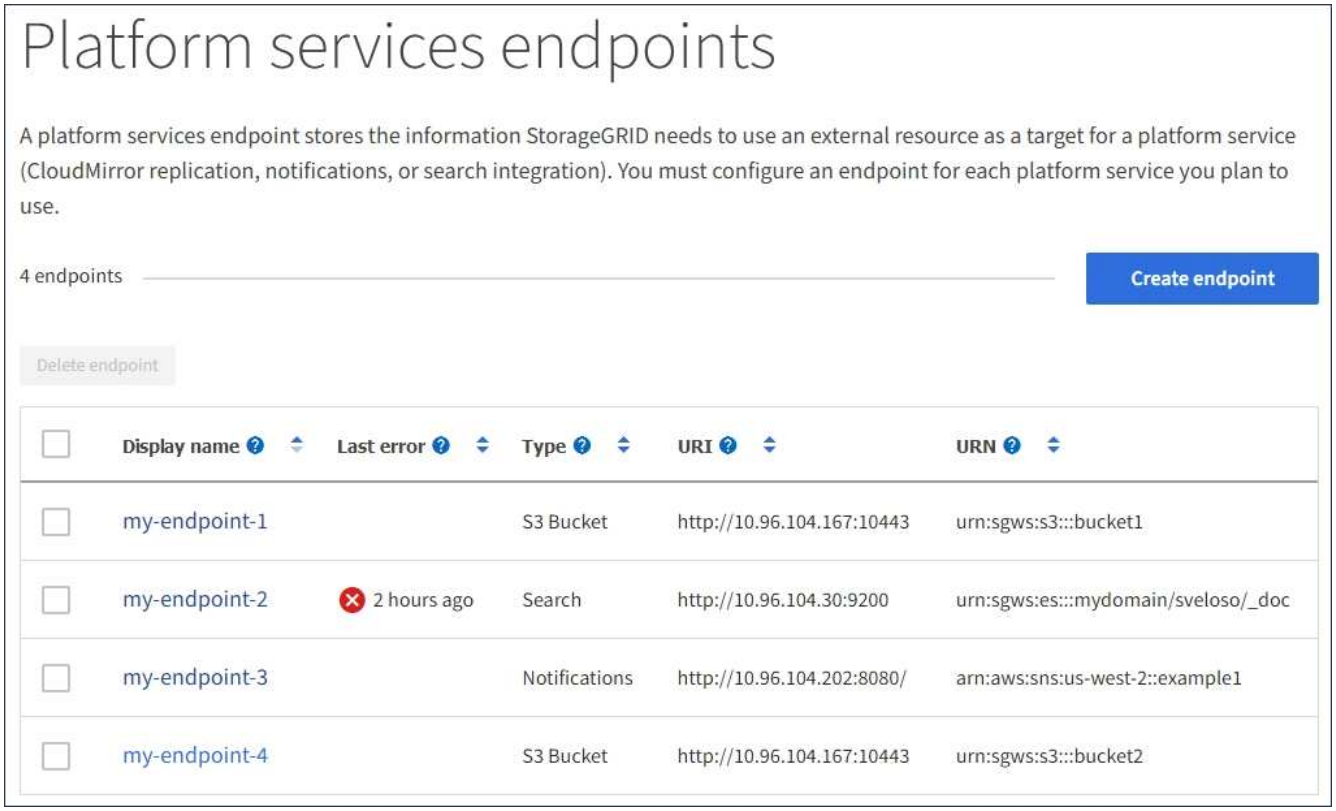
Sobre esta tarefa

O StorageGRID não valida se as credenciais têm as permissões corretas.

Passos

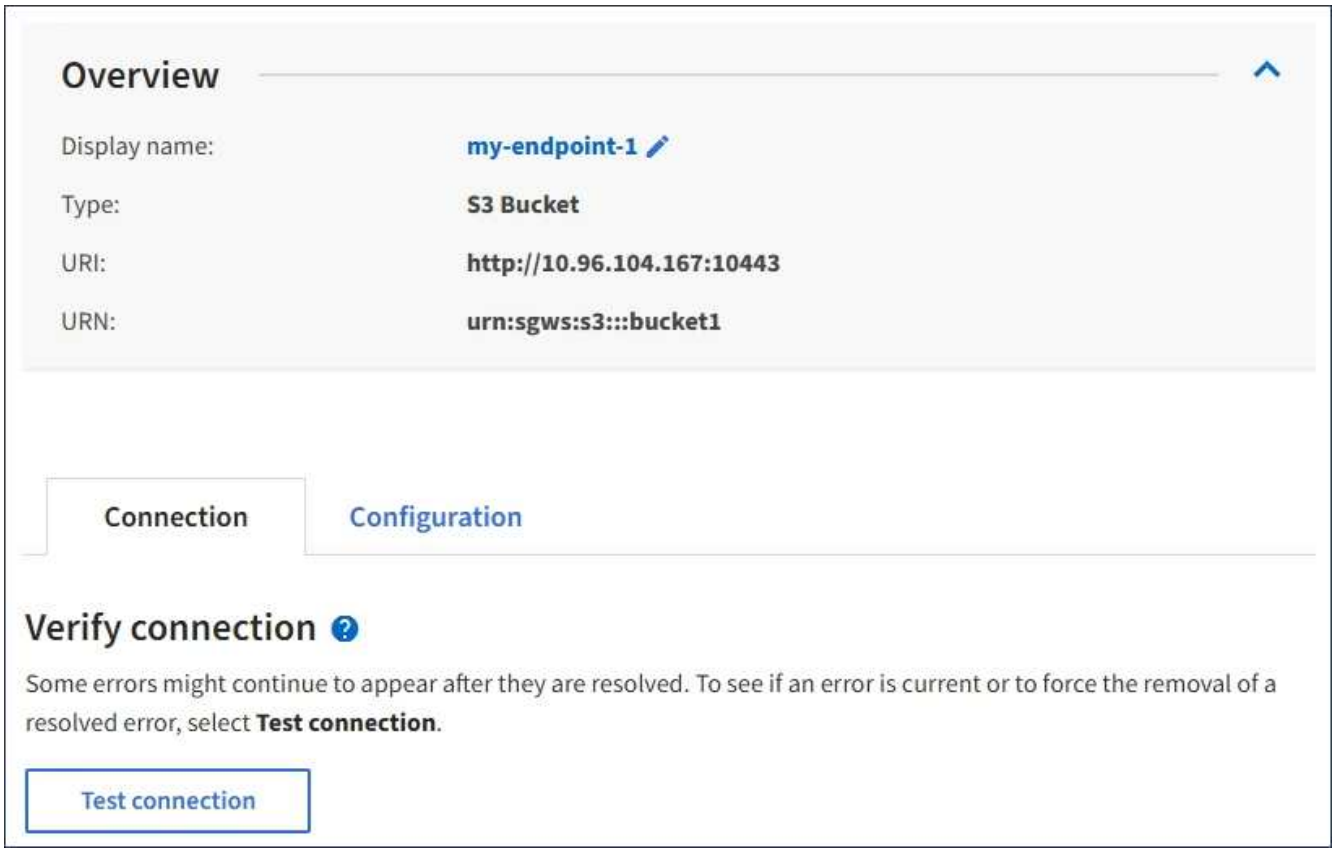
1. Selecione **STORAGE (S3) endpoints de serviços de plataforma**.

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**.

Edição de um 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. Você não pode alterar a URN para um endpoint de serviços de plataforma.

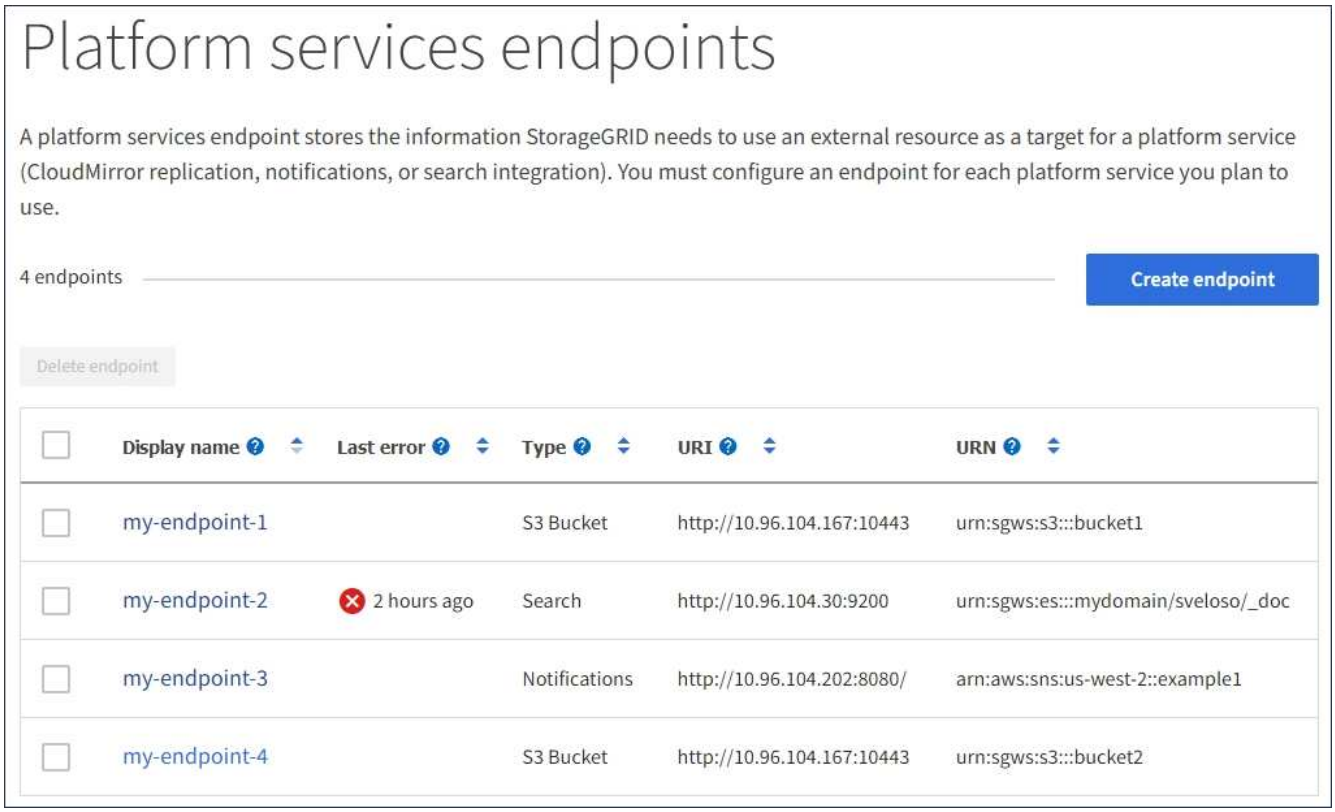
O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar Endpoints.

Passos

1. Selecione **STORAGE (S3) endpoints de serviços de plataforma**.

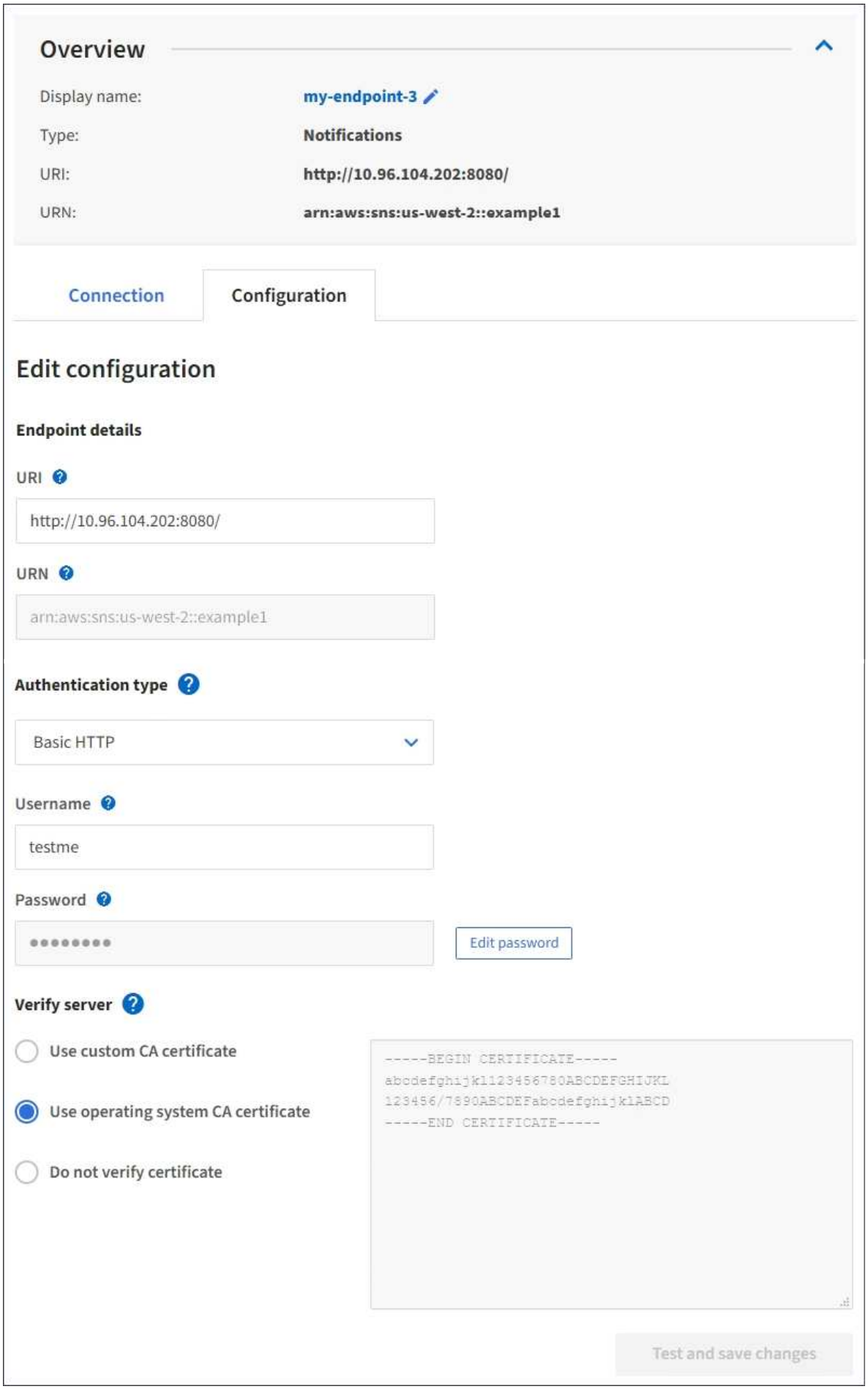
   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.



2. Selecione o ponto de extremidade que pretende editar.

   A página de detalhes do ponto final é exibida.

3. Selecione **Configuração**.


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

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 HTTP básica, altere o nome de usuário conforme necessário. Altere a senha conforme necessário selecionando **Editar senha** e inserindo a nova senha. Se você precisar cancelar suas alterações, selecione **Revert password edit**.
      - 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**.
   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**.

Informações relacionadas

"Criando um endpoint de serviços de plataforma"

Excluindo um endpoint de serviços de plataforma

Você pode excluir um endpoint se não quiser mais usar o serviço de plataforma associado.

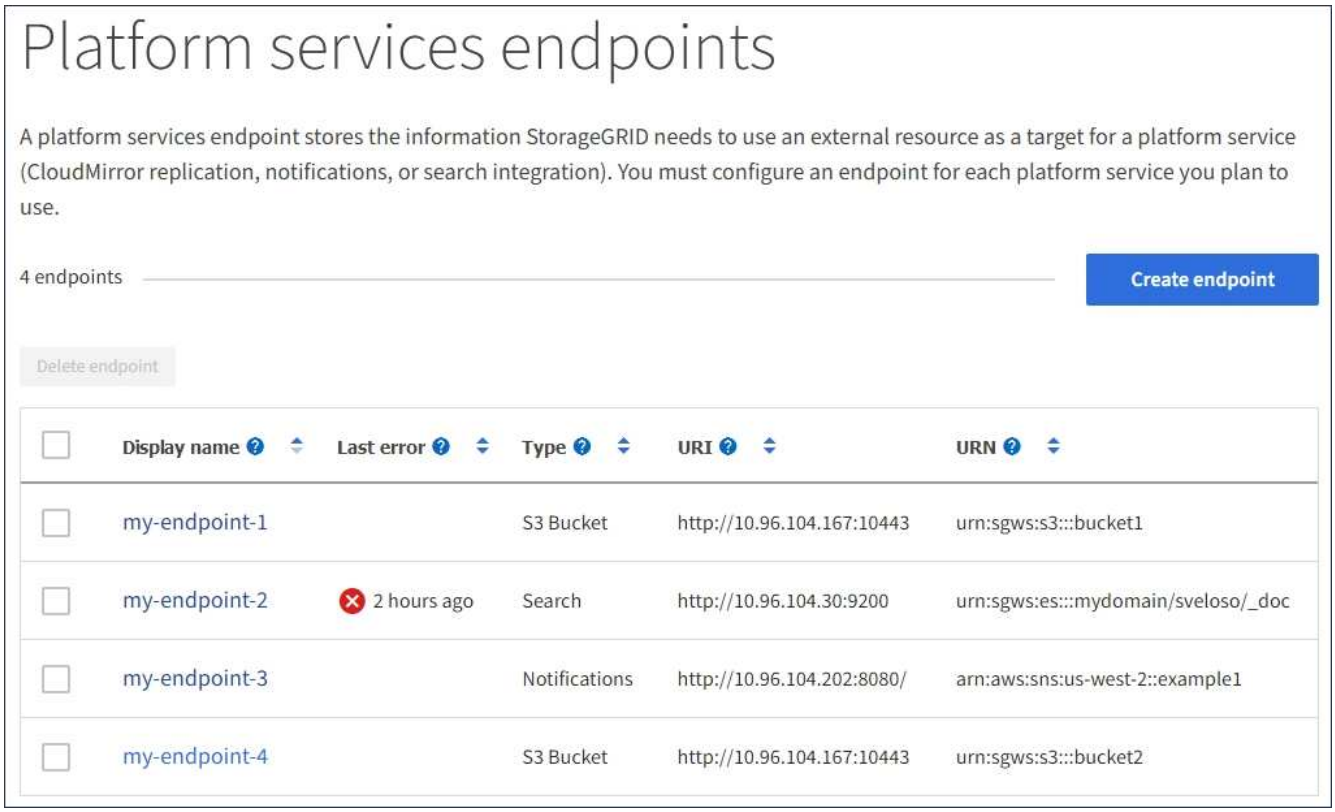
O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão **Manage Endpoints**.

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.

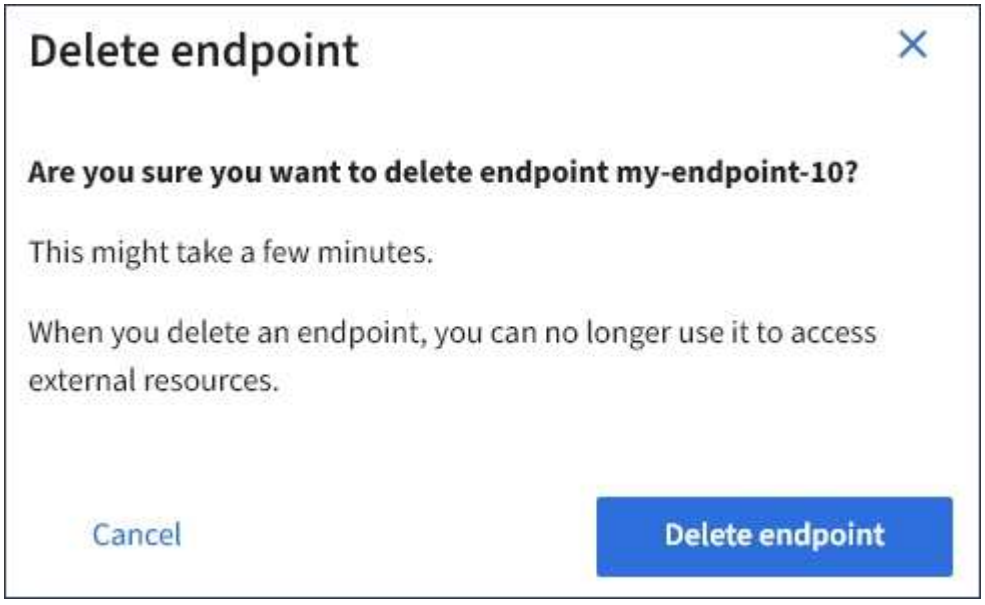


2. Marque a caixa de seleção para cada ponto de extremidade que deseja excluir.

> 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.



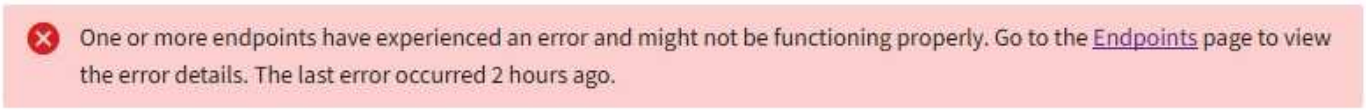
4. Selecione **Excluir endpoint**.

Solução de problemas de erros de endpoint de serviços de plataforma

Se ocorrer um erro quando o StorageGRID tenta se comunicar com um endpoint de serviços de plataforma, uma mensagem é exibida no Dashboard. 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.

Determinar se ocorreu um erro

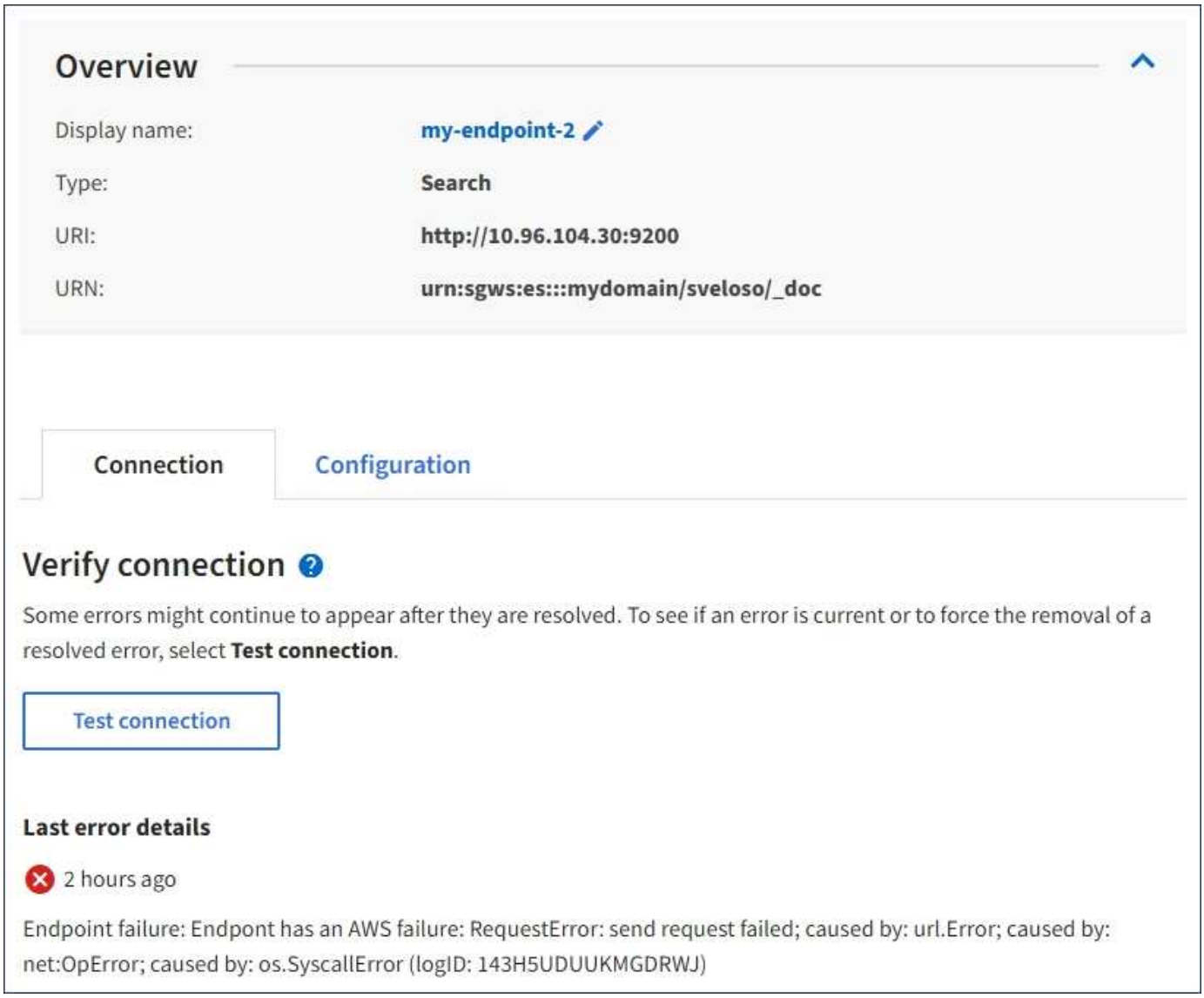
Se algum erro de endpoint de serviços de plataforma tiver ocorrido nos últimos 7 dias, o Painel do Gerenciador do Locatário exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.



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.



Verificar se um 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.

Resolução de 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 do endpoint ou o acesso ao 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.

Solução de problemas de serviços de plataforma adicionais

Para obter informações adicionais sobre os serviços de plataforma de solução de problemas, consulte as instruções de administração do StorageGRID.

"Administrar o StorageGRID"

Informações relacionadas

"Criando um endpoint de serviços de plataforma"

"Testando a conexão para um endpoint de serviços de plataforma"

"Edição de um endpoint de serviços de plataforma"

Configurando a replicação do CloudMirror

O serviço de replicação do CloudMirror é um dos três serviços de plataforma StorageGRID. Você pode usar a replicação do CloudMirror para replicar automaticamente objetos para um bucket externo do S3.

O que você vai precisar

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado um bucket para agir como a origem da replicação.
- O endpoint que você pretende usar como destino para a replicação do CloudMirror já deve existir, e você deve ter sua URN.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário.

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 ativar a replicação do CloudMirror para um bucket, você deve criar e aplicar XML de configuração de replicação de bucket válida. O XML de configuração de replicação deve usar a URN de um endpoint de bucket do S3 para cada destino.

> A replicação não é suportada para buckets de origem ou destino com o bloqueio de objetos S3 ativado.

Para obter informações gerais sobre replicação de bucket e como configurá-la, consulte a documentação da Amazon sobre replicação entre regiões (CRR). Para obter informações sobre como o StorageGRID implementa a API de configuração de replicação de bucket S3, consulte as instruções para implementar aplicativos cliente S3.

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. 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:

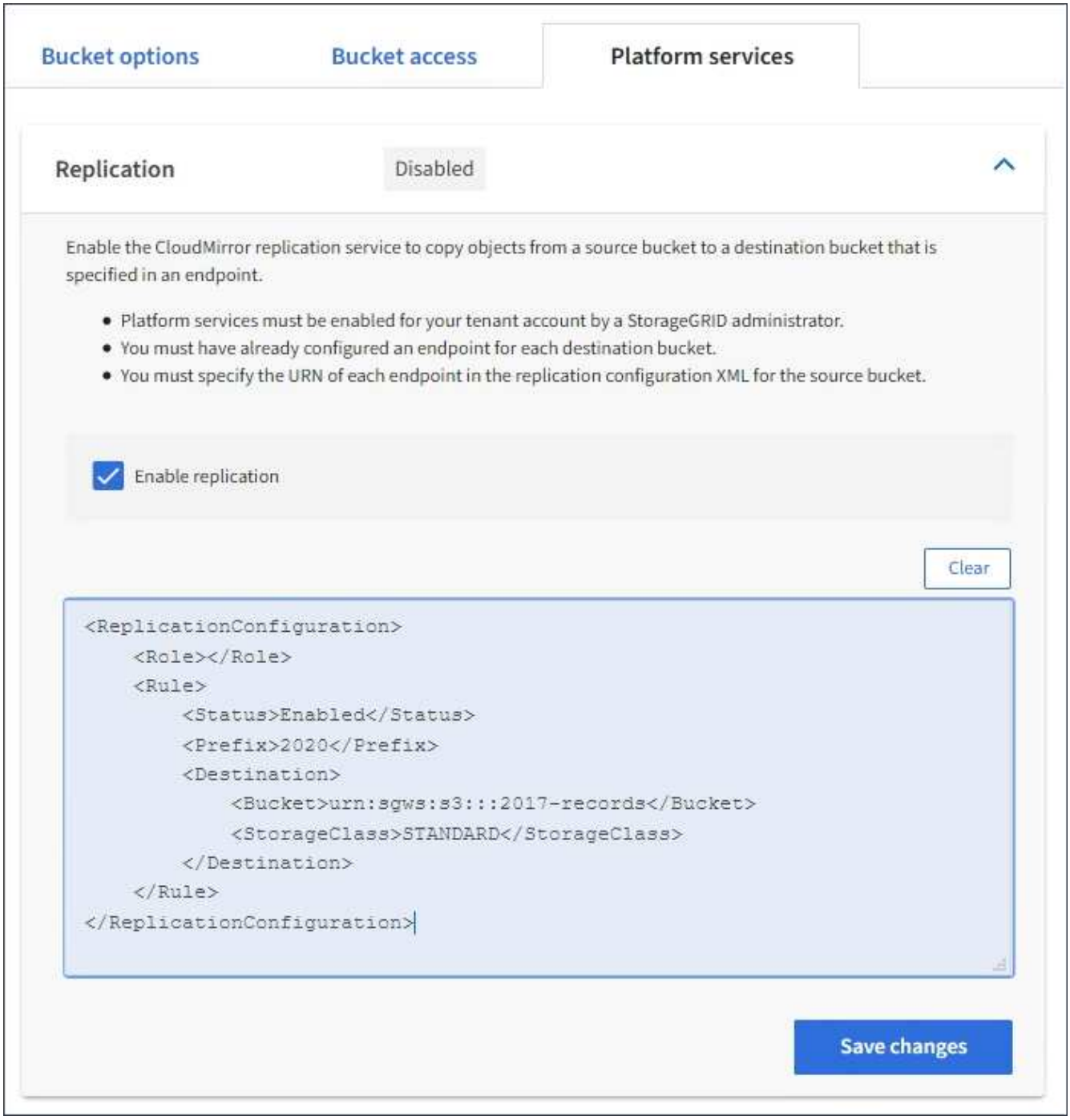
   - Observe que o StorageGRID só suporta V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue convenções V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
   - 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. 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 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

"Entendendo o serviço de replicação do CloudMirror"

"Use S3"

"Criando um endpoint de serviços de plataforma"

Configurando notificações de eventos

O serviço de notificações é um dos três serviços da plataforma StorageGRID. Você pode habilitar notificações de um bucket para enviar informações sobre eventos especificados para um serviço de destino compatível com o AWS Simple Notification Service (SNS).

O que você vai precisar

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado um bucket para agir como a fonte das notificações.
- O endpoint que você pretende usar como destino para notificações de eventos já deve existir, e você deve ter sua URNA.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário. 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 as notificações de eventos, sempre que um evento especificado ocorre para um objeto no intervalo de origem, uma notificação é gerada e enviada para o tópico Serviço de notificação simples (SNS) usado como ponto de extremidade de destino. Para ativar notificações para um bucket, você deve criar e aplicar XML de configuração de notificação válida. O XML de configuração de notificação deve usar a URNA de um endpoint de notificações de eventos para cada destino.

Para obter informações gerais sobre notificações de eventos e como configurá-las, consulte a documentação da Amazon. Para obter informações sobre como o StorageGRID implementa a API de configuração de notificação de bucket do S3, consulte as instruções para implementar aplicativos cliente do S3.

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

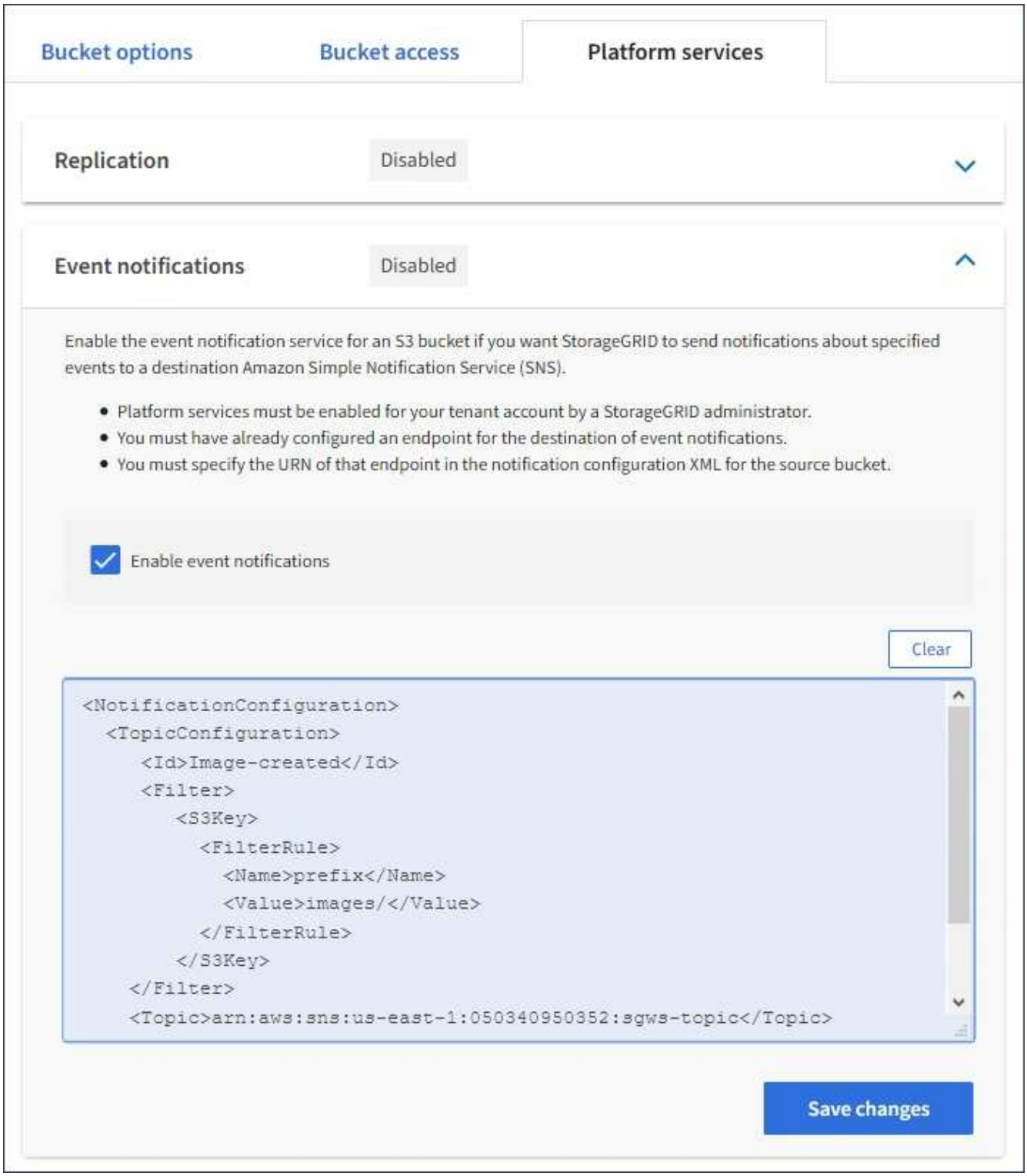
1. Ativar notificações para o intervalo de origem:
    - Use um editor de texto para criar a configuração de notificação XML necessário para habilitar notificações de eventos, conforme especificado na API de notificação S3.
    - Ao configurar o XML, use a URNA de um endpoint de notificações de eventos 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 SNS de destino.

Por exemplo, se o tópico de destino estiver hospedado no AWS Simple Notification Service (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

"Entendendo as notificações para buckets"

"Use S3"

"Criando um endpoint de serviços de plataforma"

Usando o serviço de integração de pesquisa

O serviço de integração de pesquisa é um dos três serviços da plataforma StorageGRID. Você pode habilitar esse serviço para enviar metadados de objetos para um índice de pesquisa de destino sempre que um objeto for criado, excluído ou seus metadados ou tags forem atualizados.

Você pode configurar a integração de pesquisa usando o Gerenciador de inquilinos para aplicar XML de configuração personalizada do StorageGRID a um bucket.

> 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 configuração de notificação de *metadata XML*. Esse XML de configuração é diferente da configuração *notificação XML* usada para ativar notificações de eventos.

Consulte as instruções para implementar aplicativos cliente S3 para obter detalhes sobre as seguintes operações personalizadas da API REST do StorageGRID S3:

- EXCLUIR solicitação de configuração de notificação de metadados do bucket
- OBTER solicitação de configuração de notificação de metadados do bucket
- COLOCAR solicitação de configuração de notificação de metadados do bucket

Informações relacionadas

"Configuração XML para integração de pesquisa"

"Metadados de objetos incluídos nas notificações de metadados"

"JSON gerado pelo serviço de integração de pesquisa"

"Configurando o serviço de integração de pesquisa"

"Use S3"

Configuração XML para integração de pesquisa

O serviço de integração de pesquisa é configurado usando um conjunto de regras contidas nas `<MetadataNotificationConfiguration>` tags e `</MetadataNotificationConfiguration>` . Cada regra especifica os objetos aos quais a regra se aplica e o destino ao qual o StorageGRID deve enviar os metadados desses 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 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.

Os destinos devem ser especificados usando a URNA de um endpoint StorageGRID que foi criado para o serviço de integração de pesquisa. Esses endpoints referem-se a um índice e tipo definidos em um cluster do Elasticsearch.

```
<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

Nome	Descrição	Obrigatório
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
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

Use o XML de configuração de notificação de metadados de amostra para aprender a construir seu próprio XML.

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>
```

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>
```

Informações relacionadas

"Use S3"

"JSON gerado pelo serviço de integração de pesquisa"

"Configurando o serviço de integração de pesquisa"

O serviço de integração de pesquisa 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.

O que você vai precisar

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado 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 deve existir, e você deve ter sua URNA.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário. 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. Você deve atualizar esses objetos existentes para garantir que seus metadados sejam adicionados ao índice de pesquisa de destino.

Passos

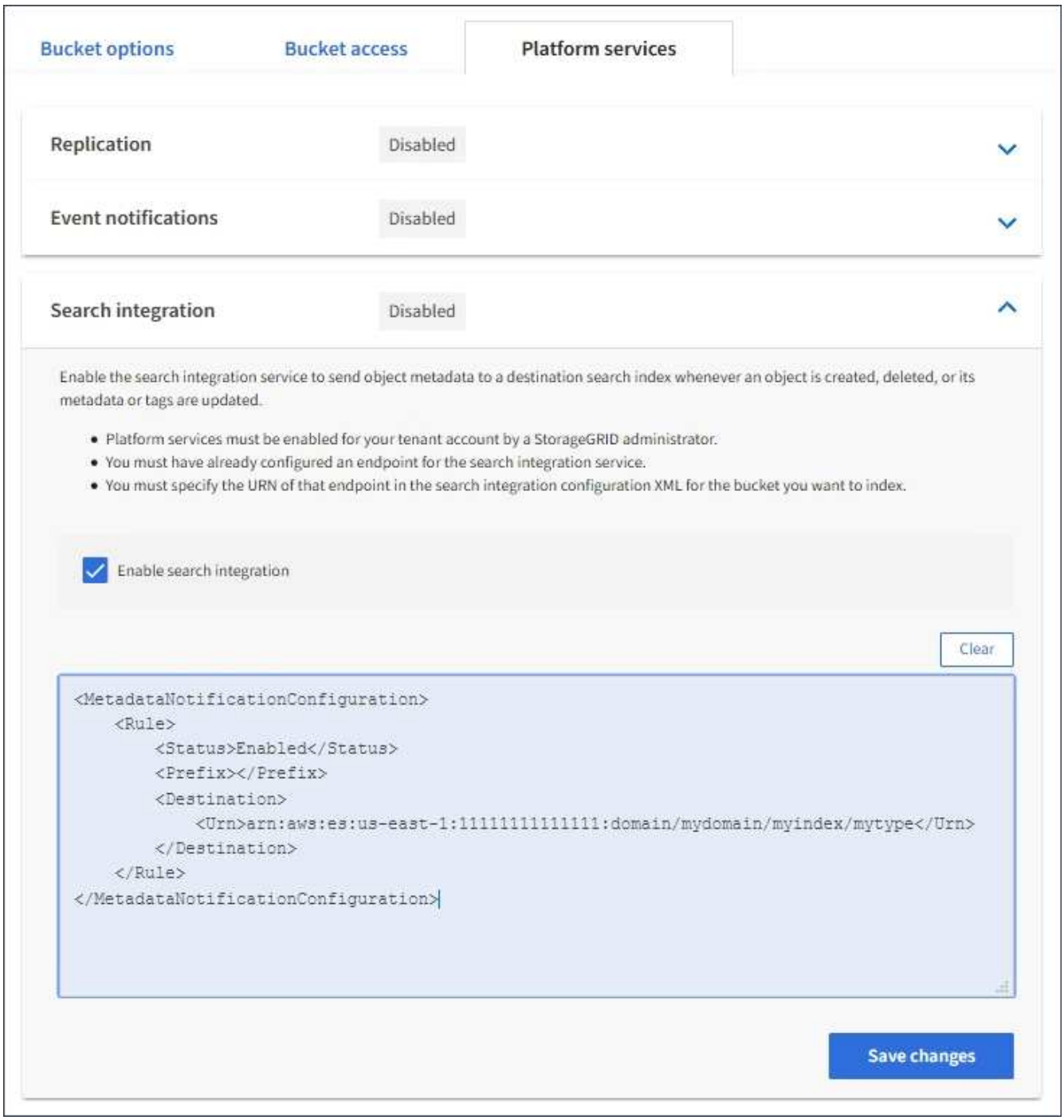
1. Use um editor de texto para criar o XML de notificação de metadados necessário para habilitar a integração de pesquisa.
   - Consulte as informações sobre o XML de configuração para integração de pesquisa.
   - Ao configurar o XML, use a URNA de um endpoint de integração de pesquisa como o destino.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

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 integração de pesquisa**
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 **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.

Informações relacionadas

"Compreender o serviço de integração de pesquisa"

"Configuração XML para integração de pesquisa"

"Use S3"

"Criando um endpoint de serviços de plataforma"

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 e descrição do item
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`

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.

Use S3

Saiba como os aplicativos clientes podem usar a API S3 para fazer interface com o sistema StorageGRID.

- "Suporte para a API REST do S3"
- "Configurando contas de locatário e conexões"
- "Como o StorageGRID implementa a API REST do S3"
- "S3 operações e limitações suportadas pela API REST"
- "Operações da API REST do StorageGRID S3"
- "Políticas de acesso ao bucket e ao grupo"
- "Configurando a segurança para a API REST"
- "Operações de monitoramento e auditoria"
- "Benefícios de conexões HTTP ativas, ociosas e simultâneas"

Suporte para a API REST do S3

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 conectar aplicações orientadas a serviços desenvolvidas para serviços da Web do S3 ao storage de objetos no local que usa o sistema StorageGRID. Isso requer alterações mínimas no uso atual de chamadas de API REST do aplicativo cliente S3.

- "Alterações ao suporte à API REST do S3"
- "Versões suportadas"
- "Suporte para serviços de plataforma StorageGRID"

Alterações ao suporte à API REST do S3

Você deve estar ciente das alterações no suporte do sistema StorageGRID para a API REST do S3.

Solte	Comentários
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 e lista atualizada de pacotes de criptografia TLS suportados. • O serviço CLB está obsoleto.
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. • Lista atualizada dos conjuntos de encriptação TLS suportados. 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 configuração de controle de 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.

Versões suportadas

O StorageGRID suporta as seguintes versões específicas do S3 e HTTP.

Item	Versão
Especificação S3	*Referência da API de serviço de armazenamento simples* 2006-03-01
HTTP	1,1 Para obter mais informações sobre HTTP, consulte HTTP/1,1 (RFCs 7230-35). **Nota**: O StorageGRID não suporta a canalização HTTP/1,1.

Informações relacionadas

"IETF RFC 2616: Protocolo de transferência de hipertexto (HTTP/1,1)"

"Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service"

Suporte para serviços de plataforma StorageGRID

Os serviços da plataforma StorageGRID permitem que as contas de locatários do StorageGRID aproveitem serviços externos, como um bucket remoto do S3, um endpoint do Serviço de notificação simples (SNS) ou um cluster do Elasticsearch para estender os serviços fornecidos por uma grade.

A tabela a seguir resume os serviços de plataforma disponíveis e as APIs do S3 usadas para configurá-los.

Serviço de plataforma	Finalidade	S3 API usada para configurar o serviço
Replicação do CloudMirror	Replica objetos de um bucket do StorageGRID de origem para o bucket do S3 remoto configurado.	COLOQUE a replicação do balde
Notificações	Envia notificações sobre eventos em um bucket do StorageGRID de origem para um endpoint configurado do Serviço de notificação simples (SNS).	COLOCAR notificação de balde
Integração de pesquisa	Envia metadados de objetos para objetos armazenados em um bucket do StorageGRID para um índice Elasticsearch configurado.	NOTIFICAÇÃO DE metadados do Bucket **Observação:** esta é uma API S3D personalizada do StorageGRID.

Um administrador de grade deve habilitar o uso de serviços de plataforma para uma conta de locatário antes

que eles possam ser usados. Em seguida, um administrador de locatário deve criar um endpoint que represente o serviço remoto na conta de locatário. Esta etapa é necessária antes que um serviço possa ser configurado.

Recomendações para o uso de serviços de plataforma

Antes de usar os serviços de plataforma, você deve estar ciente das seguintes recomendações:

- A NetApp recomenda que você não permita 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.
- Se um bucket do S3 no sistema do StorageGRID tiver o controle de versão e a replicação do CloudMirror habilitado, a NetApp recomenda que o endpoint de destino também tenha o controle de versão do bucket do S3 habilitado. Isso permite que a replicação do CloudMirror gere versões de objetos semelhantes no endpoint.
- A replicação do CloudMirror não é suportada se o bucket de origem tiver o S3 Object Lock ativado.
- A replicação do CloudMirror falhará com um erro AccessDenied se o intervalo de destino tiver conformidade legada habilitada.

Informações relacionadas

"Use uma conta de locatário"

"Administrar o StorageGRID"

"Operações em baldes"

"COLOCAR solicitação de configuração de notificação de metadados do bucket"

Configurando contas de locatário e conexões

Configurar o StorageGRID para aceitar conexões de aplicativos cliente requer a criação de uma ou mais contas de locatário e a configuração das conexões.

Criação e configuração de contas de locatário do S3

Uma conta de locatário S3 é necessária antes que os clientes API S3D possam armazenar e recuperar objetos no StorageGRID. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários, além de contentores e objetos.

As contas de locatário do S3 são criadas por um administrador de grade do StorageGRID usando o Gerenciador de grade ou a API de gerenciamento de grade. Ao criar uma conta de locatário do S3, o administrador da grade especifica as seguintes informações:

- Nome de exibição para o locatário (o ID da conta do locatário é atribuído automaticamente e não pode ser alterado).
- Se a conta de locatário tem permissão para usar serviços de plataforma. Se o uso de serviços de plataforma for permitido, a grade deve ser configurada para suportar seu uso.
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).
- Se a federação de identidade estiver ativada para o sistema StorageGRID, qual grupo federado tem

permissão de acesso root para configurar a conta de locatário.

- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.

Depois que uma conta de locatário do S3 for criada, os usuários do locatário poderão acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configure a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e crie grupos e usuários locais
- Gerenciar S3 chaves de acesso
- Crie e gerencie buckets do S3, incluindo buckets que têm o bloqueio de objetos do S3 ativado
- Usar serviços de plataforma (se ativado)
- Monitorar o uso do storage

> Os usuários de locatários do S3 podem criar e gerenciar buckets do S3 com o Tenant Manager, mas precisam ter S3 chaves de acesso e usar a API REST do S3 para ingerir e gerenciar objetos.

Informações relacionadas

"Administrar o StorageGRID"

"Use uma conta de locatário"

Como as conexões do cliente podem ser configuradas

Um administrador de grade faz escolhas de configuração que afetam a forma como os clientes S3 se conetam ao StorageGRID para armazenar e recuperar dados. As informações específicas que você precisa para fazer uma conexão dependem da configuração escolhida.

Os aplicativos clientes podem armazenar ou recuperar objetos conetando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway, ou, opcionalmente, o endereço IP virtual de um grupo de alta disponibilidade (HA) de nós de administração ou nós de gateway
- O serviço CLB em nós de Gateway, ou, opcionalmente, o endereço IP virtual de um grupo de nós de gateway de alta disponibilidade

> O serviço CLB está obsoleto. Os clientes configurados antes da versão do StorageGRID 11,3 podem continuar a usar o serviço CLB nos nós de gateway. Todos os outros aplicativos clientes que dependem do StorageGRID para fornecer balanceamento de carga devem se conetar usando o serviço de balanceamento de carga.

- Nós de storage, com ou sem um balanceador de carga externo

Ao configurar o StorageGRID, um administrador de grade pode usar o Gerenciador de grade ou a API de gerenciamento de grade para executar as seguintes etapas, todas opcionais:

1. Configure endpoints para o serviço Load Balancer.

   Você deve configurar endpoints para usar o serviço Load Balancer. O serviço Load Balancer em nós de administração ou nós de gateway distribui conexões de rede recebidas de aplicativos clientes para nós de

storage. Ao criar um endpoint de balanceador de carga, o administrador do StorageGRID especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).

2. Configurar redes de clientes não confiáveis.

   Se um administrador do StorageGRID configurar a rede cliente de um nó para não ser confiável, o nó só aceita conexões de entrada na rede cliente em portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

3. Configurar grupos de alta disponibilidade.

   Se um administrador criar um grupo de HA, as interfaces de rede de vários nós de Admin ou nós de Gateway serão colocadas em uma configuração de backup ativo. As conexões de cliente são feitas usando o endereço IP virtual do grupo HA.

Para obter mais informações sobre cada opção, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Resumo: Endereços IP e portas para conexões de clientes

Os aplicativos cliente se conetam ao StorageGRID usando o endereço IP de um nó de grade e o número da porta de um serviço nesse nó. Se os grupos de alta disponibilidade (HA) estiverem configurados, os aplicativos clientes poderão se conetar usando o endereço IP virtual do grupo HA.

Informações necessárias para fazer conexões com o cliente

A 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. Contate o administrador do StorageGRID para obter mais informações ou consulte as instruções de administração do StorageGRID para obter uma descrição de como localizar essas informações 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 de extremidade do balanceador de carga
Grupo HA	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas S3 padrão: • HTTPS: 8082 • HTTP: 8084
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	• Porta de extremidade do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	• Porta de extremidade do balanceador de carga
Nó de gateway	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP do nó de gateway **Nota:** por predefinição, as portas HTTP para CLB e LDR não estão ativadas.	Portas S3 padrão: • HTTPS: 8082 • HTTP: 8084
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084

Exemplo

Para conetar um cliente S3 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 de um endpoint do balanceador de carga S3 for 10443, um cliente S3 poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.5:10443`

É possível configurar um nome DNS para o endereço IP que os clientes usam para se conetar ao StorageGRID. Contacte o administrador da rede local.

Informações relacionadas

"Administrar o StorageGRID"

Decidir usar conexões HTTPS ou HTTP

Quando as conexões de cliente são feitas usando um endpoint de Load Balancer, as conexões devem ser feitas usando o protocolo (HTTP ou HTTPS) especificado para esse endpoint. Para usar HTTP para conexões de cliente a nós de armazenamento ou ao serviço CLB em nós de gateway, você deve habilitar seu uso.

Por padrão, quando os aplicativos cliente se conetam a nós de armazenamento ou ao serviço CLB nos nós de Gateway, eles devem usar HTTPS criptografado para todas as conexões. Opcionalmente, você pode habilitar conexões HTTP menos seguras selecionando a opção de grade **Ativar conexão HTTP** no Gerenciador de Grade. Por exemplo, um aplicativo cliente pode usar HTTP ao testar a conexão com um nó de armazenamento em um ambiente que não seja de produção.

> Tenha cuidado ao ativar o HTTP para uma grade de produção, já que as solicitações serão enviadas sem criptografia.

O serviço CLB está obsoleto.

Se a opção **Enable HTTP Connection** estiver selecionada, os clientes devem usar portas diferentes para HTTP do que para HTTPS. Consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

"Benefícios de conexões HTTP ativas, ociosas e simultâneas"

Nomes de domínio de endpoint para solicitações S3

Antes de poder usar nomes de domínio S3 para solicitações de cliente, um administrador do StorageGRID deve configurar o sistema para aceitar conexões que usam nomes de domínio S3 em solicitações de estilo de caminho S3 e S3 solicitações virtuais de estilo hospedado.

Sobre esta tarefa

Para permitir que você use S3 solicitações de estilo hospedadas virtuais, um administrador de grade deve executar as seguintes tarefas:

- 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`, o administrador de grade deve garantir que o certificado usado para conexões HTTPS inclua o `s3.company.com` endpoint e o nome alternativo (SAN) de assunto universal (Wildcard Subject Alternative Name) do endpoint: `*.s3.company.com`.

- Configure o servidor DNS usado pelo cliente para incluir Registros DNS que correspondam aos nomes de domínio de endpoint, incluindo todos os Registros curinga necessários.

Se o cliente se conetar usando o serviço Load Balancer, o certificado que o administrador da grade configura é o certificado para o ponto de extremidade do balanceador de carga que o cliente usa.

Cada ponto de extremidade do balanceador de carga tem seu próprio certificado e cada ponto de extremidade pode ser configurado para reconhecer nomes de domínio de endpoint diferentes.

Se o cliente conetar nós de armazenamento ou ao serviço CLB nos nós de Gateway, o certificado que o administrador de grade configura é o único certificado de servidor personalizado usado para a grade.

O serviço CLB está obsoleto.

Consulte as instruções para administrar o StorageGRID para obter mais informações.

Depois que essas etapas forem concluídas, você poderá usar solicitações virtuais de estilo hospedado (por exemplo, `bucket.s3.company.com`).

Informações relacionadas

"Administrar o StorageGRID"

"Configurando a segurança para a API REST"

Testando 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 no sistema.

O que você vai precisar

- Você deve ter baixado e instalado a AWS CLI do "aws.amazon.com/cli".
- Você deve ter criado uma conta de locatário do S3 no sistema StorageGRID.

Passos

1. Configure as configurações do Amazon Web Services para usar a conta criada no sistema StorageGRID:
   a. Entre no modo de configuração: `aws configure`
   b. Insira o ID da chave de acesso da AWS para a conta criada.
   c. Insira a chave de acesso secreto da AWS para a conta criada.
   d. Digite a região padrão a ser usada, 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.

   ```
   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

Um aplicativo cliente pode usar S3 chamadas de API REST para se conetar ao StorageGRID para criar, excluir e modificar buckets, bem como armazenar e recuperar objetos.

- "Solicitações de cliente conflitantes"
- "Controles de consistência"
- "Como as regras do StorageGRID ILM gerenciam objetos"
- "Controle de versão de objetos"
- "Recomendações para a implementação da API REST do S3"

Solicitações de cliente conflitantes

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos".

O calendário 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.

Controles de consistência

Os controles de consistência fornecem uma troca entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós e sites de storage, conforme exigido pelo 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 um nível de consistência diferente, você pode especificar um controle de consistência para cada bucket ou para cada operação de API.

Controles de consistência

O controle de 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 o controle de consistência para um bucket ou uma operação de API para um dos seguintes valores:

Controle de 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. Corresponde às garantias de consistência do Amazon S3. **Observação:** se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, defina o controle de consistência como "disponível", a menos que você exija garantias de consistência semelhantes ao Amazon S3.
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência "read-after-novo-write", mas apenas fornece consistência eventual para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

Usando os controles de consistência "read-after-new-write" e "available"

Quando uma operação HEAD ou GET usa o controle de consistência "read-after-novo-write" ou uma operação GET usa o controle de consistência "'disponível'", 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 nível de consistência até atingir o mais alto nível de consistência, "All", o que requer que todas as cópias dos metadados do objeto estejam disponíveis.

Se uma operação HEAD ou GET usar o controle de consistência "read-after-novo-write", mas o objeto não existir, a pesquisa de objetos sempre alcançará o nível de consistência "'all'". Como esse nível de consistência exige que todas as cópias dos metadados do objeto estejam disponíveis, você pode receber um número alto de 500 erros de servidor interno se um ou mais nós de storage não estiverem disponíveis.

A menos que você precise de garantias de consistência semelhantes ao Amazon S3, você pode evitar esses erros para operações HEAD definindo o controle de consistência como "disponível". Quando uma operação HEAD usa o controle de consistência "disponível", o StorageGRID fornece consistência eventual apenas. Ele não tenta novamente uma operação com falha até atingir o nível de consistência "'tudo'", portanto, não requer que todas as cópias dos metadados do objeto estejam disponíveis.

Especificando o controle de consistência para uma operação de API

Para definir o controle de consistência para uma operação de API individual, os controles de consistência devem ser suportados para a operação e você deve especificar o controle de consistência no cabeçalho da solicitação. Este exemplo define o controle de consistência como "local-trong" para uma operação GET Object.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```

> Você deve usar o mesmo controle de consistência para as operações COLOCAR Objeto e OBTER Objeto.

Especificando o controle de consistência para um bucket

Para definir o controle de consistência para o bucket, você pode usar a solicitação de consistência do bucket do StorageGRID PUT e a solicitação DE consistência do bucket do GET. Ou você pode usar o Gerenciador do Locatário ou a API de Gerenciamento do Locatário.

Ao definir os controlos de consistência para um balde, tenha em atenção o seguinte:

- Definir o controle de consistência para um balde determina qual controle de consistência é usado para operações S3D realizadas nos objetos no balde ou na configuração do balde. Não afeta as operações no próprio balde.
- O controle de consistência para uma operação de API individual substitui o controle de consistência para o bucket.
- Em geral, os buckets devem usar o controle de 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 o controle de consistência para cada solicitação de API. Defina o controle de consistência no nível do balde apenas como último recurso.

Como os controles de consistência e as regras de ILM interagem para afetar a proteção de dados

Tanto a sua escolha de controle de consistência quanto a sua regra ILM afetam a forma como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, o controle de consistência usado 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 nível de consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Strict**: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido ao cliente.
- **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.
- * Commit duplo*: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

> Antes de selecionar o comportamento de ingestão para uma regra ILM, leia a descrição completa dessas configurações nas instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Exemplo de como o controle de consistência e a regra ILM podem interagir

Suponha que você tenha uma grade de dois locais com a seguinte regra ILM e a seguinte configuração de nível de consistência:

- **Regra ILM**: Crie duas cópias de objeto, uma no local e outra em um local remoto. O comportamento de ingestão estrita é selecionado.
- **Nível de consistência**: "Trong-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 o nível de consistência "site-trong", o cliente poderá receber uma mensagem de sucesso depois que os dados do objeto forem replicados para o sitqe 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 níveis de consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Informações relacionadas

"Gerenciar objetos com ILM"

"OBTER pedido de consistência de balde"

"COLOCAR pedido consistência balde"

Como as regras do StorageGRID ILM gerenciam objetos

O administrador da grade cria regras de gerenciamento do ciclo de vida das informações (ILM) para gerenciar dados de objetos ingeridos no sistema StorageGRID a partir de aplicativos clientes da API REST do S3. Essas regras são então adicionadas à política ILM para determinar como e onde os dados do objeto são armazenados ao longo do tempo.

As configurações de ILM determinam os seguintes aspetos de um objeto:

- **Geografia**

  O local dos dados de um objeto, seja no sistema StorageGRID (pool de storage) ou em um pool de storage de nuvem.

- **Grau de armazenamento**

  O tipo de storage usado para armazenar dados de objetos: Por exemplo, flash ou disco giratório.

- * Proteção contra perdas*

  Quantas cópias são feitas e os tipos de cópias criadas: Replicação, codificação de apagamento ou ambos.

- **Retenção**

  As mudanças ao longo do tempo para como os dados de um objeto são gerenciados, onde são armazenados e como eles são protegidos contra perda.

- **Proteção durante o consumo**

  O método usado para proteger dados de objetos durante a ingestão: Colocação síncrona (usando as opções balanceadas ou rigorosas para o comportamento de ingestão) ou fazendo cópias provisórias (usando a opção de confirmação dupla).

As regras do ILM podem filtrar e selecionar objetos. Para objetos ingeridos usando S3, as regras do ILM podem filtrar objetos com base nos seguintes metadados:

- Conta de locatário
- Nome do balde
- Tempo de ingestão
- Chave
- Último tempo de acesso

Por padrão, as atualizações para o último tempo de acesso são desativadas para todos os buckets do S3. Se o seu sistema StorageGRID incluir uma regra ILM que use a opção último tempo de acesso, você deverá habilitar as atualizações para o último tempo de acesso para os buckets do S3 especificados nessa regra. Você pode habilitar as atualizações da última hora de acesso usando a solicitação de última hora de acesso do PUT Bucket, a caixa de seleção **S3 Buckets Configurar último tempo de acesso** no Gerenciador de locatário ou usando a API de Gerenciamento de locatário. Ao ativar as atualizações da última hora de acesso, esteja ciente de que o desempenho do StorageGRID pode ser reduzido, especialmente em sistemas com objetos pequenos.

- Restrição de localização
- Tamanho do objeto
- Metadados do utilizador
- Etiqueta Objeto

Para obter mais informações sobre o ILM, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Informações relacionadas

"Use uma conta de locatário"

"Gerenciar objetos com ILM"

"COLOCAR o último pedido de tempo de acesso do balde"

Controle de versão de objetos

Você pode usar o controle de versão para reter várias versões de um objeto, o que protege contra a exclusão acidental de objetos e permite recuperar e restaurar 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 1.000 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 para ativar essa funcionalidade para o bucket. Cada objeto no seu 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 ao versionamento permite criar regras ILM que usam o tempo não-atual como o tempo de referência. Quando um objeto é atualizado, suas versões anteriores se tornam não atuais. O uso de um filtro de tempo não atual permite criar políticas que reduzam 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.

Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações para obter um exemplo de política ILM para objetos com versão S3.

Informações relacionadas

"Gerenciar objetos com ILM"

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 seu aplicativo verifica rotineiramente para ver se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o controle de consistência ""disponível"". Por exemplo, você deve usar o controle de consistência "disponível" se seu aplicativo dirigir um local antes DE COLOCÁ-lo.

Caso contrário, se a operação PRINCIPAL não encontrar o objeto, você poderá receber um número alto de 500 erros de servidor interno se um ou mais nós de storage não estiverem disponíveis.

Você pode definir o controle de consistência "'disponível'" para cada bucket usando a solicitação de consistência do PUT Bucket, ou você pode especificar o controle de consistência no cabeçalho da solicitação para uma operação de API individual.

Recomendações para chaves de objeto

Para buckets criados no StorageGRID 11,4 ou posterior, não é mais necessário restringir nomes de chaves do objeto para atender às práticas recomendadas de desempenho. Por exemplo, agora você pode usar valores aleatórios para os primeiros quatro carateres de nomes de chave de objeto.

Para buckets que foram criados em versões anteriores ao StorageGRID 11,4, continue seguindo estas recomendações para nomes de chaves de objeto:

- Você não deve usar 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, você deve usar 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, você deve prefixar 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
```

Recomendações para "leituras de intervalo"

Se a opção **Compress Stored Objects** estiver selecionada (**Configuration Grid Options**), os aplicativos cliente S3 devem evitar executar operações GET Object que especificem um intervalo de bytes serão retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é muito 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.

Informações relacionadas

"Controles de consistência"

"COLOCAR pedido consistência balde"

"Administrar o StorageGRID"

S3 operações e limitações suportadas pela API REST

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.

- "Autenticando solicitações"
- "Operações no serviço"
- "Operações em baldes"
- "Operações personalizadas em buckets"
- "Operações em objetos"
- "Operações para uploads de várias partes"
- "Respostas de erro"

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 cabeçalhos de solicitação comuns definidos pela *Simple Storage Service API Reference*, 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: • O valor SHA256 não é calculado para o corpo da solicitação. O valor enviado pelo usuário é aceito sem validação, como se o valor `UNSIGNED-PAYLOAD` tivesse sido fornecido para o `x-amz-content-sha256` cabeçalho.
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

Informações relacionadas

"Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service"

Autenticando 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.

Usando 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.

Usando 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
Serviço GET	Implementado com todo o comportamento da API REST do Amazon S3.
OBTER 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. 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.

Informações relacionadas

"OBTER solicitação de uso de armazenamento"

Operações em baldes

O sistema StorageGRID dá suporte a um máximo de 1.000 buckets para cada conta de locatário de S3 TB.

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 do S3.

"Documentação do Amazon Web Services (AWS): Restrições e limitações do bucket"

"Nomes de domínio de endpoint para solicitação S3"

As operações GET Bucket (List Objects) e GET Bucket Versions suportam controles de consistência do StorageGRID.

Você pode verificar se as atualizações para a última hora de acesso estão ativadas ou desativadas para buckets individuais.

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
ELIMINAR balde	Implementado com todo o comportamento da API REST do Amazon S3.
ELIMINAR Cors balde	Esta operação exclui a configuração CORS para o bucket.
ELIMINAR encriptação Bucket	Esta operação exclui a criptografia padrão do intervalo. Os objetos criptografados existentes permanecem criptografados, mas todos os novos objetos adicionados ao bucket não são criptografados.
ELIMINAR ciclo de vida do balde	Esta operação exclui a configuração do ciclo de vida do bucket.
ELIMINAR política de balde	Esta operação exclui a política anexada ao bucket.
ELIMINAR replicação de balde	Esta operação exclui a configuração de replicação anexada ao bucket.
ELIMINAR marcação de intervalo	Esta operação usa o `tagging` subrecurso para remover todas as tags de um bucket.

Operação	Implementação
GET Bucket (List Objects), versão 1 e versão 2	Esta operação retorna alguns ou todos (até 1.000) dos objetos em um balde. 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.
OBTER acl balde	Esta operação retorna uma resposta positiva e a ID, DisplayName e permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
OBTER Bucket Cors	Esta operação retorna a `cors` configuração do balde.
OBTER criptografia Bucket	Esta operação retorna a configuração de criptografia padrão para o bucket.
OBTENHA o ciclo de vida do Bucket	Esta operação retorna a configuração do ciclo de vida do bucket.
OBTER localização do balde	Esta operação retorna a região que foi definida usando o `LocationConstraint` elemento na solicitação PUT Bucket. Se a região do bucket for `us-east-1`, uma string vazia será retornada para a região.
OBTER notificação Bucket	Esta operação retorna a configuração de notificação anexada ao bucket.
OBTER versões Objeto balde	Com ACESSO DE LEITURA em um bucket, essa operação com o `versions` subrecurso lista metadados de todas as versões de objetos no bucket.
OBTER política Bucket	Esta operação retorna a política anexada ao bucket.

Operação	Implementação
OBTER replicação do bucket	Esta operação retorna a configuração de replicação anexada ao bucket.
OBTER marcação Bucket	Esta operação usa o `tagging` subrecurso para retornar todas as tags para um bucket.
OBTENHA o controle de versão do Bucket	Essa implementação usa `versioning` o subrecurso para retornar o estado de controle de versão de um bucket. O estado de versionamento retornado indica se o bucket está "não versionado" ou se o bucket é a versão "habilitado" ou "suspenso".
OBTER Configuração bloqueio Objeto	Esta operação determina se o bloqueio de objetos S3D está ativado para um balde. "Usando S3 Object Lock"
Balde DA cabeça	Esta operação determina se existe um intervalo e você tem permissão para acessá-lo.

Operação	Implementação
COLOQUE o balde	Esta operação 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 PUT Bucket 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. 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 intervalo. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket. "Usando S3 Object Lock"

Operação	Implementação
COLOQUE cors de balde	Esta operação 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`.
COLOQUE a criptografia Bucket	Esta operação define o estado de criptografia padrão de um bucket 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).

Operação	Implementação
COLOQUE o ciclo de vida do balde	Essa operação 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: • Validade (dias, Data) • Não-currentVersionExpiration (não-currentDays) • Filtro (prefixo, Tag) • Estado • ID O StorageGRID não oferece suporte a essas ações: • AbortIncompleteMultipartUpload • ExpiredObjectDeleteMarker • Transição Para entender como a ação Expiration em um ciclo de vida de um bucket interage com as instruções de colocação do ILM, consulte "como o ILM opera ao longo da vida de um objeto" nas instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações. **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

COLOCAR notificação de balde	Esta operação 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 Serviço de notificação simples (SNS) 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 seguinte listagem:
	• **EventSource**
	
	`sgws:s3`
	
	• **AwsRegion**
	
	não incluído
	
	• **x-amz-id-2**
	
	não incluído
	
	• **arn**
	
	`urn:sgws:s3:::bucket_name`

Política COLOCAR balde	Esta operação define a política anexada ao balde.

Operação	Implementação
COLOQUE a replicação do balde	Esta operação configura a 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. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes. • 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. 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
COLOQUE a marcação de balde	Esta operação 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.
COLOQUE o controle de versão do Bucket	Essa implementação usa `versioning` o 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` .

Informações relacionadas

"Documentação do Amazon Web Services (AWS): Replicação entre regiões"

"Controles de consistência"

"OBTER último pedido de tempo de acesso do Bucket"

"Políticas de acesso ao bucket e ao grupo"

"Usando S3 Object Lock"

"S3 operações rastreadas nos logs de auditoria"

"Gerenciar objetos com ILM"

"Use uma conta de locatário"

Criando uma 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 a criação de configurações de ciclo de vida do S3, consulte a seção sobre gerenciamento do ciclo de vida do objeto no *Amazon Simple Storage Service Developer Guide*. Observe que o StorageGRID suporta apenas ações de expiração; ele não oferece suporte a ações de transição.

"Amazon Simple Storage Service Developer Guide: Gerenciamento do ciclo de vida do objeto"

O que é uma configuração de 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

Se você aplicar uma configuração de ciclo de vida a um bucket, as configurações de ciclo de vida do bucket sempre substituem as configurações de ILM do StorageGRID. O StorageGRID usa as configurações de expiração para o bucket, não o ILM, para determinar se deseja excluir ou reter objetos específicos.

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, consulte "como o ILM opera ao longo da vida de um objeto" nas instruções para gerenciar objetos com gerenciamento do ciclo de vida da informação.

> 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:

- ELIMINAR ciclo de vida do balde
- OBTENHA o ciclo de vida do Bucket
- COLOQUE o ciclo de vida do balde

Criando a 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"
        }
    ]
}
```

Aplicando uma configuração de ciclo de vida a um bucket

Depois de criar o arquivo de configuração do ciclo de vida, aplique-o a um bucket emitindo uma solicitação DE ciclo de vida do PUT Bucket.

Esta solicitação aplica a configuração do ciclo de vida no arquivo de exemplo a objetos em um bucket chamado `testbucket`:bucket

```
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 DE ciclo de vida do GET Bucket. 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.

A validação da expiração do ciclo de vida do bucket se aplica a um objeto

É possível determinar se uma regra de expiração na configuração do ciclo de vida se aplica a um objeto específico ao emitir uma SOLICITAÇÃO PUT Object, HEAD Object ou GET Object. 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, consulte ""como a retenção de objetos é determinada"" nas instruções para executar a administração do StorageGRID.

Por exemplo, essa SOLICITAÇÃO PUT Object 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 de objeto PRINCIPAL 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": {}
}
```

Informações relacionadas

"Operações em baldes"

"Gerenciar objetos com ILM"

Operações personalizadas em buckets

O sistema StorageGRID dá suporte a operações de bucket personalizadas que são adicionadas à API REST do S3 e são específicas do sistema.

A tabela a seguir lista as operações de bucket personalizadas suportadas pelo StorageGRID.

Operação	Descrição	Para mais informações
OBTER consistência de balde	Retorna o nível de consistência que está sendo aplicado a um balde específico.	"OBTER pedido de consistência de balde"

Operação	Descrição	Para mais informações
COLOQUE a consistência do balde	Define o nível de consistência aplicado a um balde específico.	"COLOCAR pedido consistência balde"
OBTER último tempo de acesso do Bucket	Retorna se as atualizações da última hora de acesso estão ativadas ou desativadas para um intervalo específico.	"OBTER último pedido de tempo de acesso do Bucket"
COLOQUE o último tempo de acesso do balde	Permite-lhe ativar ou desativar as atualizações da última hora de acesso para um intervalo específico.	"COLOCAR o último pedido de tempo de acesso do balde"
ELIMINAR configuração de notificação de metadados do bucket	Exclui o XML de configuração de notificação de metadados associado a um bucket específico.	"EXCLUIR solicitação de configuração de notificação de metadados do bucket"
OBTER configuração de notificação de metadados do bucket	Retorna o XML de configuração de notificação de metadados associado a um intervalo específico.	"OBTER solicitação de configuração de notificação de metadados do bucket"
COLOQUE a configuração de notificação de metadados do bucket	Configura o serviço de notificação de metadados para um bucket.	"COLOCAR solicitação de configuração de notificação de metadados do bucket"
COLOQUE modificações no balde para conformidade	Obsoleto e não suportado: Você não pode mais criar novos buckets com a conformidade ativada.	"Obsoleto: Modificações de solicitação de Bucket para conformidade"
OBTENHA conformidade com o balde	Obsoleto, mas suportado: Retorna as configurações de conformidade atualmente em vigor para um bucket compatível com legado existente.	"Obsoleto: OBTER solicitação de conformidade do bucket"
COLOQUE a conformidade do balde	Obsoleto, mas suportado: Permite modificar as configurações de conformidade para um bucket compatível com legado existente.	"Obsoleto: COLOQUE a solicitação de conformidade do bucket"

Informações relacionadas

"S3 operações rastreadas nos logs de auditoria"

Operações em objetos

Esta seção descreve como o sistema StorageGRID implementa S3 operações de API REST para objetos.

- "Usando S3 Object Lock"
- "Usando criptografia do lado do servver"
- "Objeto GET"
- "Objeto HEAD"
- "Restauração PÓS-objeto"
- "Objeto PUT"
- "COLOCAR Objeto - Copiar"

As seguintes condições se aplicam a todas as operações de objetos:

- Os controles de consistência do StorageGRID são suportados por todas as operações em objetos, com exceção do seguinte:
  - OBTER ACL Objeto
  - `OPTIONS /`
  - COLOCAR guarda legal Objeto
  - COLOCAR retenção Objeto
- As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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
Objeto DELETE	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Ao processar uma solicitação DE EXCLUSÃO de objetos, 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 habilitado para versão, 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 suspenso de versão, 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.
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.

Operação	Implementação
ELIMINAR marcação Objeto	Usa o `tagging` subrecurso para remover todas as tags de um objeto. Implementado com todo o comportamento da API REST do Amazon S3. **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'" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.
Objeto GET	"Objeto GET"
OBTER ACL Objeto	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.
OBTER retenção legal Objeto	"Usando S3 Object Lock"
OBTER retenção de objetos	"Usando S3 Object Lock"
OBTER marcação de objetos	Usa o `tagging` subrecurso para retornar todas as tags para um objeto. Implementado com todo o comportamento da API REST do Amazon S3 **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'" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.
Objeto HEAD	"Objeto HEAD"
Restauração PÓS-objeto	"Restauração PÓS-objeto"
Objeto PUT	"Objeto PUT"

Operação	Implementação
COLOCAR Objeto - Copiar	"COLOCAR Objeto - Copiar"
COLOCAR guarda legal Objeto	"Usando S3 Object Lock"
COLOCAR retenção Objeto	"Usando S3 Object Lock"

Operação	Implementação
COLOQUE a marcação Objeto	Usa o `tagging` subrecurso para adicionar um conjunto de tags a um objeto existente. Implementado com todo o comportamento da API REST do Amazon S3 **Atualizações de tags e comportamento de ingestão** Quando você usa a marcação "COLOCAR objeto" 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 clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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'" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Informações relacionadas

"Controles de consistência"

"S3 operações rastreadas nos logs de auditoria"

Usando S3 Object Lock

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 e, em seguida, especificar as configurações de retenção legal e de retenção para cada versão de objeto adicionada a esse bucket.

O bloqueio de objetos S3 permite especificar configurações no nível do objeto para impedir que objetos sejam excluídos ou substituídos por um período fixo de tempo ou indefinidamente.

O recurso bloqueio de objetos do StorageGRID S3 fornece um modo de retenção único equivalente ao modo de conformidade do Amazon S3. Por padrão, uma versão de objeto protegido não pode ser substituída ou excluída por nenhum usuário. O recurso bloqueio de objetos do StorageGRID S3 não suporta um modo de governança e não permite que usuários com permissões especiais ignorem as configurações de retenção ou excluam objetos protegidos.

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. Você pode usar qualquer um destes métodos:

- Crie o bucket usando o Gerenciador do locatário.

  "Use uma conta de locatário"

- Crie o bucket usando uma solicitação DE COLOCAR balde com o `x-amz-bucket-object-lock_enabled` cabeçalho de solicitação.

  "Operações em baldes"

Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação do bucket. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.

Um bucket com S3 Object Lock ativado pode conter uma combinação de objetos com e sem configurações de bloqueio de objeto S3. O StorageGRID não suporta retenção padrão para os objetos nos buckets do bloqueio de objetos do S3, portanto, a operação do bucket Configuração do bloqueio de objetos do PUT não é suportada.

Determinar se o bloqueio de objeto S3 está ativado para um bucket

Para determinar se o bloqueio de objeto S3 está ativado, use a solicitação DE configuração OBTER bloqueio de objeto.

"Operações em baldes"

Criando um objeto com S3 configurações de bloqueio de objeto

Para especificar as configurações de bloqueio de objeto S3 ao adicionar uma versão de objeto a um intervalo que tenha o bloqueio de objeto S3 ativado, emita um Objeto PUT, COLOCAR Objeto - Copiar ou inicie uma solicitação de upload de várias partes. Use os cabeçalhos de solicitação a seguir.

Você deve habilitar o bloqueio de objeto S3 quando criar um bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um intervalo.

- `x-amz-object-lock-mode`, Que deve ser CONFORMIDADE (sensível a maiúsculas e 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 DE Objeto PUT. `Content-MD5` Não é necessário para COLOCAR Objeto - Copiar ou iniciar carregamento Multipart.
- 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 put Object 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 DE GET ou HEAD Object 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*`.
- Uma solicitação DE versão DE EXCLUSÃO de objeto subsequente ou versões de EXCLUSÃO de objetos falhará se for antes da data de retenção ou se uma retenção legal estiver ativada.

A atualizar as definições de bloqueio de objetos do S3

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:

- `PUT Object legal-hold`

  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.

- `PUT Object retention`
  - O valor do modo deve ser CONFORMIDADE (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.

Informações relacionadas

"Gerenciar objetos com ILM"

"Use uma conta de locatário"

"Objeto PUT"

"COLOCAR Objeto - Copiar"

"Inicie o carregamento de várias peças"

"Controle de versão de objetos"

"Guia do usuário do Amazon Simple Storage Service: Usando o bloqueio de objeto S3"

Usando 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.

Usando 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:

- Objeto PUT
- COLOCAR Objeto - Copiar
- Inicie o carregamento de várias peças

Usando 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:

- Objeto GET
- Objeto HEAD
- Objeto PUT
- COLOCAR Objeto - Copiar
- Inicie o carregamento de várias peças
- Carregar artigo
- Carregar artigo - Copiar

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 do CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

Informações relacionadas

"Objeto GET"

"Objeto HEAD"

"Objeto PUT"

"COLOCAR Objeto - Copiar"

"Inicie o carregamento de várias peças"

"Carregar artigo"

"Carregar artigo - Copiar"

"Guia do desenvolvedor do Amazon S3: Protegendo dados usando criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)"

Objeto GET

Você pode usar a solicitação S3 GET Object para recuperar um objeto de um bucket do S3.

O parâmetro pedido de número de peça não é suportado

O `partNumber` parâmetro Request não é suportado para OBTER solicitações Objeto. Não é possível executar uma SOLICITAÇÃO GET para recuperar uma parte específica de um objeto multipart. Um erro 501 não implementado é retornado com a seguinte mensagem:

```
GET Object by partNumber is not implemented
```

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 em "usar criptografia do lado do servidor".

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 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" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Comportamento DO GET Object para objetos Pool de storage de nuvem

Se um objeto tiver sido armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), o comportamento de uma SOLICITAÇÃO GET Object depende do estado do objeto. Consulte "Objeto PRINCIPAL" 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 DE OBTENÇÃO de objetos tentarão recuperar dados da grade, antes de recuperá-los do pool de armazenamento em nuvem.

Estado do objeto	Comportamento de GET Object
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.

Estado do objeto	Comportamento de GET Object
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 solicitação de restauração PÓS-objeto 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 restauração PÓS-objeto 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 GET Object 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 GET Object pode retornar alguns dados, mas parar no meio da transferência.
- Uma solicitação OBTER Objeto subsequente pode retornar `403 Forbidden`.

Informações relacionadas

"Usando criptografia do lado do servidor"

"Gerenciar objetos com ILM"

"Restauração PÓS-objeto"

"S3 operações rastreadas nos logs de auditoria"

Objeto HEAD

Você pode usar a solicitação de Objeto S3 HEAD 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 Objeto HEAD para determinar o estado de transição do objeto.

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 em "usar criptografia do lado do servidor".

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 pedido não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented`:

- `x-amz-website-redirect-location`

Cabeçalhos de resposta para objetos Pool de armazenamento em nuvem

Se o objeto for armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), 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 objeto PRINCIPAL
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.)

Estado do objeto	Resposta ao objeto PRINCIPAL

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 solicitação de restauração PÓS-Objeto 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`

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"`

Estado do objeto	Resposta ao objeto PRINCIPAL

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 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 de objeto PRINCIPAL 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.

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" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Informações relacionadas

"Usando criptografia do lado do servidor"

"Gerenciar objetos com ILM"

"Restauração PÓS-objeto"

"S3 operações rastreadas nos logs de auditoria"

Restauração PÓS-objeto

Você pode usar a solicitação de restauração PÓS-objeto S3 para restaurar um objeto armazenado em um pool de storage de nuvem.

Tipo de solicitação suportada

O StorageGRID suporta apenas solicitações de restauração PÓS-objeto 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 da restauração PÓS-objeto em objetos do Cloud Storage Pool

Se um objeto tiver sido armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), uma solicitação de restauração PÓS-objeto terá o seguinte comportamento, com base no estado do objeto. Consulte "Objeto PRINCIPAL" 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 será necessário restaurar o objeto emitindo uma solicitação de restauração PÓS-objeto. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma SOLICITAÇÃO GET Object.

Estado do objeto	Comportamento da restauração PÓS-objeto
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`.
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. **Atenção**: Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou se o Cloud Storage Pool usar o armazenamento Blob do Azure, 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`

Estado do objeto	Comportamento da restauração PÓS-objeto
Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK` **Observação:** se um objeto foi restaurado para um estado recuperável, você pode alterar o mesmo `expiry-date` reemitindo a solicitação de restauração PÓS-objeto com um novo valor para `Days`. A data de restauração é atualizada em relação à hora da solicitação.

Informações relacionadas

"Gerenciar objetos com ILM"

"Objeto HEAD"

"S3 operações rastreadas nos logs de auditoria"

Objeto PUT

Você pode usar a solicitação de objetos S3D PUT para adicionar um objeto a um bucket.

Resolução de conflitos

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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 StorageGRID suporta objetos de até 5 TB de tamanho.

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 PUT, PUT Object-Copy, GET e HEAD 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-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-<em>name</em>: <em>value</em>
  ```

  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 as opções balanceadas ou rigorosas para o comportamento de ingestão. 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`

"Usando S3 Object Lock"

- 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`

"S3 operações e limitações suportadas pela API REST"

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- O `x-amz-acl` cabeçalho da solicitação não é suportado.
- O `x-amz-website-redirect-location` cabeçalho da solicitação não é suportado e 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 que corresponde a um objeto ingerido usar a opção estrita para comportamento 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 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 nós de storage diferentes.

    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.

Atenção: 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 pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

Nota: 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`
- **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.

Atenção: 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 em "usar criptografia do lado do servidor".

Nota: Se um objeto for criptografado com SSE ou SSE-C, qualquer configuração de criptografia em nível de bucket ou em nível de grade será ignorada.

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.

Informações relacionadas

"Gerenciar objetos com ILM"

"Operações em baldes"

"S3 operações rastreadas nos logs de auditoria"

"Usando criptografia do lado do servidor"

"Como as conexões do cliente podem ser configuradas"

COLOCAR Objeto - Copiar

Você pode usar a solicitação S3 PUT Object - Copy para criar uma cópia de um objeto que já está armazenado no S3. Uma operação PUT Object - Copy é a mesma que executar um GET e depois um PUT.

Resolução de conflitos

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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 StorageGRID suporta objetos de até 5 TB de tamanho.

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`

"Usando S3 Object Lock"

- 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

"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-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 especificar um comportamento de ingestão de confirmação dupla ou 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.

Usando x-amz-copy-source em PUT Object - Copy

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 COLOCAR Objeto - Copiar para criptografar um objeto existente no lugar ou para alterar a criptografia de um objeto existente no lugar. 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 você usar criptografia no lado do servidor, 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 PUT Object - Copy, para que o objeto possa ser descriptografado e copiado:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` `AES256` Especifique .
  - `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.

Atenção: 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 em "usar 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 no pedido COLOCAR Objeto - Copiar:
  - `x-amz-server-side-encryption`

Nota: 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` então retornará um valor "'null'".

Informações relacionadas

"Gerenciar objetos com ILM"

"Usando criptografia do lado do servidor"

"S3 operações rastreadas nos logs de auditoria"

"Objeto PUT"

Operações para uploads de várias partes

Esta seção descreve como o StorageGRID suporta operações para uploads de várias partes.

- "Listar carregamentos de várias partes"
- "Inicie o carregamento de várias peças"
- "Carregar artigo"
- "Carregar artigo - Copiar"
- "Concluir carregamento Multipart"

As seguintes condições e notas aplicam-se a todas as operações de carregamento em várias partes:

- Você não deve exceder 1.000 uploads simultâneos de várias partes para um único bucket, porque os resultados das consultas de uploads de várias partes 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 de peças grandes 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 comportamento de ingestão rigoroso ou equilibrado. 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, quando o upload multipart concluir algumas partes do objeto talvez não atendam aos requisitos atuais do ILM. Qualquer peça que não seja colocada corretamente está na fila para reavaliação ILM e é 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, 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 como um todo, todas as partes do objeto são movidas para DC1.
- Todas as operações de upload em várias partes suportam controles de consistência do StorageGRID.
- Conforme necessário, você pode usar a criptografia do lado do servidor com uploads de várias partes. Para usar o 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 de upload de múltiplas partes. 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 de carregamento de múltiplas partes Iniciar e em cada solicitação de peça de carregamento subsequente.

Operação	Implementação
Listar carregamentos Multipart	Consulte "Listar carregamentos Multipart"
Inicie o carregamento de várias peças	Consulte "Inicie o carregamento de várias peças"
Carregar artigo	Consulte "Carregar artigo"
Carregar artigo - Copiar	Consulte "Carregar artigo - Copiar"
Concluir carregamento Multipart	Consulte "Concluir carregamento Multipart"
Abortar carregamento Multipart	Implementado com todo o comportamento da API REST do Amazon S3
Listar peças	Implementado com todo o comportamento da API REST do Amazon S3

Informações relacionadas

"Controles de consistência"

"Usando criptografia do lado do servidor"

Listar carregamentos Multipart

A operação List Multipart uploads lista uploads em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

- `encoding-type`
- `max-uploads`
- `key-marker`
- `prefix`

- `upload-id-marker`

O `delimiter` parâmetro Request não é suportado.

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. Quando a operação completa de Upload Multipart é executada, esse é o ponto em que os objetos são criados (e versionados, se aplicável).

Inicie o carregamento de várias peças

A operação 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 a opção estrita para comportamento 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 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 nós de storage diferentes.

    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.

Atenção: 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 pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

Nota: 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.

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `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`

"Usando S3 Object Lock"

- 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`

"S3 operações e limitações suportadas pela API REST"

Para obter informações sobre como o StorageGRID lida com carateres UTF-8, consulte a documentação do PUT Object.

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 de carregamento de múltiplas partes se você quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações de Upload Part.
  - `x-amz-server-side-encryption`
- **SSE-C**: Use todos esses três cabeçalhos na solicitação de Upload Multipart iniciada (e em cada solicitação de Upload Part 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.

Atenção: 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 em "usar criptografia do lado do servidor".

Cabeçalhos de solicitação não suportados

O cabeçalho de solicitação a seguir não é suportado e retorna `XNotImplemented`

- `x-amz-website-redirect-location`

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 completa de Upload Multipart é executada.

Informações relacionadas

"Gerenciar objetos com ILM"

"Usando criptografia do lado do servidor"

"Objeto PUT"

Carregar artigo

A operação Upload Part carrega uma peça em um upload multipart para um objeto.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Length`
- `Content-MD5`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação de carregamento de múltiplas peças iniciada, você também deve incluir os seguintes cabeçalhos de solicitação em cada solicitação de Upload de peça:

- `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 Iniciar carregamento Multipart.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação de Envio de Multipart Iniciar.

> 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 em "usar 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 completa de Upload Multipart é executada.

Informações relacionadas

"Usando criptografia do lado do servidor"

Carregar artigo - Copiar

A operação Upload Part - Copy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação Upload Part - Copy é implementada com todo o comportamento da API REST do Amazon S3.

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 a criptografia SSE-C para a solicitação de carregamento de múltiplas partes, você também deve incluir os seguintes cabeçalhos de solicitação em cada peça de carregamento - solicitação de cópia:

- `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 Iniciar carregamento Multipart.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação de Envio de Multipart Iniciar.

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 de Upload Part - Copy, 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 em "usar 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 completa de Upload Multipart é executada.

Concluir carregamento Multipart

A operação completa de Upload Multipart completa um upload multipart de um objeto, montando as peças carregadas anteriormente.

Resolução de conflitos

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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 StorageGRID suporta objetos de até 5 TB de tamanho.

Cabeçalhos de solicitação

O `x-amz-storage-class` cabeçalho de solicitação é suportado e afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM correspondente especificar um comportamento de ingestão de confirmação dupla ou 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.

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.

Se isso ocorrer, um alarme é gerado no Gerenciador de Grade em Eventos totais (SMTT). A mensagem último evento exibe "'Falha ao publicar notificações para chave de bucket-naameobject'" para o último objeto cuja notificação falhou. (Para ver esta mensagem, selecione **nós *Storage Node* Eventos**. Veja o último evento no topo da tabela.) As mensagens de evento também são listadas em `/var/local/log/bycast-err.log`.

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.

Informações relacionadas

"Gerenciar objetos com ILM"

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

Nome	Status HTTP
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
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

Nome	Status HTTP
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
XBucketPolicyParseException	Falha ao analisar JSON da política de bucket recebida.	400 pedido incorreto
XComplianceConflict	Operação negada devido às configurações de conformidade legadas.	403 proibido
XComplianceReducedRedundancy Forbidden	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 da API REST do StorageGRID S3

Há operações adicionadas à API REST do S3 que são específicas do sistema StorageGRID.

OBTER pedido de consistência de balde

A solicitação GET Bucket Consistency permite determinar o nível de consistência que está sendo aplicado a um determinado bucket.

Os controles de consistência padrão são definidos 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Resposta

No XML de resposta `<Consistency>`, retornará um dos seguintes valores:

Controle de 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.

Controle de consistência	Descrição
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. Corresponde às garantias de consistência do Amazon S3. **Observação:** se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, defina o controle de consistência como "disponível", a menos que você exija garantias de consistência semelhantes ao Amazon S3.
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência "read-after-novo-write", mas apenas fornece consistência eventual para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

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

"Controles de consistência"

COLOCAR pedido consistência balde

A solicitação de consistência do PUT Bucket permite especificar o nível de consistência a ser aplicado às operações realizadas em um bucket.

Os controles de consistência padrão são definidos para garantir leitura após gravação para objetos recém-criados.

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:

Controle de 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. Corresponde às garantias de consistência do Amazon S3. **Observação:** se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, defina o controle de consistência como "disponível", a menos que você exija garantias de consistência semelhantes ao Amazon S3.
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência "read-after-novo-write", mas apenas fornece consistência eventual para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

Nota: em geral, você deve usar o valor de controle de 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 o controle de consistência para cada solicitação de API. Defina o controle de consistência no nível do balde apenas como último recurso.

Exemplo de solicitação

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Informações relacionadas

"Controles de consistência"

OBTER último pedido de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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>
```

COLOCAR o último pedido de 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, a caixa de seleção **S3 Buckets Change Last Access Setting** no Gerenciador de locatários ou na API de Gerenciamento do locatário.

Se as atualizações da última hora de acesso estiverem desativadas para um bucket, o seguinte comportamento é aplicado às operações no bucket:

- OBTER Objeto, OBTER ACL Objeto, OBTER marcação Objeto e solicitações Objeto HEAD não atualizam a última hora de acesso. O objeto não é adicionado às filas para avaliação do gerenciamento do ciclo de vida das informações (ILM).
- COLOCAR Objeto - Copiar e COLOCAR solicitações de marcação de objetos 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 o último tempo de acesso estiverem desativadas para o intervalo de origem, as solicitações COLOCAR Objeto - cópia não atualizam o último tempo 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, COLOCAR Objeto - solicitações de cópia sempre atualizam o último tempo de acesso. A cópia do objeto é adicionada às filas para avaliação ILM.
- Concluir a atualização de pedidos de carregamento de várias peças da última vez 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Este exemplo desativa a última hora de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Informações relacionadas

"Use uma conta de locatário"

EXCLUIR solicitação de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

OBTER solicitação de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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

Nome	Descrição	Obrigatório
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

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"

COLOCAR solicitação de 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

Nome	Descrição	Obrigatório
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

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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>
```

Informações relacionadas

"Use uma conta de locatário"

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

Observação: 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.

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 GET Service 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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

"Controles de consistência"

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 automaticamente quando você atualizar para o StorageGRID 11,5. 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.

"Usando S3 Object Lock"

"Gerenciar objetos com ILM"

"Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

Obsoleto: Modificações de solicitação de Bucket 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.

> 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.

"Usando S3 Object Lock"

"Gerenciar objetos com ILM"

"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 as modificações de solicitação DE armazenamento 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.
```

Informações relacionadas

"Gerenciar objetos com ILM"

"Use uma conta de locatário"

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.

"Usando S3 Object Lock"

"Gerenciar objetos com ILM"

"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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
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.

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.

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`.

Informações relacionadas

"Gerenciar objetos com ILM"

"Use uma conta de locatário"

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.

"Usando S3 Object Lock"

"Gerenciar objetos com ILM"

"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: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
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. **Atenção:** ao especificar um novo valor para RetentionPeriodMinutes, você deve especificar um valor igual ou maior que o período de retenção atual do bucket. Após o período de retenção do balde ser definido, não é possível diminuir esse valor; só é possível aumentá-lo.
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.

Nome	Descrição
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.

Nível de 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 o nível de 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 atingir o nível de 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 o nível de consistência **strong-site**.

> Nunca force o nível de 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 o nível de consistência é reduzido 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 um nível de consistência inferior, 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 do nível de consistência **strong-site**, reemita 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"

"Use uma conta de locatário"

"Gerenciar objetos com ILM"

Políticas de acesso ao bucket e ao grupo

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 configuradas usando a política OBTER bucket, COLOCAR bucket e EXCLUIR Bucket policy S3 operações de API. 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.

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 construídas usando esta estrutura para especificar permissões: Conceder efeito para permitir/negar que o principal execute Ação em recurso quando a condição se aplica.

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":"*"
```

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:iam:s3:::mybucket",
        "arn:aws:iam: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.

Informações relacionadas

"Use uma conta de locatário"

Configurações de controle de consistência para políticas

Por padrão, quaisquer atualizações feitas para políticas de grupo são eventualmente consistentes. Uma vez que 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 também são, eventualmente, 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 se torne efetiva o mais rápido possível por razões de segurança.

Nesse caso, você pode definir o `Consistency-Control` cabeçalho na solicitação de política COLOCAR balde ou usar a solicitação DE consistência COLOCAR balde. Ao alterar o controle de consistência para essa solicitação, você deve usar o valor **All**, que fornece a maior garantia de consistência de leitura após gravação. Se você especificar qualquer outro valor de controle de consistência em um cabeçalho para a solicitação DE consistência de armazenamento PUT, a solicitação será rejeitada. Se você especificar qualquer outro valor para uma solicitação DE política PUT Bucket, o valor será ignorado. Depois que uma política de bucket se tornar consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao armazenamento em cache de políticas.

> Se você definir o nível de consistência como **All** para forçar uma nova política de bucket a entrar em vigor mais cedo, certifique-se de definir o controle de nível de bucket de volta ao valor original quando terminar. Caso contrário, todas as futuras solicitações de bucket usarão a configuração **All**.

Usando o ARN nas 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 de política PUT Bucket deve ser codificado com charset UTF-8.

Especificando 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.

Informações relacionadas

"Especificando variáveis em uma política"

Especificando 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.

Especificando 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 de replicação PUT e DELETE Bucket. 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	COLOQUE o balde	
S3:DeleteBucket	ELIMINAR balde	
S3:DeleteBucketMetadataNotification	ELIMINAR configuração de notificação de metadados do bucket	Sim
S3:DeleteBucketPolicy	ELIMINAR política de balde	
S3:DeleteReplicationConfiguration	ELIMINAR replicação de balde	Sim, permissões separadas para COLOCAR e EXCLUIR*
S3:GetBucketAcl	OBTER ACL balde	
S3:GetBucketCompliance	OBTER conformidade com balde (obsoleto)	Sim
S3:GetBucketConsistência	OBTER consistência de balde	Sim
S3:GetBucketCORS	OBTER Bucket Cors	
S3:GetEncryptionConfiguration	OBTER criptografia Bucket	
S3:GetBucketLastAccessTime	OBTER último tempo de acesso do Bucket	Sim
S3:GetBucketLocation	OBTER localização do balde	
S3:GetBucketMetadataNotification	OBTER configuração de notificação de metadados do bucket	Sim
S3:GetBucketNotification	OBTER notificação Bucket	
S3:GetBucketObjectLockConfiguration	OBTER Configuração bloqueio Objeto	
S3:GetBucketPolicy	OBTER política Bucket	
S3:GetBucketTagging	OBTER marcação Bucket	
S3:GetBucketControle de versão	OBTENHA o controle de versão do Bucket	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetLifecycleConfiguration	OBTENHA o ciclo de vida do Bucket	
S3:GetReplicationConfiguration	OBTER replicação do bucket	
S3:ListAllMyBuckets	• Serviço GET • OBTER uso de armazenamento	Sim, para OBTER uso de armazenamento
S3: ListBucket	• OBTER balde (Listar objetos) • Balde DA cabeça • Restauração PÓS-objeto	
S3:ListBucketMultipartUploads	• Listar carregamentos Multipart • Restauração PÓS-objeto	
S3:ListBucketVersions	OBTER versões Bucket	
S3:PutBucketCompliance	COLOCAR conformidade com balde (obsoleto)	Sim
S3:PutBucketConsistência	COLOQUE a consistência do balde	Sim
S3:PutBucketCORS	• ELIMINAR Cors Bucket† • COLOQUE cors de balde	
S3:PutEncryptionConfiguration	• ELIMINAR encriptação Bucket • COLOQUE a criptografia Bucket	
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	COLOCAR notificação de balde	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:PutBucketObjectLockConfiguration	COLOCAR balde com o `x-amz-bucket-object-lock-enabled: true` cabeçalho de pedido (também requer a permissão S3:CreateBucket)	
S3:PutBucketPolicy	Política COLOCAR balde	
S3:PutBucketTagging	• ELIMINAR marcação de intervalo† • COLOQUE a marcação de balde	
S3:PutBucketControle de versão	COLOQUE o controle de versão do Bucket	
S3:PutLifecycleConfiguration	• ELIMINAR ciclo de vida do balde† • COLOQUE o ciclo de vida do balde	
S3:PutReplicationConfiguration	COLOQUE a replicação do balde	Sim, permissões separadas para COLOCAR e EXCLUIR*

Permissões que se aplicam a objetos

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:AbortMultipartUpload	• Abortar carregamento Multipart • Restauração PÓS-objeto	
S3:DeleteObject	• Objeto DELETE • Excluir vários objetos • Restauração PÓS-objeto	
S3:DeleteObjectTagging	ELIMINAR marcação Objeto	
S3:DeleteObjectVersionTagging	EXCLUIR marcação de objetos (uma versão específica do objeto)	
S3:DeleteObjectVersion	DELETE Object (uma versão específica do objeto)	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetObject	• Objeto GET • Objeto HEAD • Restauração PÓS-objeto	
S3:GetObjectAcl	OBTER ACL Objeto	
S3:GetObjectLegalHod	OBTER retenção legal Objeto	
S3:GetObjectRetention	OBTER retenção de objetos	
S3:GetObjectTagging	OBTER marcação Objeto	
S3:GetObjectVersionTagging	OBTER marcação de objetos (uma versão específica do objeto)	
S3:GetObjectVersion	OBTER Objeto (uma versão específica do objeto)	
S3:ListMultipartUploadParts	Listar Artigos, PÓS-restauração de objetos	
S3:PutObject	• Objeto PUT • COLOCAR Objeto - Copiar • Restauração PÓS-objeto • Inicie o carregamento de várias peças • Concluir carregamento Multipart • Carregar artigo • Carregar artigo - Copiar	
S3:PutObjectLegalHod	COLOCAR guarda legal Objeto	
S3:retenção de objetos Put	COLOCAR retenção Objeto	
S3:PutObjectTagging	Colocar marcação Objeto	
S3:PutObjectVersionTagging	COLOCAR marcação de objetos (uma versão específica do objeto)	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:PutOverwriteObject	• Objeto PUT • COLOCAR Objeto - Copiar • COLOQUE a marcação Objeto • ELIMINAR marcação Objeto • Concluir carregamento Multipart	Sim
S3:RestoreObject	Restauração PÓS-objeto	

Usando 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 substituir 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 do S3 estiver ativado, a configuração Negar impede que as operações de marcação DE objetos PUT ou DELETE 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 seleção **Prevent Client Modification** estiver selecionada (**Configuration Grid Options**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Informações relacionadas

"S3 exemplos de políticas de grupo"

Especificando 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: {
     <em>condition_type</em>: {
          <em>condition_key</em>: <em>condition_values</em>
```

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.

Operadores de condição	Descrição
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.
NumericGreaterThan	Compara uma chave com um valor numérico baseado na correspondência "'maior que".
NumericGreaterThanEquals	Compara uma chave com um valor numérico com base na correspondência "'maior que ou igual'".
NumericLessThan	Compara uma chave com um valor numérico baseado na correspondência "'menos que'".
NumericLessThanEquals	Compara uma chave com um valor numérico baseado na correspondência "'menor que ou igual".
Bool	Compara uma chave com um valor booleano baseado na correspondência "'true or false".
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

Categoria	Chaves de condição aplicáveis	Descrição
Operadores IP	AWS:SourceIp	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, uma vez que sua validade não pode ser determinada.
Recurso/identidade	aws:nome de usuário	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.
S3: ListBucket e. S3:ListBucketVersions Permissions	s3:delimitador	Irá comparar com o parâmetro delimitador especificado em uma solicitação OBTER bucket ou OBTER versões de Objeto bucket.
S3: ListBucket e. S3:ListBucketVersions Permissions	s3: teclas de max	Irá comparar-se com o parâmetro Max-keys especificado em uma solicitação GET Bucket ou GET Bucket Object Versions.
S3: ListBucket e. S3:ListBucketVersions Permissions	s3:prefixo	Irá comparar com o parâmetro de prefixo especificado em uma solicitação GET Bucket ou GET Bucket Object Versions.

Especificando 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.
`${s3:prefix}`	Usa a chave de prefixo específica do serviço como a variável fornecida.
`${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.

Criação de políticas que exigem manipulação 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
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

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento de StorageGRID
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 **Configuração Opções de Grade** e marque a caixa de seleção **impedir modificação de cliente**.
- 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 PUT Object ALLOW à política S3.

> ⓘ A configuração DeleteObject para NEGAR em uma política 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 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

"Gerenciar objetos com ILM"

"Criação de políticas que exigem manipulação especial"

"Como as regras do StorageGRID ILM gerenciam objetos"

"S3 exemplos de políticas de grupo"

S3 exemplos de políticas

Use os exemplos nesta seção para criar políticas de acesso ao StorageGRID para buckets e grupos.

S3 exemplos de política de bucket

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a diretiva está anexada. As políticas de bucket são configuradas usando a API S3 PutBucketPolicy.

Uma política de bucket pode ser configurada usando a AWS CLI de acordo com o seguinte comando:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
<em>file://policy.json</em>
```

Exemplo: Permita que todos acessem somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, podem listar objetos no bucket e executar operações Get Object em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que essa política pode não ser particularmente útil, já que 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 GET Object 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/*"
    }
  ]
}
```

Informações relacionadas

"Operações em baldes"

S3 exemplos de políticas de grupo

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, uma vez que está implícita. As políticas de grupo são configuradas usando o Gerenciador de inquilinos ou a API.

Exemplo: Definindo a política de grupo usando o Gerenciador do locatário

Ao usar o Gerenciador do Locatário para adicionar ou editar um grupo, você pode selecionar como deseja criar a política de grupo que define quais permissões de acesso S3 membros deste grupo terão, da seguinte forma:

- **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.
- **Custom**: Os usuários do grupo recebem as permissões que você especificar na caixa de texto.

  Neste exemplo, os membros do grupo só podem listar e acessar sua pasta específica (prefixo de chave) no intervalo especificado.

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}/*"
    }
  ]
}
```

Informações relacionadas

"Use uma conta de locatário"

"Usando a permissão PutOverwriteObject"

"Proteção WORM (write-once-read-many)"

Configurando a segurança para a API REST

Você deve analisar as medidas de segurança implementadas para a API REST e entender como proteger seu sistema.

Como o StorageGRID fornece segurança para a API REST

Você deve entender como o sistema StorageGRID implementa segurança, autenticação e autorização para a API REST.

O StorageGRID usa as seguintes medidas de segurança.

- As comunicações do cliente com o serviço Load Balancer usam HTTPS se o HTTPS estiver configurado para o ponto de extremidade do balanceador de carga.

  Quando você configura um ponto de extremidade do balanceador de carga, o HTTP pode ser habilitado opcionalmente. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

- Por padrão, o StorageGRID usa HTTPS para comunicações de clientes com nós de armazenamento e o serviço CLB em nós de gateway.

  O HTTP pode, opcionalmente, ser habilitado para essas conexões. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

  > O serviço CLB está obsoleto.

- 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

Os clientes podem se conetar ao serviço Load Balancer em nós de gateway ou nós de administrador, diretamente aos nós de storage ou ao serviço CLB em nós de gateway.

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 fazem isso usando o certificado que foi configurado para o ponto de extremidade do balanceador de carga específico usado para fazer a conexão. Cada endpoint tem seu próprio certificado, que é um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado que o administrador da grade gerou no StorageGRID ao configurar o endpoint.
- Quando os aplicativos cliente se conetam diretamente a um nó de armazenamento ou ao serviço CLB nos nós de gateway, 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.

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que usam para estabelecer conexões TLS.

Consulte as instruções de administração do StorageGRID para obter informações sobre a configuração de pontos de extremidade do balanceador de carga e para obter instruções sobre como adicionar um único certificado de servidor personalizado para conexões TLS diretamente aos nós de armazenamento ou ao serviço CLB nos nós de gateway.

Resumo

A tabela a seguir mostra como os problemas de segurança são implementados nas APIs REST S3 e Swift:

Problema de segurança	Implementação da API REST
Segurança da ligação	TLS

Problema de segurança	Implementação da API REST
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: Conta S3 (ID da chave de acesso e chave de acesso secreta) • Swift: Conta Swift (nome de usuário e senha)
Autorização do cliente	• S3: Propriedade do bucket e todas as políticas de controle de acesso aplicáveis • Swift: Acesso à função de administrador

Informações relacionadas

"Administrar o StorageGRID"

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto limitado de conjuntos de codificação que os aplicativos clientes podem usar ao estabelecer uma sessão de Segurança da camada de Transporte (TLS).

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.

Suítes de cifra suportadas

Versão TLS	IANA nome do conjunto de cifra
1,2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1,2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
1,2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1,3	TLS_AES_256_GCM_SHA384
1,3	TLS_CHACHA20_POLY1305_SHA256
1,3	TLS_AES_128_GCM_SHA256

Conjuntos de codificação obsoletos

Os seguintes conjuntos de codificação são obsoletos. O suporte para essas cifras será removido em uma

versão futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informações relacionadas

"Como as conexões do cliente podem ser configuradas"

Operações de monitoramento e auditoria

Você pode monitorar workloads e eficiências das operações do cliente visualizando tendências de transações para toda a grade ou para nós específicos. Você pode usar mensagens de auditoria para monitorar operações e transações do cliente.

- "Monitoramento de taxas de ingestão e recuperação de objetos"
- "Acesso e revisão de logs de auditoria"

Monitoramento de taxas de ingestão e recuperação de objetos

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.

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. No painel de instrumentos, localize a secção Protocol Operations (operações de protocolo).

   Esta seção resume o número de operações do cliente realizadas pelo seu sistema StorageGRID. As taxas de protocolo são médias nos últimos dois minutos.

3. Selecione **nós**.
4. Na página inicial dos nós (nível de implantação), clique na guia **Load Balancer**.

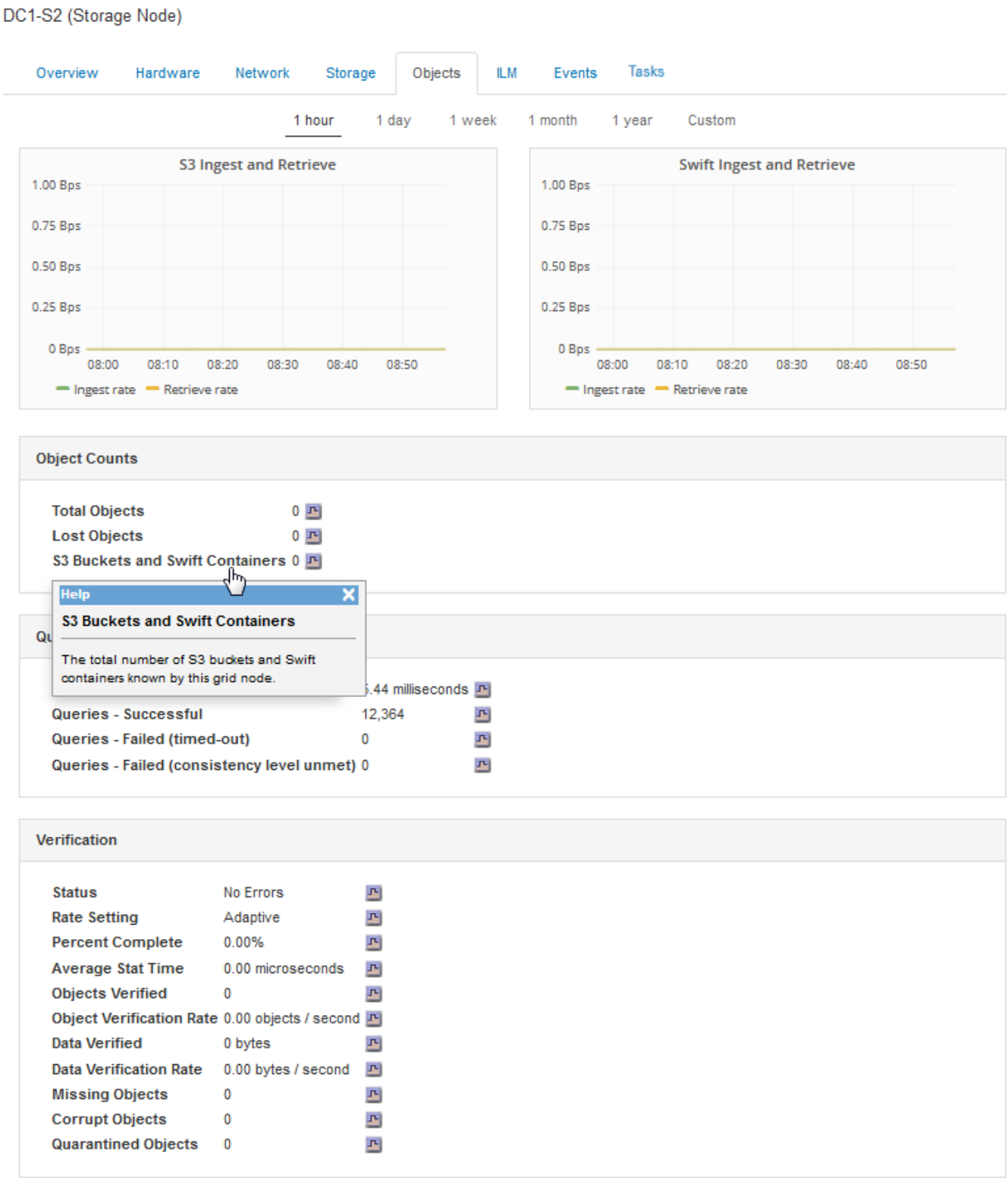
   Os gráficos mostram tendências para todo o tráfego do cliente direcionado para pontos de extremidade do balanceador de carga dentro da grade. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

5. Na home page dos nós (nível de implantação), clique na guia **objetos**.

   O gráfico mostra as taxas de ingestão e recuperação de todo o seu sistema StorageGRID em bytes por segundo e total de bytes. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

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

O gráfico mostra as taxas de ingestão e recuperação de objetos para este nó de armazenamento. A guia também inclui métricas para contagens de objetos, consultas e verificação. Você pode clicar nos rótulos para ver as definições dessas métricas.



7. Se você quiser ainda mais detalhes:
   a. Selecione **Support** > **Tools** > **Grid Topology**.
   b. Selecione ***site*** **Visão geral Principal**.

A seção operações da API exibe informações resumidas para toda a grade.

c. Selecione ***Storage Node* LDR *client Application* Overview Main**

A seção operações exibe informações resumidas para o nó de armazenamento selecionado.

Acesso e revisão de logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. As mensagens de auditoria específicas da API nos logs de auditoria fornecem dados críticos de monitoramento de segurança, operação e desempenho que podem ajudá-lo a avaliar a integridade do sistema.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Sobre esta tarefa

O arquivo de log de auditoria ativo é `audit.log` chamado , e é armazenado em nós de administração.

Uma vez por dia, o arquivo audit.log ativo é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato *`yyyy-mm-dd.txt`*.

Após um dia, o arquivo salvo é compactado e renomeado, no formato *`yyyy-mm-dd.txt.gz`*, que preserva a data original.

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
```

Passos

1. Faça login em um nó Admin:
   a. Digite o seguinte comando
   `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:

   ```
   cd /var/local/audit/export
   ```

3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

S3 operações rastreadas nos logs de auditoria

Várias operações de bucket e operações de objetos são rastreadas nos logs de auditoria do StorageGRID.

Operações de bucket rastreadas nos logs de auditoria

- ELIMINAR balde
- ELIMINAR marcação de intervalo
- Excluir vários objetos
- OBTER balde (Listar objetos)
- OBTER versões Objeto balde
- OBTER marcação Bucket
- Balde DA cabeça
- COLOQUE o balde
- COLOQUE a conformidade do balde
- COLOQUE a marcação de balde
- COLOQUE o controle de versão do Bucket

Operações de objeto rastreadas nos logs de auditoria

- Concluir carregamento Multipart
- Carregar artigo (quando a regra ILM usa os comportamentos de ingestão rigorosos ou equilibrados)
- Carregar artigo - Copiar (quando a regra ILM usa os comportamentos de ingestão estritos ou equilibrados)
- Objeto DELETE
- Objeto GET
- Objeto HEAD
- Restauração PÓS-objeto
- Objeto PUT
- COLOCAR Objeto - Copiar

Informações relacionadas

"Operações em baldes"

"Operações em objetos"

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

Informações relacionadas

- "Benefícios de manter conexões HTTP ociosas abertas"
- "Benefícios de conexões HTTP ativas"
- "Benefícios de conexões HTTP simultâneas"
- "Separação de pools de conexão HTTP para operações de leitura e gravação"

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 ou ao serviço CLB (obsoleto) em nós de Gateway, 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 armazenamento ou ao serviço CLB, limitar conexões HTTP ativas fornece os seguintes benefícios:

- Permite o balanceamento de carga ideal em todo o sistema StorageGRID.

  Ao usar o serviço CLB, você deve evitar conexões TCP/IP de longa duração para otimizar o

balanceamento de carga em todo o sistema StorageGRID. Você deve configurar aplicativos cliente para controlar a duração de cada conexão HTTP e fechar a conexão HTTP após um tempo definido para que a conexão HTTP possa ser restabelecida e reequilibrada.

O serviço CLB equilibra a carga em todo o sistema StorageGRID no momento em que um aplicativo cliente estabelece uma conexão HTTP. 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.

O serviço CLB está obsoleto.

- 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.

Use Swift

Saiba como os aplicativos clientes podem usar a API OpenStack Swift para fazer interface com o sistema StorageGRID.

- "Suporte à API OpenStack Swift no StorageGRID"
- "Configurando contas de locatário e conexões"
- "Operações suportadas pela API REST Swift"
- "Operações da API REST do StorageGRID Swift"
- "Configurando a segurança para a API REST"
- "Operações de monitoramento e auditoria"

Suporte à API OpenStack Swift no StorageGRID

O StorageGRID suporta as seguintes versões específicas do Swift e HTTP.

Item	Versão
Especificação Swift	API de storage de objetos OpenStack Swift v1 em novembro de 2015
HTTP	1,1 para obter mais informações sobre HTTP, consulte HTTP/1,1 (RFCs 7230-35). **Nota**: O StorageGRID não suporta a canalização HTTP/1,1.

Informações relacionadas

"OpenStack: API de storage de objetos"

Histórico do suporte à API Swift no StorageGRID

Você deve estar ciente das alterações no suporte do sistema StorageGRID para a API REST Swift.

Solte	Comentários
11,5	Removido o controle de consistência fraca. O nível de consistência disponível será usado em vez disso.
11,4	Adicionado suporte para TLS 1,3 e lista atualizada de pacotes de criptografia TLS suportados. O CLB está obsoleto. Adicionada descrição da inter-relação entre ILM e a configuração de consistência.
11,3	Operações PUT Object atualizadas para descrever o impactos das regras de ILM que usam o posicionamento síncrono na ingestão (as opções equilibradas e rigorosas para o comportamento de ingestão). Adicionada descrição das conexões de cliente que usam pontos de extremidade do balanceador de carga ou grupos de alta disponibilidade. Lista atualizada dos conjuntos de encriptação TLS suportados. As cifras TLS 1,1 não são mais suportadas.
11,2	Pequenas alterações editoriais ao documento.
11,1	Adicionado suporte para o uso de HTTP para conexões de cliente Swift para nós de grade. Atualizadas as definições dos controles de consistência.
11,0	Adicionado suporte para 1.000 contentores para cada conta de locatário.
10,3	Atualizações administrativas e correções do documento. Seções removidas para configurar certificados de servidor personalizados.
10,2	Suporte inicial da API Swift pelo sistema StorageGRID. A versão atualmente suportada é a API de armazenamento de objetos OpenStack Swift v1.

Como o StorageGRID implementa a API Swift REST

Um aplicativo cliente pode usar chamadas de API REST do Swift para se conetar a nós de storage e nós de Gateway para criar contentores e armazenar e recuperar objetos. Isso permite que aplicativos orientados a serviços desenvolvidos para o OpenStack Swift se conetem com storage de objetos no local fornecido pelo sistema StorageGRID.

Gerenciamento de objetos Swift

Depois que os objetos Swift foram ingeridos no sistema StorageGRID, eles são gerenciados pelas regras de gerenciamento do ciclo de vida da informação (ILM) na política ativa de ILM do sistema. As regras e a política do ILM determinam como o StorageGRID cria e distribui cópias de dados de objetos e como gerencia essas cópias ao longo do tempo. Por exemplo, uma regra ILM pode se aplicar a objetos em contentores Swift específicos e pode especificar que várias cópias de objetos sejam salvas em vários data centers por um certo número de anos.

Entre em Contato com o administrador do StorageGRID se você precisar entender como as regras e políticas do ILM da grade afetarão os objetos em sua conta de locatário do Swift.

Solicitações de cliente conflitantes

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O momento para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes Swift iniciam uma operação.

Garantias de consistência e controles

Por padrão, o StorageGRID fornece consistência de leitura após gravação para objetos recém-criados e consistência para atualizações de objetos e operações HEAD. 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.

O StorageGRID também permite que você controle a consistência por contentor. Você pode alterar o controle de consistência para fazer uma troca entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de storage e sites, conforme necessário pela aplicação.

Informações relacionadas

"Gerenciar objetos com ILM"

"OBTER solicitação de consistência de contêiner"

"COLOQUE o pedido de consistência do recipiente"

Recomendações para a implementação da API Swift REST

Você deve seguir estas recomendações ao implementar a API REST do Swift para uso com o StorageGRID.

Recomendações para heads to non-existent objects

Se seu aplicativo verifica rotineiramente para ver se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o controle de consistência ""disponível"". Por exemplo, você

deve usar o controle de consistência "disponível" se seu aplicativo executar uma operação DE CABEÇA para um local antes de executar uma OPERAÇÃO DE COLOCAÇÃO nesse local.

Caso contrário, se a operação PRINCIPAL não encontrar o objeto, você poderá receber um número alto de 500 erros de servidor interno se um ou mais nós de storage não estiverem disponíveis.

Você pode definir o controle de consistência "disponível" para cada recipiente usando o pedido de consistência de contentor PUT.

Recomendações para nomes de objetos

Você não deve usar valores aleatórios como os primeiros quatro carateres de nomes de objetos. Em vez disso, você deve usar prefixos não aleatórios, não exclusivos, como imagem.

Se você precisar usar carateres aleatórios e exclusivos em prefixos de nome de objeto, você deve prefixar os nomes de objeto com um nome de diretório. Ou seja, use este formato:

```
mycontainer/mydir/f8e3-image3132.jpg
```

Em vez deste formato:

```
mycontainer/f8e3-image3132.jpg
```

Recomendações para "leituras de intervalo"

Se a opção **Compress Stored Objects** estiver selecionada (**Configuration System Settings Grid Options**), os aplicativos cliente Swift devem evitar executar operações de objeto GET que especificam um intervalo de bytes que serão retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é muito 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.

Informações relacionadas

"OBTER solicitação de consistência de contêiner"

"COLOQUE o pedido de consistência do recipiente"

"Administrar o StorageGRID"

Configurando contas de locatário e conexões

Configurar o StorageGRID para aceitar conexões de aplicativos cliente requer a criação de uma ou mais contas de locatário e a configuração das conexões.

Criando e configurando contas de locatário Swift

Uma conta de locatário Swift é necessária antes que os clientes da API Swift possam armazenar e recuperar objetos no StorageGRID. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários, além de contentores e objetos.

As contas de locatário Swift são criadas por um administrador de grade do StorageGRID usando o Gerenciador de grade ou a API de gerenciamento de grade.

Ao criar uma conta de locatário Swift, o administrador da grade especifica as seguintes informações:

- Nome de exibição para o locatário (o ID da conta do locatário é atribuído automaticamente e não pode ser alterado)
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).
- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.
- Se o SSO estiver ativado, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.

Depois que uma conta de locatário Swift for criada, os usuários com a permissão de acesso root podem acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e criando grupos e usuários locais
- Monitoramento do uso do storage

> Os usuários Swift devem ter a permissão de acesso root para acessar o Gerenciador do locatário. No entanto, a permissão de acesso root não permite que os usuários se autentiquem na API REST do Swift para criar contentores e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

Informações relacionadas

"Administrar o StorageGRID"

"Use uma conta de locatário"

"Endpoints de API Swift compatíveis"

Como as conexões do cliente podem ser configuradas

Um administrador de grade faz escolhas de configuração que afetam a forma como os clientes Swift se conetam ao StorageGRID para armazenar e recuperar dados. As informações específicas que você precisa para fazer uma conexão dependem da configuração escolhida.

Os aplicativos clientes podem armazenar ou recuperar objetos conetando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway, ou, opcionalmente, o endereço IP virtual de um grupo de alta disponibilidade (HA) de nós de administração ou nós de gateway
- O serviço CLB em nós de Gateway, ou, opcionalmente, o endereço IP virtual de um grupo de nós de

gateway de alta disponibilidade

> O serviço CLB está obsoleto. Os clientes configurados antes da versão do StorageGRID 11,3 podem continuar a usar o serviço CLB nos nós de gateway. Todos os outros aplicativos clientes que dependem do StorageGRID para fornecer balanceamento de carga devem se conetar usando o serviço de balanceamento de carga.

- Nós de storage, com ou sem um balanceador de carga externo

Ao configurar o StorageGRID, um administrador de grade pode usar o Gerenciador de grade ou a API de gerenciamento de grade para executar as seguintes etapas, todas opcionais:

1. Configure endpoints para o serviço Load Balancer.

   Você deve configurar endpoints para usar o serviço Load Balancer. O serviço Load Balancer em nós de administração ou nós de gateway distribui conexões de rede recebidas de aplicativos clientes para nós de storage. Ao criar um endpoint de balanceador de carga, o administrador do StorageGRID especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).

2. Configurar redes de clientes não confiáveis.

   Se um administrador do StorageGRID configurar a rede cliente de um nó para não ser confiável, o nó só aceita conexões de entrada na rede cliente em portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

3. Configurar grupos de alta disponibilidade.

   Se um administrador criar um grupo de HA, as interfaces de rede de vários nós de Admin ou nós de Gateway serão colocadas em uma configuração de backup ativo. As conexões de cliente são feitas usando o endereço IP virtual do grupo HA.

Para obter mais informações sobre cada opção, consulte as instruções para administrar o StorageGRID.

Resumo: Endereços IP e portas para conexões de clientes

Os aplicativos cliente se conetam ao StorageGRID usando o endereço IP de um nó de grade e o número da porta de um serviço nesse nó. Se os grupos de alta disponibilidade (HA) estiverem configurados, os aplicativos clientes poderão se conetar usando o endereço IP virtual do grupo HA.

Informações necessárias para fazer conexões com o cliente

A 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. Contate o administrador do StorageGRID para obter mais informações ou consulte as instruções de administração do StorageGRID para obter uma descrição de como localizar essas informações 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 de extremidade do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Grupo HA	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas Swift padrão: • HTTPS: 8083 • HTTP: 8085
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	• Porta de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	• Porta de extremidade do balanceador de carga
Nó de gateway	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP do nó de gateway **Nota:** por padrão, as portas HTTP para CLB e LDR não estão ativadas.	Portas Swift padrão: • HTTPS: 8083 • HTTP: 8085
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas Swift padrão: • HTTPS: 18083 • HTTP: 18085

Exemplo

Para conetar um cliente Swift ao endpoint 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 192.0.2.6 e o número da porta de um endpoint do Swift Load Balancer for 10444, um cliente Swift poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.6:10444`

É possível configurar um nome DNS para o endereço IP que os clientes usam para se conetar ao StorageGRID. Contacte o administrador da rede local.

Decidir usar conexões HTTPS ou HTTP

Quando as conexões de cliente são feitas usando um endpoint de Load Balancer, as conexões devem ser feitas usando o protocolo (HTTP ou HTTPS) especificado para esse endpoint. Para usar HTTP para conexões de cliente a nós de armazenamento ou ao serviço CLB em nós de gateway, você deve habilitar seu uso.

Por padrão, quando os aplicativos cliente se conetam a nós de armazenamento ou ao serviço CLB nos nós de Gateway, eles devem usar HTTPS criptografado para todas as conexões. Opcionalmente, você pode habilitar

conexões HTTP menos seguras selecionando a opção de grade **Ativar conexão HTTP** no Gerenciador de Grade. Por exemplo, um aplicativo cliente pode usar HTTP ao testar a conexão com um nó de armazenamento em um ambiente que não seja de produção.

> Tenha cuidado ao ativar o HTTP para uma grade de produção, já que as solicitações serão enviadas sem criptografia.

> O serviço CLB está obsoleto.

Se a opção **Enable HTTP Connection** estiver selecionada, os clientes devem usar portas diferentes para HTTP do que para HTTPS. Consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Testando sua conexão na configuração da API Swift

Você pode usar o Swift CLI para testar sua conexão com o sistema StorageGRID e verificar se você pode ler e gravar objetos no sistema.

O que você vai precisar

- Você deve ter baixado e instalado Python-swiftclient, o cliente de linha de comando Swift.
- Você deve ter uma conta de locatário Swift no sistema StorageGRID.

Sobre esta tarefa

Se você não tiver configurado a segurança, você deve adicionar o `--insecure` sinalizador a cada um desses comandos.

Passos

1. Consulte o URL de informações para sua implantação do StorageGRID Swift:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

   Isso é suficiente para testar se sua implantação do Swift está funcional. Para testar ainda mais a configuração da conta armazenando um objeto, continue com as etapas adicionais.

2. Coloque um objeto no recipiente:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Obtenha o contentor para verificar o objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Eliminar o objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Eliminar o recipiente:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

Informações relacionadas

"Criando e configurando contas de locatário Swift"

"Configurando a segurança para a API REST"

Operações suportadas pela API REST Swift

O sistema StorageGRID dá suporte à maioria das operações na API OpenStack Swift. Antes de integrar clientes API REST do Swift com o StorageGRID, revise os detalhes de implementação para operações de conta, contentor e objeto.

Operações suportadas no StorageGRID

As seguintes operações da API Swift são suportadas:

- "Operações de conta"
- "Operações de contêiner"
- "Operações de objetos"

Cabeçalhos de resposta comuns para todas as operações

O sistema StorageGRID implementa todos os cabeçalhos comuns para operações com suporte, conforme definido pela API de armazenamento de objetos OpenStack Swift v1.

Informações relacionadas

"OpenStack: API de storage de objetos"

Endpoints de API Swift compatíveis

O StorageGRID oferece suporte aos seguintes endpoints da API Swift: O URL de informações, o URL de autenticação e o URL de armazenamento.

URL de informações

Você pode determinar os recursos e limitações da implementação do StorageGRID Swift emitindo uma solicitação GET para o URL base do Swift com o caminho /info.

```
https://FQDN | Node IP:Swift Port/info/
```

No pedido:

- *FQDN* é o nome de domínio totalmente qualificado.
- *Node IP* É o endereço IP do nó de armazenamento ou do nó de gateway na rede StorageGRID.
- *Swift Port* É o número de porta usado para conexões Swift API no nó de armazenamento ou nó de gateway.

Por exemplo, o seguinte URL de informações solicitaria informações de um nó de armazenamento com o endereço IP de 10.99.106.103 e usando a porta 18083.

```
https://10.99.106.103:18083/info/
```

A resposta inclui os recursos da implementação Swift como um dicionário JSON. Uma ferramenta cliente pode analisar a resposta JSON para determinar os recursos da implementação e usá-los como restrições para operações de armazenamento subsequentes.

A implementação do StorageGRID do Swift permite o acesso não autenticado ao URL de informações.

URL de autenticação

Um cliente pode usar o URL de autenticação Swift para autenticar como usuário de conta de locatário.

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

Você deve fornecer o ID da conta do locatário, o nome de usuário e a senha como parâmetros nos `X-Auth-User` cabeçalhos e `X-Auth-Key` da solicitação, da seguinte forma:

```
X-Auth-User: Tenant_Account_ID:Username

X-Auth-Key: Password
```

Nos cabeçalhos de solicitação:

- *`Tenant_Account_ID`* É o ID de conta atribuído pelo StorageGRID quando o locatário Swift foi criado. Esse é o mesmo ID de conta de locatário usado na página de login do Gerenciador do Locatário.
- *`Username`* É o nome de um usuário do locatário que foi criado no Gerenciador do Locatário. Esse usuário deve pertencer a um grupo que tenha a permissão Swift Administrator. O usuário raiz do locatário não pode ser configurado para usar a API REST do Swift.

  Se a Federação de identidade estiver ativada para a conta de locatário, forneça o nome de usuário e a senha do usuário federado do servidor LDAP. Em alternativa, forneça o nome de domínio do utilizador LDAP. Por exemplo:

  ```
  X-Auth-User: Tenant_Account_ID:Username@Domain_Name
  ```

- *`Password`* é a senha para o usuário do locatário. As senhas de usuário são criadas e gerenciadas no Gerenciador do locatário.

A resposta a uma solicitação de autenticação bem-sucedida retorna um URL de armazenamento e um token de autenticação, como segue:

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID

X-Auth-Token: token

X-Storage-Token: token
```

Por padrão, o token é válido por 24 horas a partir do tempo de geração.

Os tokens são gerados para uma conta de locatário específica. Um token válido para uma conta não autoriza um usuário a acessar outra conta.

URL de armazenamento

Um aplicativo cliente pode emitir chamadas de API REST Swift para executar operações de conta, contentor e objeto com suporte em um nó de gateway ou nó de storage. As solicitações de armazenamento são endereçadas ao URL de armazenamento retornado na resposta de autenticação. A solicitação também deve incluir o cabeçalho X-Auth-Token e o valor retornado da solicitação de autenticação.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID

[/container][/object]

X-Auth-Token: token
```

Alguns cabeçalhos de resposta de armazenamento que contêm estatísticas de uso podem não refletir números precisos para objetos modificados recentemente. Pode levar alguns minutos para que números precisos apareçam nesses cabeçalhos.

Os cabeçalhos de resposta a seguir para operações de conta e contentor são exemplos daqueles que contêm estatísticas de uso:

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Informações relacionadas

"Como as conexões do cliente podem ser configuradas"

"Criando e configurando contas de locatário Swift"

"Operações de conta"

"Operações de contêiner"

"Operações de objetos"

Operações de conta

As seguintes operações da API Swift são realizadas em contas.

OBTER conta

Esta operação recupera a lista de contentores associada às estatísticas de uso de conta e conta.

É necessário o seguinte parâmetro de pedido:

- `Account`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes parâmetros de consulta de solicitação suportados são opcionais:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Prefix`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta HTTP/1,1 204 no content" se a conta for encontrada e não tiver contentores ou a lista de contentores estiver vazia; ou uma resposta HTTP/1,1 200 OK se a conta for encontrada e a lista de contentores não estiver vazia:

- `Accept-Ranges`

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Conta principal

Esta operação recupera informações de conta e estatísticas de uma conta Swift.

É necessário o seguinte parâmetro de pedido:

- `Account`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "'HTTP/1,1 204 no Content'":

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Informações relacionadas

"Operações rápidas rastreadas nos logs de auditoria"

Operações de contêiner

O StorageGRID suporta um máximo de 1.000 contentores por conta Swift. As seguintes operações da API Swift são executadas em contentores.

ELIMINAR recipiente

Esta operação remove um contentor vazio de uma conta Swift em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 204 sem conteúdo":

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

PEGUE o recipiente

Esta operação recupera a lista de objetos associada ao contentor juntamente com estatísticas de contentor e metadados em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes parâmetros de consulta de solicitação suportados são opcionais:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Path`
- `Prefix`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 200 success" ou "HTTP/1,1 204 no content":

- `Accept-Ranges`
- `Content-Length`

- `Content-Type`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Recipiente DA cabeça

Esta operação recupera estatísticas de contentor e metadados de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 204 sem conteúdo":

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

COLOQUE o recipiente

Esta operação cria um contentor para uma conta em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 201 criado" ou "HTTP/1,1 202 aceito" (se o contentor já existir sob esta conta):

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

Um nome de contêiner deve ser exclusivo no namespace StorageGRID. Se o contentor existir sob outra conta, o seguinte cabeçalho é retornado: "Conflito HTTP/1,1 409".

Informações relacionadas

"Operações rápidas rastreadas nos logs de auditoria"

Operações de objetos

As seguintes operações da API Swift são executadas em objetos.

ELIMINAR objeto

Esta operação exclui o conteúdo e os metadados de um objeto do sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`
- `Object`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos de resposta com uma `HTTP/1.1 204 No Content` resposta:

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Ao processar uma solicitação DE EXCLUSÃO de objetos, 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.

Para obter mais informações sobre como os objetos são excluídos, consulte as instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

OBTER objeto

Esta operação recupera o conteúdo do objeto e obtém os metadados do objeto de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`
- `Object`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes cabeçalhos de solicitação são opcionais:

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com `HTTP/1.1 200 OK` uma resposta:

- `Accept-Ranges`
- `Content-Disposition`, retornada somente se `Content-Disposition` os metadados tiverem sido definidos
- `Content-Encoding`, retornada somente se `Content-Encoding` os metadados tiverem sido definidos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

Objeto PRINCIPAL

Esta operação recupera metadados e propriedades de um objeto ingerido a partir de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`
- `Object`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 200 OK":

- `Accept-Ranges`
- `Content-Disposition`, retornada somente se `Content-Disposition` os metadados tiverem sido definidos
- `Content-Encoding`, retornada somente se `Content-Encoding` os metadados tiverem sido definidos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

COLOQUE o objeto

Essa operação cria um novo objeto com dados e metadados ou substitui um objeto existente por dados e metadados em um sistema StorageGRID.

O StorageGRID suporta objetos de até 5 TB de tamanho.

> As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O momento para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes Swift iniciam uma operação.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`
- `Object`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes cabeçalhos de solicitação são opcionais:

- `Content-Disposition`
- `Content-Encoding`

  Não use em pedaços `Content-Encoding` se a regra ILM que se aplica a um objeto filtra objetos com

base no tamanho e usa o posicionamento síncrono na ingestão (as opções balanceadas ou rigorosas para o comportamento de ingestão).

- `Transfer-Encoding`

  Não use compactado ou dividido `Transfer-Encoding` se a regra ILM que se aplica a um objeto filtra objetos com base no tamanho e usa o posicionamento síncrono na ingestão (as opções balanceadas ou rigorosas para o comportamento de ingestão).

- `Content-Length`

  Se uma regra de ILM filtrar objetos por tamanho e usar o posicionamento síncrono na ingestão, você deverá especificar `Content-Length`.

  > Se você não seguir estas diretrizes para `Content-Encoding`, `Transfer-Encoding` e `Content-Length`, o StorageGRID deve salvar o objeto antes que ele possa determinar o tamanho do objeto e aplicar a regra ILM. Em outras palavras, o StorageGRID deve criar cópias provisórias de um objeto na ingestão. Ou seja, o StorageGRID deve usar a opção de confirmação dupla para o comportamento de ingestão.

  Para obter mais informações sobre o posicionamento síncrono e as regras de ILM, consulte as instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (metadados relacionados a objetos)

  Se você quiser usar a opção **tempo de criação definido pelo usuário** como tempo de referência para uma regra ILM, você deve armazenar o valor em um cabeçalho definido pelo usuário chamado `X-Object-Meta-Creation-Time`. Por exemplo:

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  Este campo é avaliado em segundos desde 1 de janeiro de 1970.

- `X-Storage-Class: reduced_redundancy`

  Esse cabeçalho afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM que corresponde a um objeto ingerido especificar um comportamento de ingestão de confirmação dupla ou equilibrada.

  - **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.

    O `reduced_redundancy` cabeçalho é melhor usado 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.

O uso do `reduced_redundancy` cabeçalho não é recomendado em outras circunstâncias porque aumenta o risco de perda de dados de objetos 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.

Observe que 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 pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 201 criado":

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Trans-Id`

Informações relacionadas

"Gerenciar objetos com ILM"

"Operações rápidas rastreadas nos logs de auditoria"

Pedido de OPÇÕES

A SOLICITAÇÃO DE OPÇÕES verifica a disponibilidade de um serviço Swift individual. A SOLICITAÇÃO DE OPÇÕES é processada pelo nó de armazenamento ou nó de gateway especificado no URL.

Método de OPÇÕES

Por exemplo, os aplicativos clientes podem emitir uma SOLICITAÇÃO DE OPÇÕES para a porta Swift em um nó de armazenamento, sem fornecer credenciais de autenticação Swift, para determinar se o nó de armazenamento está disponível. Você pode usar essa solicitação para monitoramento ou para permitir que balanceadores de carga externos identifiquem quando um nó de storage está inativo.

Quando usado com o URL info ou o URL de armazenamento, o método OPTIONS retorna uma lista de verbos suportados para o URL dado (por exemplo, HEAD, GET, OPTIONS E PUT). O método DE OPÇÕES não pode ser usado com o URL de autenticação.

É necessário o seguinte parâmetro de pedido:

- `Account`

Os seguintes parâmetros de pedido são opcionais:

- `Container`
- `Object`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta HTTP/1,1 204 no content". A SOLICITAÇÃO DE OPÇÕES para o URL de armazenamento não exige que o destino exista.

- `Allow` (Uma lista de verbos suportados para o URL dado, por exemplo, HEAD, GET, OPTIONS e PUT)
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Informações relacionadas

"Endpoints de API Swift compatíveis"

Respostas de erro às operações da API Swift

Entender as possíveis respostas de erro pode ajudá-lo a solucionar problemas de operações.

Os seguintes códigos de status HTTP podem ser retornados quando erros ocorrem durante uma operação:

Nome de erro Swift	Status HTTP
AccountNameToLong, ContainerNameToLong, HeaderToBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameToLong, MetadataValueToBig, MissingSecurityHeader, ObjectNameToLong, ToManyContainers, ToManyMetadataItems, TotalMetataTooLarge	400 pedido incorreto
AccessDenied	403 proibido
ContainerNotEmpty, ContainerAlreadyExists	409 conflito
InternalError (erro internacional)	500 erro interno do servidor
Intervalo Invalidável	416 intervalo solicitado não satisfatório
MetodNotAlloved	Método 405 não permitido
MissingContentLength	411 comprimento necessário

Nome de erro Swift	Status HTTP
Não encontrado	404 não encontrado
Sem Implementado	501 não implementado
Pré-condiçãoFailed	412 Pré-condição falhou
ResourceNotFound	404 não encontrado
Não autorizado	401 não autorizado
UnprocessableEntity	422 entidade não processável

Operações da API REST do StorageGRID Swift

Há operações adicionadas à API REST do Swift que são específicas do sistema StorageGRID.

OBTER solicitação de consistência de contêiner

O nível de consistência faz uma troca entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós e sites de storage. A solicitação GET Container Consistency permite que você determine o nível de consistência que está sendo aplicado a um contentor específico.

Pedido

Solicitar cabeçalho HTTP	Descrição
`X-Auth-Token`	Especifica o token de autenticação Swift para a conta a ser usada para a solicitação.
`x-ntap-sg-consistency`	Especifica o tipo de solicitação, onde `true` OBTÉM consistência de contentor e `false` OBTÉM contentor.
`Host`	O nome do host para o qual a solicitação é direcionada.

Exemplo de solicitação

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Resposta

Cabeçalho HTTP de resposta	Descrição
`Date`	A data e a hora da resposta.
`Connection`	Se a conexão com o servidor está aberta ou fechada.
`X-Trans-Id`	O identificador de transação exclusivo para a solicitação.
`Content-Length`	O comprimento do corpo de resposta.
`x-ntap-sg-consistency`	O nível de controle de consistência que está sendo aplicado ao recipiente. Os seguintes valores são suportados: • **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**: 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. **Nota**: Se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, use o nível "disponível". • **Available** (eventual consistência para OPERAÇÕES DE CABEÇA): Comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações DE CABEÇA. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis.

Exemplo de resposta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

Informações relacionadas

"Use uma conta de locatário"

COLOQUE o pedido de consistência do recipiente

A solicitação de consistência de contentor PUT permite especificar o nível de consistência a ser aplicado às operações realizadas em um contentor. Por padrão, novos contentores são criados usando o nível de consistência "read-after-new-write".

Pedido

Solicitar cabeçalho HTTP	Descrição
`X-Auth-Token`	O token de autenticação Swift para a conta a ser usada para a solicitação.

Solicitar cabeçalho HTTP	Descrição
`x-ntap-sg-consistency`	O nível de controle de consistência a aplicar às operações no recipiente. Os seguintes valores são suportados: • **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**: 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. **Nota**: Se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, use o nível "disponível". • **Available** (eventual consistência para OPERAÇÕES DE CABEÇA): Comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações DE CABEÇA. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis.
`Host`	O nome do host para o qual a solicitação é direcionada.

Como os controles de consistência e as regras de ILM interagem para afetar a proteção de dados

Tanto a sua escolha de controle de consistência quanto a sua regra ILM afetam a forma como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, o controle de consistência usado 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 nível de consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Strict**: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido ao cliente.
- **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.
- * Commit duplo*: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

> Antes de selecionar o comportamento de ingestão para uma regra ILM, leia a descrição completa dessas configurações nas instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Exemplo de como o controle de consistência e a regra ILM podem interagir

Suponha que você tenha uma grade de dois locais com a seguinte regra ILM e a seguinte configuração de nível de consistência:

- **Regra ILM**: Crie duas cópias de objeto, uma no local e outra em um local remoto. O comportamento de ingestão estrita é selecionado.
- **Nível de consistência**: "Trong-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 o nível de consistência "site-trong", o cliente poderá receber uma mensagem de sucesso depois que os dados do objeto forem 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 níveis de consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Exemplo de solicitação

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Resposta

Cabeçalho HTTP de resposta	Descrição
`Date`	A data e a hora da resposta.
`Connection`	Se a conexão com o servidor está aberta ou fechada.
`X-Trans-Id`	O identificador de transação exclusivo para a solicitação.
`Content-Length`	O comprimento do corpo de resposta.

Exemplo de resposta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Informações relacionadas

"Use uma conta de locatário"

Configurando a segurança para a API REST

Você deve analisar as medidas de segurança implementadas para a API REST e entender como proteger seu sistema.

Como o StorageGRID fornece segurança para a API REST

Você deve entender como o sistema StorageGRID implementa segurança, autenticação e autorização para a API REST.

O StorageGRID usa as seguintes medidas de segurança.

- As comunicações do cliente com o serviço Load Balancer usam HTTPS se o HTTPS estiver configurado para o ponto de extremidade do balanceador de carga.

  Quando você configura um ponto de extremidade do balanceador de carga, o HTTP pode ser habilitado opcionalmente. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

- Por padrão, o StorageGRID usa HTTPS para comunicações de clientes com nós de armazenamento e o serviço CLB em nós de gateway.

  O HTTP pode, opcionalmente, ser habilitado para essas conexões. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

O serviço CLB está obsoleto.

- 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

Os clientes podem se conetar ao serviço Load Balancer em nós de gateway ou nós de administrador, diretamente aos nós de storage ou ao serviço CLB em nós de gateway.

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 fazem isso usando o certificado que foi configurado para o ponto de extremidade do balanceador de carga específico usado para fazer a conexão. Cada endpoint tem seu próprio certificado, que é um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado que o administrador da grade gerou no StorageGRID ao configurar o endpoint.
- Quando os aplicativos cliente se conetam diretamente a um nó de armazenamento ou ao serviço CLB nos nós de gateway, 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.

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que usam para estabelecer conexões TLS.

Consulte as instruções de administração do StorageGRID para obter informações sobre a configuração de pontos de extremidade do balanceador de carga e para obter instruções sobre como adicionar um único certificado de servidor personalizado para conexões TLS diretamente aos nós de armazenamento ou ao serviço CLB nos nós de gateway.

Resumo

A tabela a seguir mostra como os problemas de segurança são implementados nas APIs REST S3 e Swift:

Problema de segurança	Implementação da API REST
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: Conta S3 (ID da chave de acesso e chave de acesso secreta) • Swift: Conta Swift (nome de usuário e senha)

Problema de segurança	Implementação da API REST
Autorização do cliente	• S3: Propriedade do bucket e todas as políticas de controle de acesso aplicáveis • Swift: Acesso à função de administrador

Informações relacionadas

"Administrar o StorageGRID"

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto limitado de conjuntos de codificação que os aplicativos clientes podem usar ao estabelecer uma sessão de Segurança da camada de Transporte (TLS).

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.

Suítes de cifra suportadas

Versão TLS	IANA nome do conjunto de cifra
1,2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1,3	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Conjuntos de codificação obsoletos

Os seguintes conjuntos de codificação são obsoletos. O suporte para essas cifras será removido em uma versão futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informações relacionadas

"Como as conexões do cliente podem ser configuradas"

Operações de monitoramento e auditoria

Você pode monitorar workloads e eficiências das operações do cliente visualizando tendências de transações para toda a grade ou para nós específicos. Você pode usar mensagens de auditoria para monitorar operações e transações do cliente.

Monitoramento de taxas de ingestão e recuperação de objetos

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.

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. No painel de instrumentos, localize a secção Protocol Operations (operações de protocolo).

   Esta seção resume o número de operações do cliente realizadas pelo seu sistema StorageGRID. As taxas de protocolo são médias nos últimos dois minutos.

3. Selecione **nós**.
4. Na página inicial dos nós (nível de implantação), clique na guia **Load Balancer**.

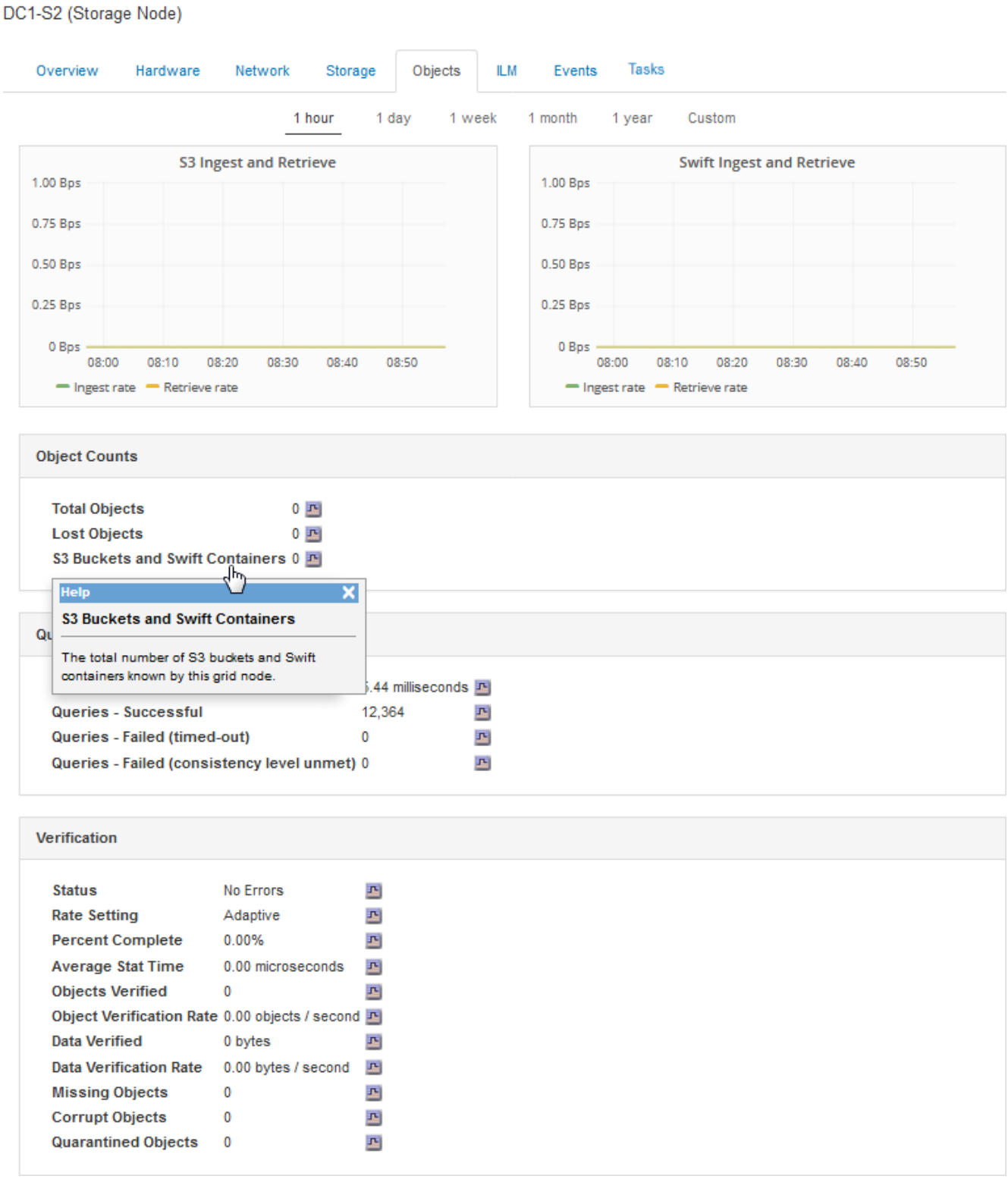
   Os gráficos mostram tendências para todo o tráfego do cliente direcionado para pontos de extremidade do balanceador de carga dentro da grade. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

5. Na home page dos nós (nível de implantação), clique na guia **objetos**.

   O gráfico mostra as taxas de ingestão e recuperação de todo o seu sistema StorageGRID em bytes por segundo e total de bytes. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

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

   O gráfico mostra as taxas de ingestão e recuperação de objetos para este nó de armazenamento. A guia também inclui métricas para contagens de objetos, consultas e verificação. Você pode clicar nos rótulos para ver as definições dessas métricas.



7. Se você quiser ainda mais detalhes:
   a. Selecione **Support** > **Tools** > **Grid Topology**.
   b. Selecione ***site* Visão geral Principal**.

      A seção operações da API exibe informações resumidas para toda a grade.

   c. Selecione ***Storage Node* LDR *client Application* Overview Main**

A seção operações exibe informações resumidas para o nó de armazenamento selecionado.

Acesso e revisão de logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. As mensagens de auditoria específicas da API nos logs de auditoria fornecem dados críticos de monitoramento de segurança, operação e desempenho que podem ajudá-lo a avaliar a integridade do sistema.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Sobre esta tarefa

O arquivo de log de auditoria ativo é `audit.log` chamado , e é armazenado em nós de administração.

Uma vez por dia, o arquivo audit.log ativo é salvo e um novo arquivo audit.log é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato `yyyy-mm-dd.txt`.

Após um dia, o arquivo salvo é compactado e renomeado, no formato `yyyy-mm-dd.txt.gz`, que preserva a data original.

Este exemplo mostra o arquivo audit.log ativo, o arquivo do dia anterior (2018-04-15.txt) e o arquivo compactado para o dia anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:`cd /var/local/audit/export`
3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

Informações relacionadas

"Rever registos de auditoria"

Operações rápidas rastreadas nos logs de auditoria

Todas as operações bem-sucedidas de EXCLUSÃO, RECEBIMENTO, CABEÇALHO, POST e PUT DE armazenamento são rastreadas no log de auditoria do StorageGRID. As falhas não são registradas, nem são solicitações de informações, autenticação ou OPÇÕES.

Consulte *Entendendo mensagens de auditoria* para obter detalhes sobre as informações rastreadas para as

seguintes operações do Swift.

Operações de conta

- OBTER conta
- Conta principal

Operações de contêiner

- ELIMINAR recipiente
- PEGUE o recipiente
- Recipiente DA cabeça
- COLOQUE o recipiente

Operações de objetos

- ELIMINAR objeto
- OBTER objeto
- Objeto PRINCIPAL
- COLOQUE o objeto

Informações relacionadas

"Rever registos de auditoria"

"Operações de conta"

"Operações de contêiner"

"Operações de objetos"

Monitorar e solucionar problemas

Monitorar um sistema StorageGRID

Saiba como monitorar um sistema StorageGRID e como avaliar problemas que possam ocorrer. Lista todos os alertas do sistema.

- "Usando o Gerenciador de Grade para monitoramento"
- "Informações que você deve monitorar regularmente"
- "Gerenciamento de alertas e alarmes"
- "Utilizar a monitorização SNMP"
- "A recolher dados StorageGRID adicionais"
- "Solução de problemas de um sistema StorageGRID"
- "Referência de alertas"
- "Referência de alarmes (sistema legado)"
- "Referência de ficheiros de registo"

Usando o Gerenciador de Grade para monitoramento

O Gerenciador de Grade é a ferramenta mais importante para monitorar seu sistema StorageGRID. Esta seção apresenta o Painel do Gerenciador de Grade e fornece informações detalhadas sobre as páginas de nós.

- "Requisitos do navegador da Web"
- "Visualização do Dashboard"
- "Exibindo a página de nós"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

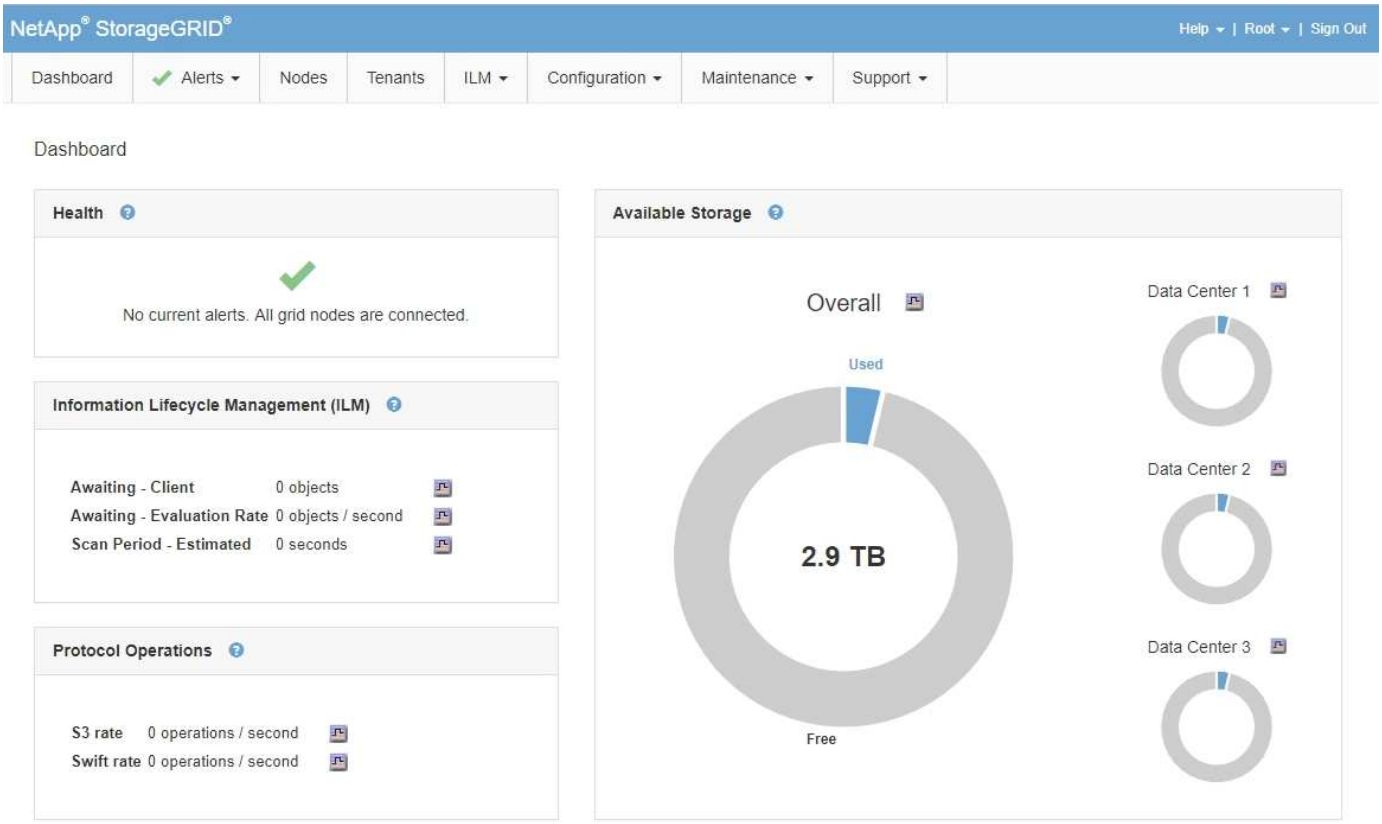
Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024

Largura do navegador	Pixels
Ótimo	1280

Visualização do Dashboard

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



Painel de saúde

Descrição	Veja detalhes adicionais	Saiba mais
Resume a saúde do sistema. Uma marca de seleção verde significa que não há alertas atuais e todos os nós de grade estão conetados. Qualquer outro ícone significa que há pelo menos um alerta atual ou nó desconetado.	Você pode ver um ou mais dos seguintes links: • **Detalhes da grade**: Aparece se algum nó estiver desconetado (estado de conexão desconhecido ou administrativamente inativo). Clique no link ou clique no ícone azul ou cinza para determinar que nó ou nós são afetados. • **Alertas atuais**: Aparece se algum alerta estiver ativo no momento. Clique no link ou clique em **Crítica**, **Principal** ou **menor** para ver os detalhes na página **Alertas atual**. • **Alertas resolvidos recentemente**: Aparece se algum alerta acionado na semana passada estiver resolvido. Clique no link para ver os detalhes na página **Alertas resolvido**. • **Alarms Legacy**: Aparece se algum alarme (sistema legado) estiver ativo no momento. Clique no link para ver os detalhes na página **suporte Alarmes (legado) Alarmes atuais**. • **Licença**: Aparece se houver um problema com a licença de software para este sistema StorageGRID. Clique no link para ver os detalhes na página **Manutenção sistema Licença**.	• "Monitorização dos estados de ligação do nó" • "Visualização de alertas atuais" • "Visualização de alertas resolvidos" • "Visualização de alarmes legados" • "Administrar o StorageGRID"

Painel de armazenamento disponível

Descrição	Veja detalhes adicionais	Saiba mais
Exibe a capacidade de armazenamento disponível e usada em toda a grade, não incluindo Mídia de arquivamento. O gráfico geral apresenta totais em toda a grade. Se esta for uma grade de vários locais, gráficos adicionais serão exibidos para cada local do data center. Você pode usar essas informações para comparar o armazenamento usado com o armazenamento disponível. Se você tem uma grade de vários locais, você pode determinar qual site está consumindo mais armazenamento.	• Para visualizar a capacidade, coloque o cursor sobre as seções de capacidade disponível e usada do gráfico. • Para exibir tendências de capacidade em um intervalo de datas, clique no ícone de gráfico da grade geral ou em um local de data center. • Para ver detalhes, selecione **nós**. Em seguida, exiba a guia Storage (armazenamento) para toda a grade, um site inteiro ou um nó de armazenamento único.	• "Visualizar o separador armazenamento" • "Monitoramento da capacidade de armazenamento"

Painel ILM (Information Lifecycle Management)

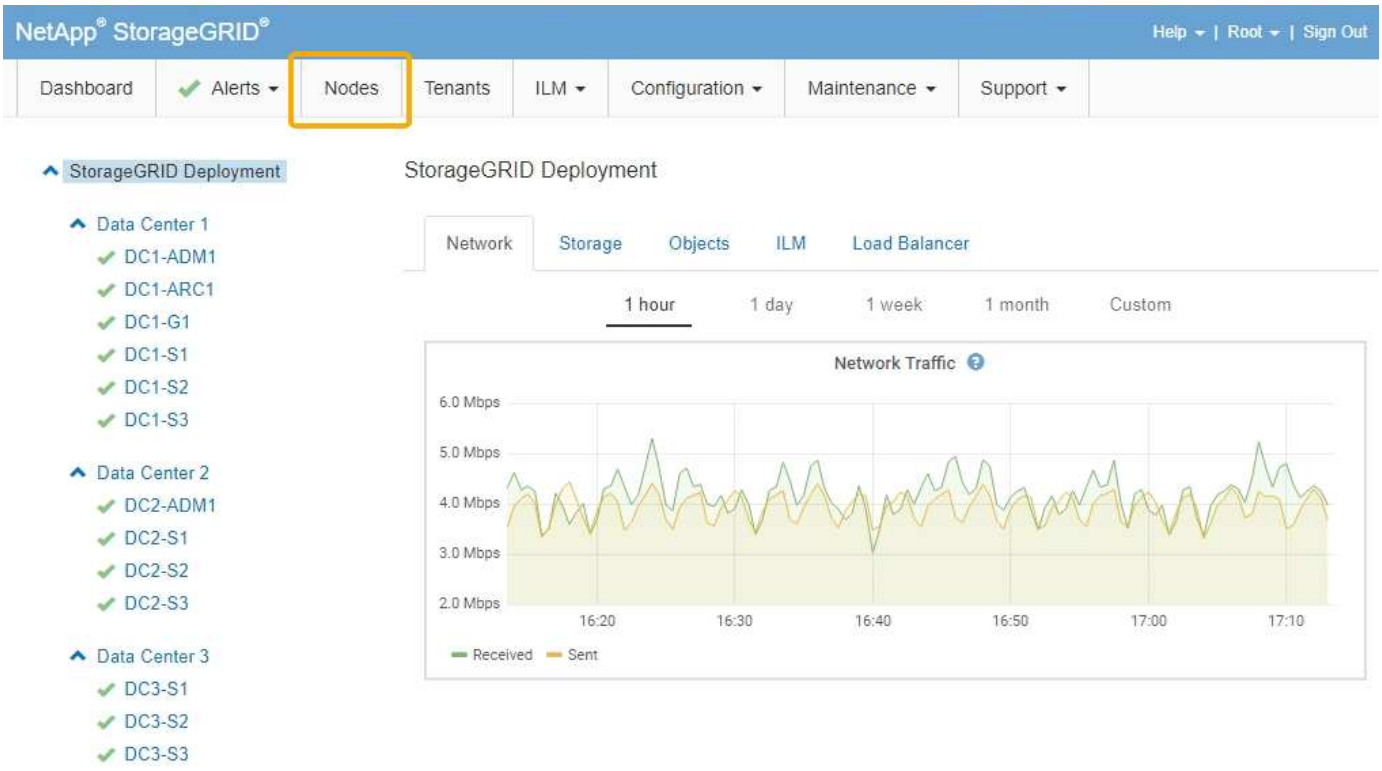
Descrição	Veja detalhes adicionais	Saiba mais
Exibe as operações ILM atuais e as filas ILM para o seu sistema. Você pode usar essas informações para monitorar a carga de trabalho do sistema. • **Aguardando - Cliente**: O número total de objetos aguardando avaliação ILM das operações do cliente (por exemplo, ingest). • **Aguardando - taxa de avaliação**: A taxa atual na qual os objetos são avaliados em relação à política ILM na grade. • **Período de digitalização - estimado**: O tempo estimado para concluir uma varredura ILM completa de todos os objetos. **Nota:** Uma verificação completa não garante que o ILM tenha sido aplicado a todos os objetos.	• Para ver detalhes, selecione **nós**. Em seguida, exiba a guia ILM para toda a grade, um site inteiro ou um nó de armazenamento único. • Para ver as regras existentes do ILM, selecione **ILM Rules**. • Para ver as políticas ILM existentes, selecione **ILM Policies**.	• "Visualizar o separador ILM" • "Administrar o StorageGRID".

Painel Protocol Operations (operações de protocolo)

Descrição	Veja detalhes adicionais	Saiba mais
Exibe o número de operações específicas do protocolo (S3 e Swift) executadas pelo seu sistema. Use essas informações para monitorar os workloads e a eficiência do sistema. As taxas de protocolo são médias nos últimos dois minutos.	• Para ver detalhes, selecione **nós**. Em seguida, exiba a guia objetos para toda a grade, um site inteiro ou um nó de armazenamento único. • Para ver tendências ao longo de um intervalo de datas, clique no ícone de gráfico à direita da taxa de protocolo S3 ou Swift.	• "Exibindo a guia objetos" • "Use S3" • "Use Swift"

Exibindo a página de nós

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



Na exibição em árvore à esquerda, você pode ver todos os sites e todos os nós no seu sistema StorageGRID. O ícone de cada nó indica se o nó está conetado ou se há alertas ativos.

Ícones de estado da ligação

Se um nó for desconetado da grade, a exibição em árvore mostrará um ícone de estado de conexão azul ou cinza, e não o ícone de alertas subjacentes.

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

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

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

Ícones de alerta

Se um nó estiver conetado à grade, a exibição em árvore mostrará um dos ícones a seguir, dependendo se houver algum alerta atual para o nó.

- **Crítico** : existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido.
- **Major** : existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não pare a operação normal de um nó ou serviço StorageGRID.
- **Minor** : o sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.
- **Normal** : nenhum alerta está ativo e o nó está conetado à grade.

Exibindo detalhes de um sistema, site ou nó

Para visualizar as informações disponíveis, clique nos links apropriados à esquerda, como segue:

- Selecione o nome da grade para ver um resumo agregado das estatísticas de todo o seu sistema StorageGRID. (A captura de tela mostra um sistema chamado implantação do 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.

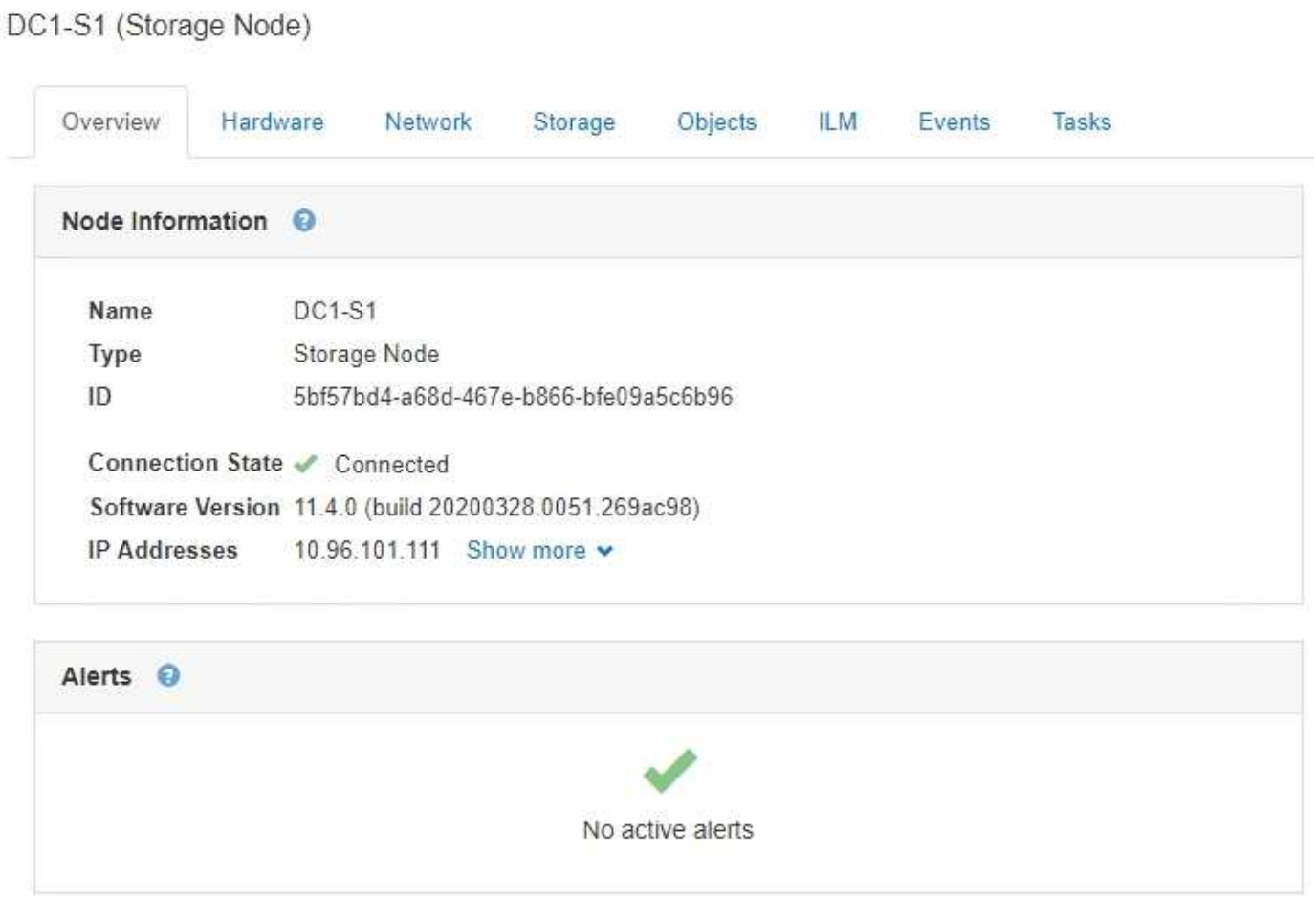
Exibindo a guia Visão geral

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

A guia Visão geral é mostrada para todos os nós.

Informações do nó

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

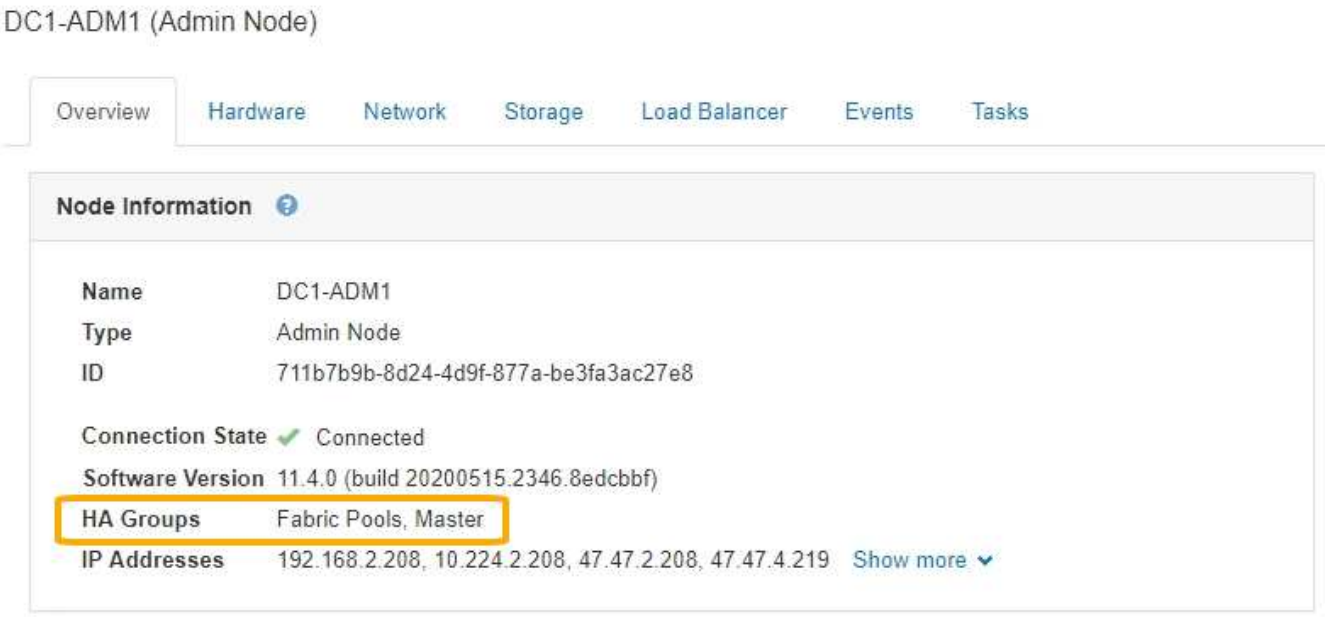


As informações de visão geral de um nó incluem o seguinte:

- **Nome**: O nome do host atribuído ao nó e exibido no Gerenciador de Grade.
- **Tipo**: O tipo de nó — nó Admin, nó de armazenamento, nó de gateway ou nó de arquivo.
- **ID**: O identificador exclusivo para o nó, que também é conhecido como UUID.
- **Estado da conexão**: Um dos três estados. É apresentado o ícone para o estado mais grave.
  - **Não conetado - desconhecido** : o nó não está conetado à grade por um motivo desconhecido. Por exemplo, a conexão de rede entre nós foi perdida ou a energia está inativa. O alerta **não é possível se comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos. Esta situação requer atenção imediata.

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

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



- **Endereços IP**: Os endereços IP do nó. Clique em **Mostrar mais** para visualizar os endereços IPv4 e IPv6 do nó e mapeamentos de interface:
  - eth0: Rede de rede
  - eth1: Rede de administração
  - Eth2: Rede de Clientes

Alertas

A seção Alertas da guia Visão geral lista todos os alertas que atualmente afetam esse nó que não foram silenciados. Clique no nome do alerta para ver detalhes adicionais e ações recomendadas.

Informações relacionadas

"Monitorização dos estados de ligação do nó"

"Visualização de alertas atuais"

"Visualizar um alerta específico"

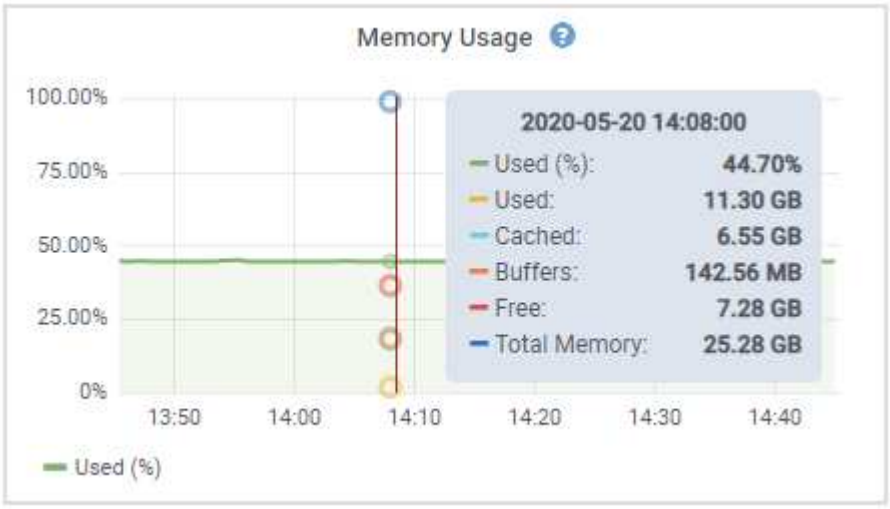
Exibindo a guia hardware

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

A guia hardware é exibida para todos os nós.

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

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



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

Informações relacionadas

"Exibição de informações sobre os nós de storage do dispositivo"

"Exibindo informações sobre nós de administração do dispositivo e nós de gateway"

Visualizar o separador 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.

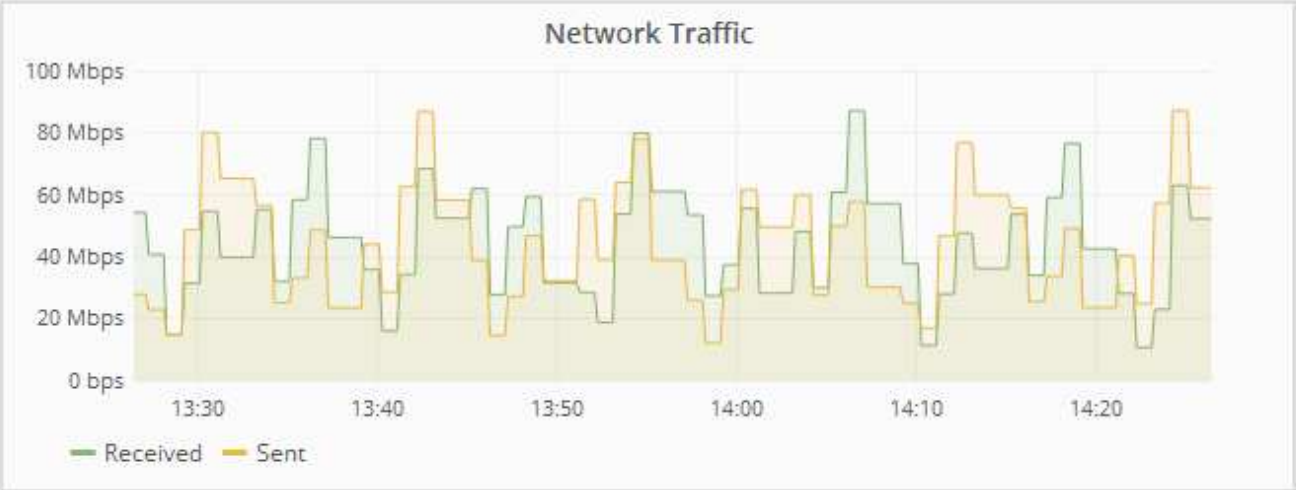
Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico ou gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.

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

DC1-S1-226 (Storage Node)

Overview | Hardware | Network | Storage | Objects | ILM | Events

1 hour | 1 day | 1 week | 1 month | 1 year | Custom



Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	00:50:56:A8:2A:75	10 Gigabit	Full	Off	Up

Network Communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	738.858 GB	904,587,345	0	14,340	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	677.555 GB	465,715,998	0	0	0	0

Informações relacionadas

"Monitoramento de conexões de rede e desempenho"

Visualizar o separador armazenamento

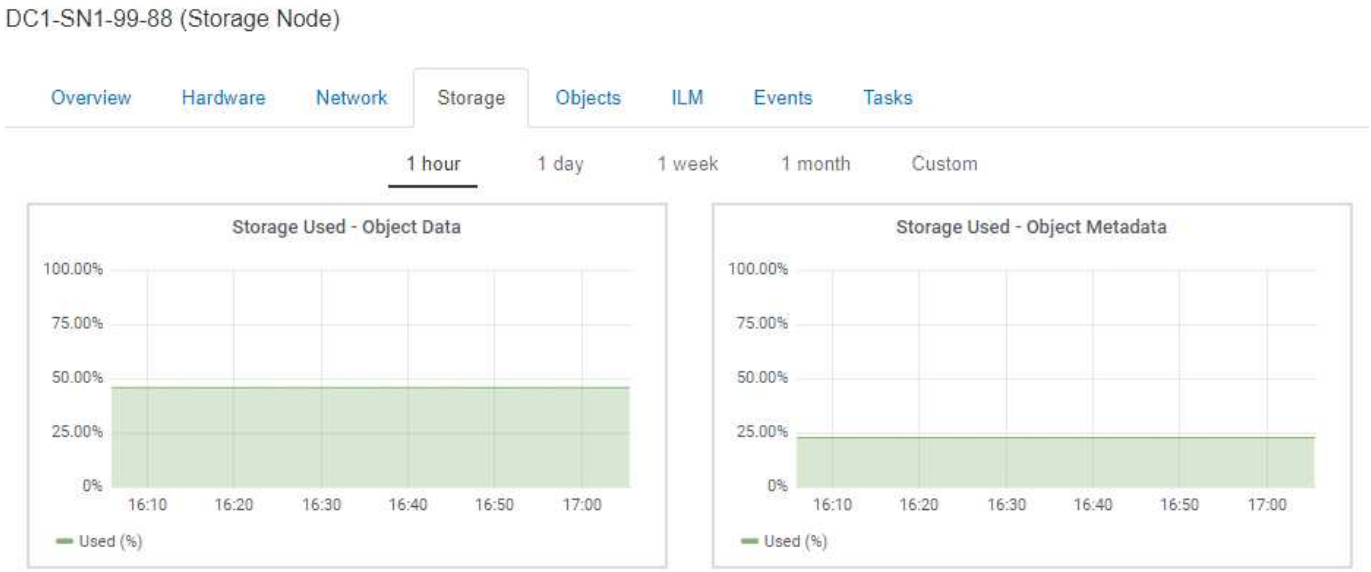
A guia armazenamento resume a disponibilidade de armazenamento e outras métricas de armazenamento.

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

Armazenamento de gráficos usados

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

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



Dispositivos de disco, volumes e tabelas de armazenamento de objetos

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	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 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

"Monitoramento da capacidade de armazenamento para toda a grade"

"Monitoramento da capacidade de storage para cada nó de storage"

"Monitoramento da capacidade dos metadados de objetos para cada nó de storage"

Visualizar o separador Eventos

A guia Eventos exibe uma contagem de qualquer erro de sistema ou eventos de falha para um nó, incluindo erros como erros de rede.

A guia Eventos é exibida para todos os nós.

Se você tiver problemas com um nó específico, poderá usar a guia Eventos para saber mais sobre o problema. O suporte técnico também pode usar as informações na guia Eventos para ajudar na solução de problemas.

Você pode executar essas tarefas na guia Eventos:

- Use as informações mostradas para o campo **último evento** na parte superior da tabela para determinar qual evento ocorreu mais recentemente.
- Clique no ícone do gráfico para um evento específico para ver quando esse evento ocorreu ao longo do tempo.

- Redefinir contagens de eventos para zero depois de resolver quaisquer problemas.

Informações relacionadas

"Monitoramento de eventos"

"Apresentação de gráficos e gráficos"

"Repor contagens de eventos"

Usando a guia tarefa para reinicializar um nó de grade

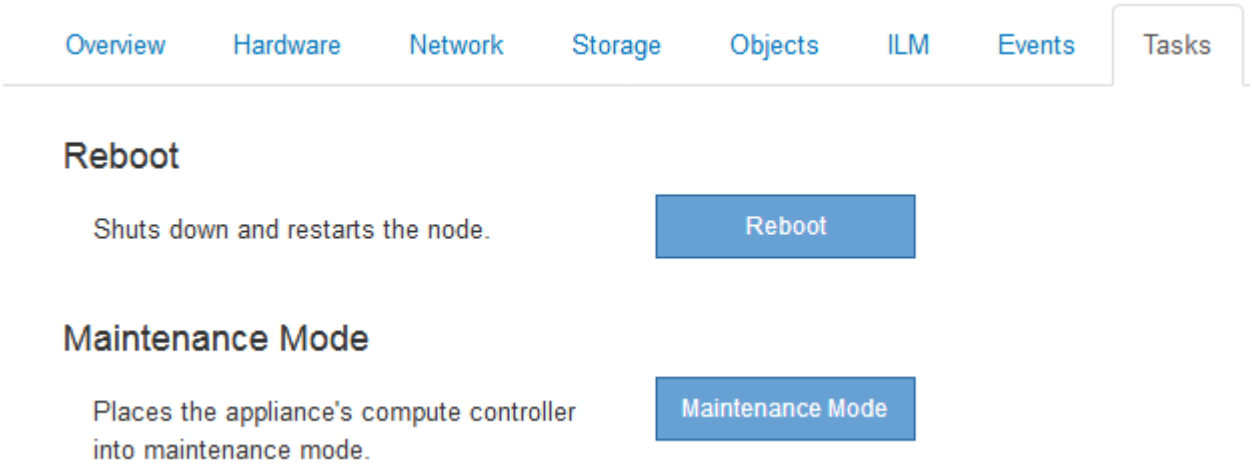
A guia tarefa permite reinicializar o nó selecionado. A guia tarefa é mostrada para todos os nós.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.

Sobre esta tarefa

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



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

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

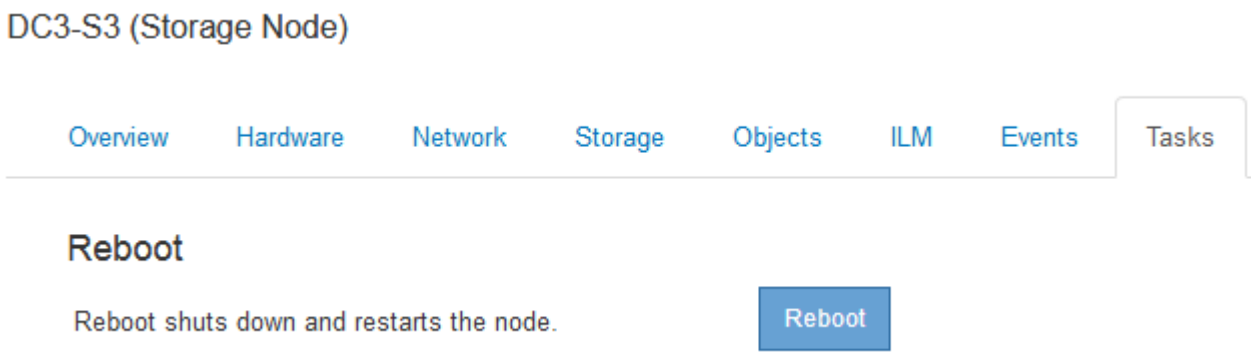
  - Se uma regra ILM especificar um comportamento de ingestão de confirmação dupla ou a regra especificar balanceado e não for possível criar imediatamente todas as cópias necessárias, o StorageGRID enviará imediatamente quaisquer objetos recém-ingeridos a dois nós de armazenamento no mesmo local e avaliará o ILM posteriormente. Se você quiser reinicializar dois ou mais nós de storage em um determinado site, talvez não seja possível acessar esses objetos durante a reinicialização.
  - Para garantir que você possa acessar todos os objetos enquanto um nó de armazenamento estiver reiniciando, pare de ingerir objetos em um site por aproximadamente uma hora antes de reiniciar o nó.

- Talvez seja necessário colocar um dispositivo StorageGRID no modo de manutenção para executar determinados procedimentos, como alterar a configuração do link ou substituir um controlador de armazenamento. Para obter instruções, consulte as instruções de instalação e manutenção do equipamento.

> Colocar um aparelho no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

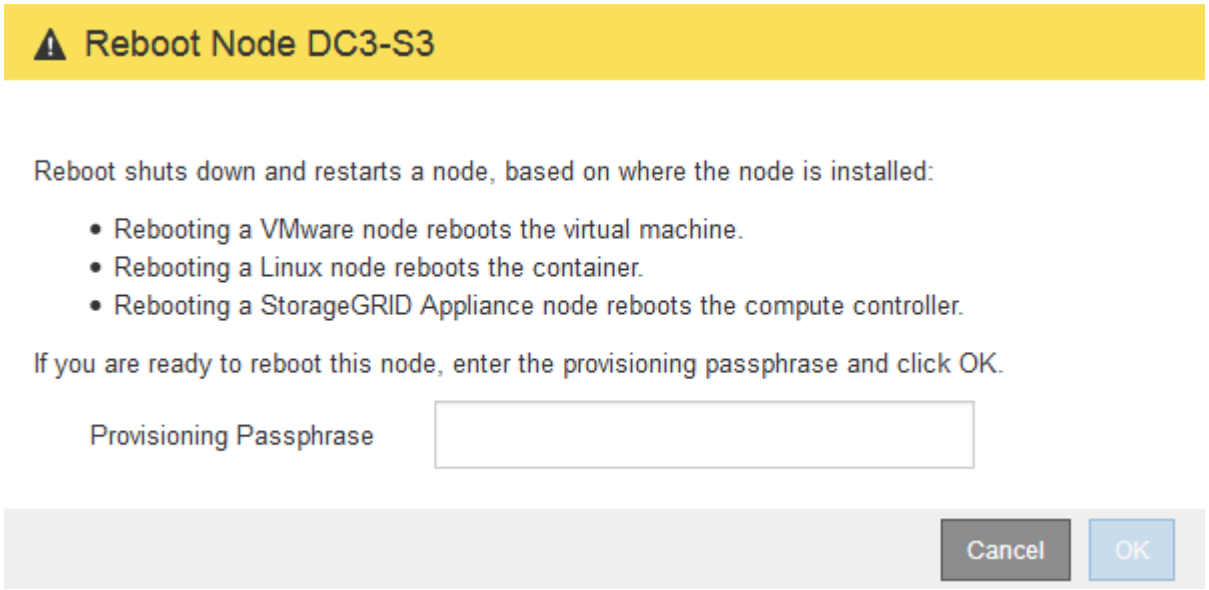
Passos

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



4. Clique em **Reboot**.

É apresentada uma caixa de diálogo de confirmação.



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

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

6. Aguarde até que o nó seja reiniciado.

   Pode levar algum tempo para que os serviços sejam desativados.

   Quando o nó é reinicializado, o ícone cinza (administrativamente para baixo) aparece no lado esquerdo da página nós. Quando todos os serviços tiverem sido iniciados novamente, o ícone muda novamente para a cor original.

Informações relacionadas

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Aparelhos de serviços SG100 SG1000"

Exibindo a guia objetos

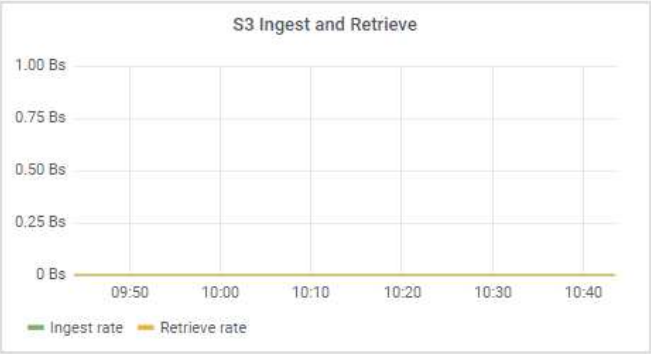
A guia objetos fornece informações sobre taxas de ingestão e recuperação S3 e Swift.

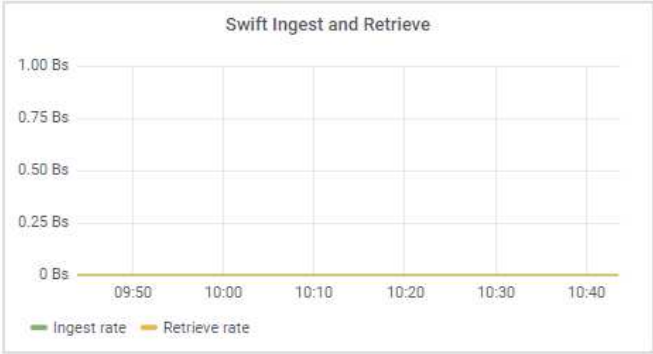
A guia objetos é exibida para cada nó de armazenamento, cada local e toda a grade. Para nós de storage, a guia objetos também fornece contagens de objetos e informações sobre consultas de metadados e verificação em segundo plano.

DC1-S1 (Storage Node)

Overview | Hardware | Network | Storage | Objects | ILM | Events | Tasks

1 hour | 1 day | 1 week | 1 month | Custom





Object Counts

Total Objects	0
Lost Objects	0
S3 Buckets and Swift Containers	0

Queries

Average Latency	5.74 milliseconds
Queries - Successful	12,403
Queries - Failed (timed-out)	0
Queries - Failed (consistency level unmet)	0

Verification

Status	No Errors
Rate Setting	Adaptive
Percent Complete	0.00%
Average Stat Time	0.00 microseconds
Objects Verified	0
Object Verification Rate	0.00 objects / second
Data Verified	0 bytes
Data Verification Rate	0.00 bytes / second
Missing Objects	0
Corrupt Objects	0
Corrupt Objects Unidentified	0
Quarantined Objects	0

Informações relacionadas

"Use S3"

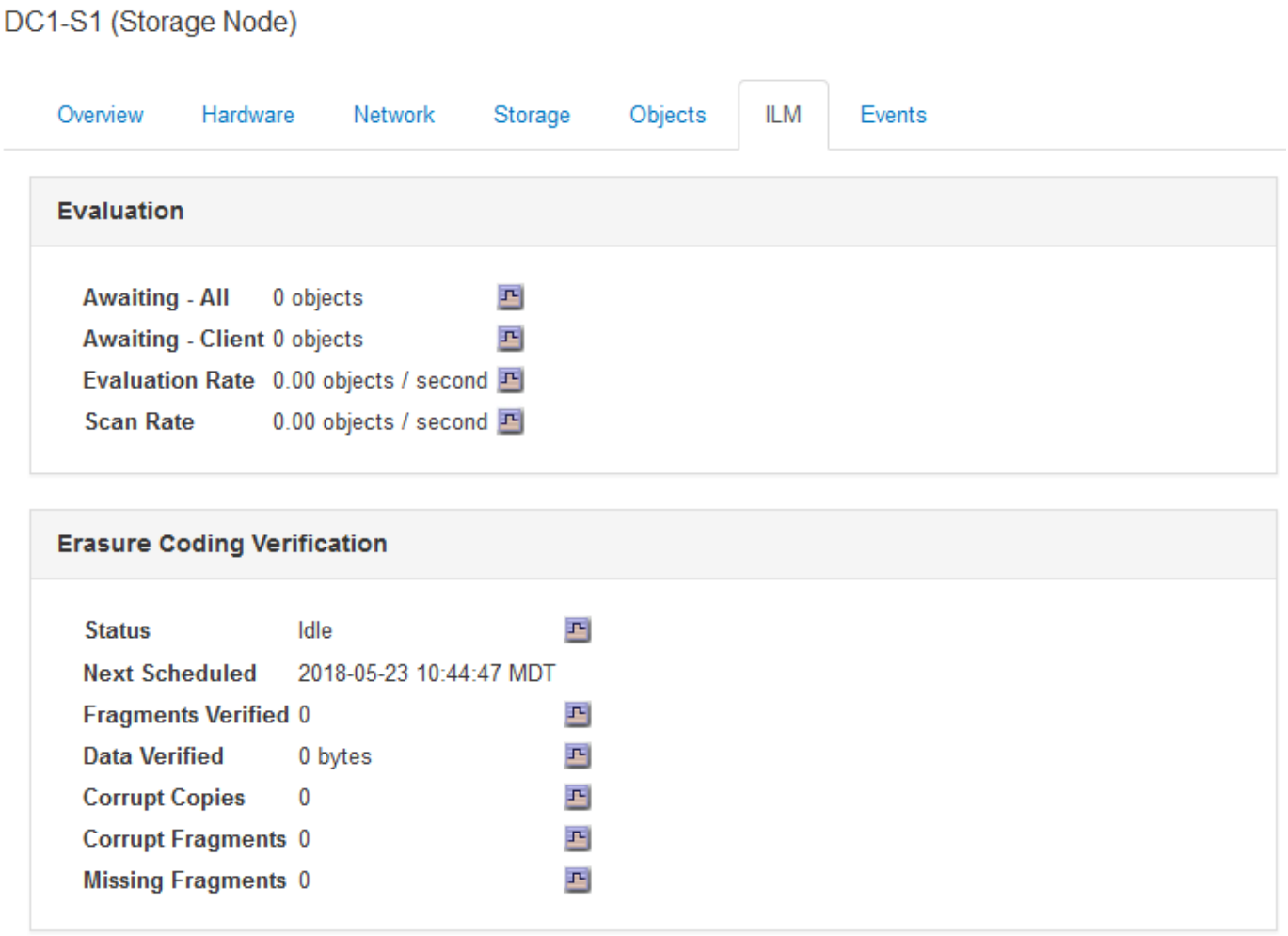
"Use Swift"

Visualizar o separador ILM

A guia ILM fornece informações sobre as operações do Information Lifecycle Management (ILM).

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

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



Informações relacionadas

"Monitoramento do gerenciamento do ciclo de vida das informações"

"Administrar o StorageGRID"

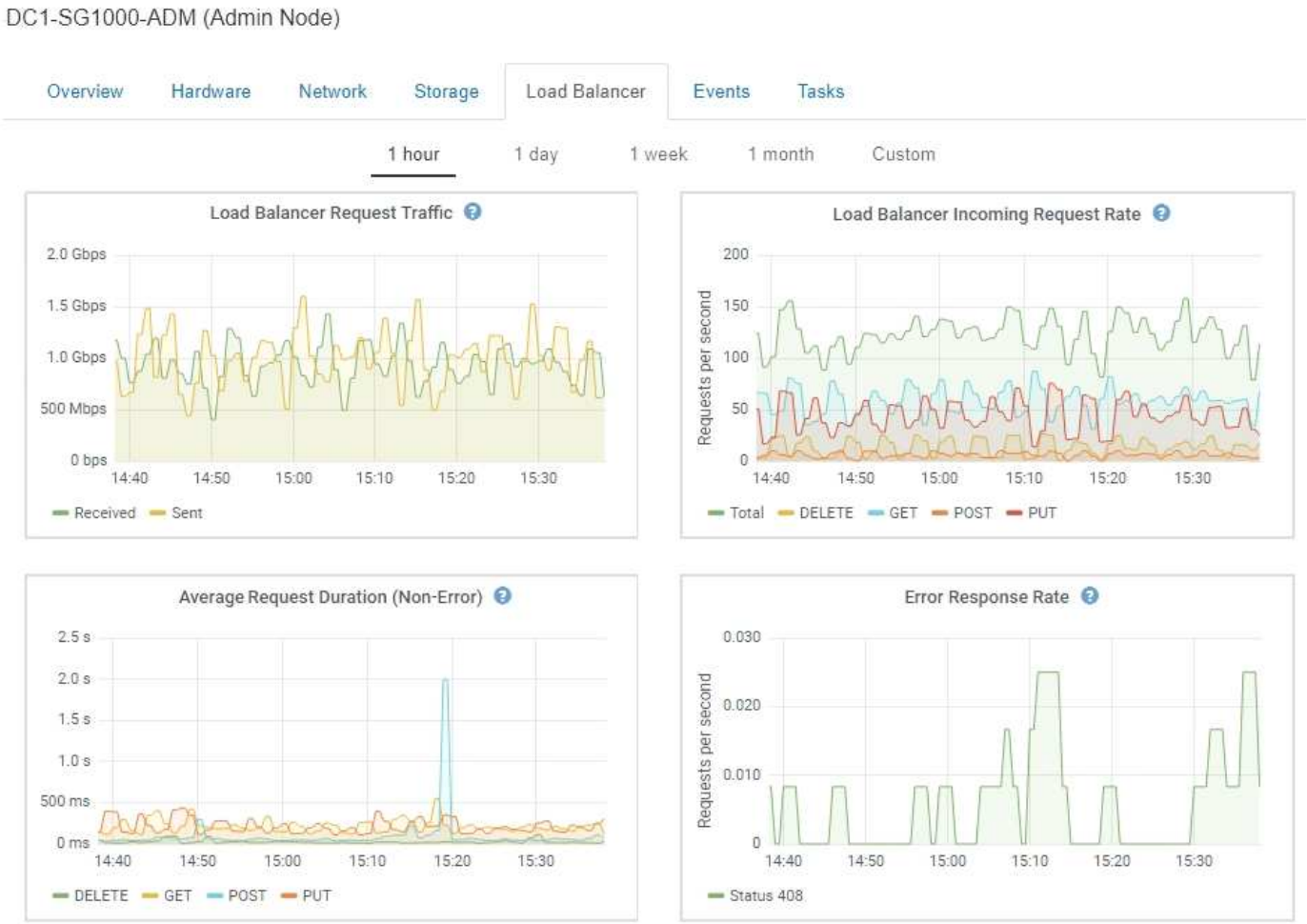
Exibindo a guia Load Balancer

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

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

todos os nós nesse local. Para toda a grade, a guia Load Balancer fornece um resumo agregado das estatísticas de todos os sites.

Se não houver nenhuma e/S sendo executada pelo serviço do Load Balancer ou se não houver nenhum balanceador de carga configurado, os gráficos exibem ""nenhum dado"."



Tráfego de solicitação do balanceador de carga

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 de entrada do Load Balancer

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 do pedido (não-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

"Monitoramento de operações de balanceamento de carga"

"Administrar o StorageGRID"

Exibindo a guia Serviços da plataforma

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

A guia Serviços de 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 as instruções para administrar o StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Exibição de 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

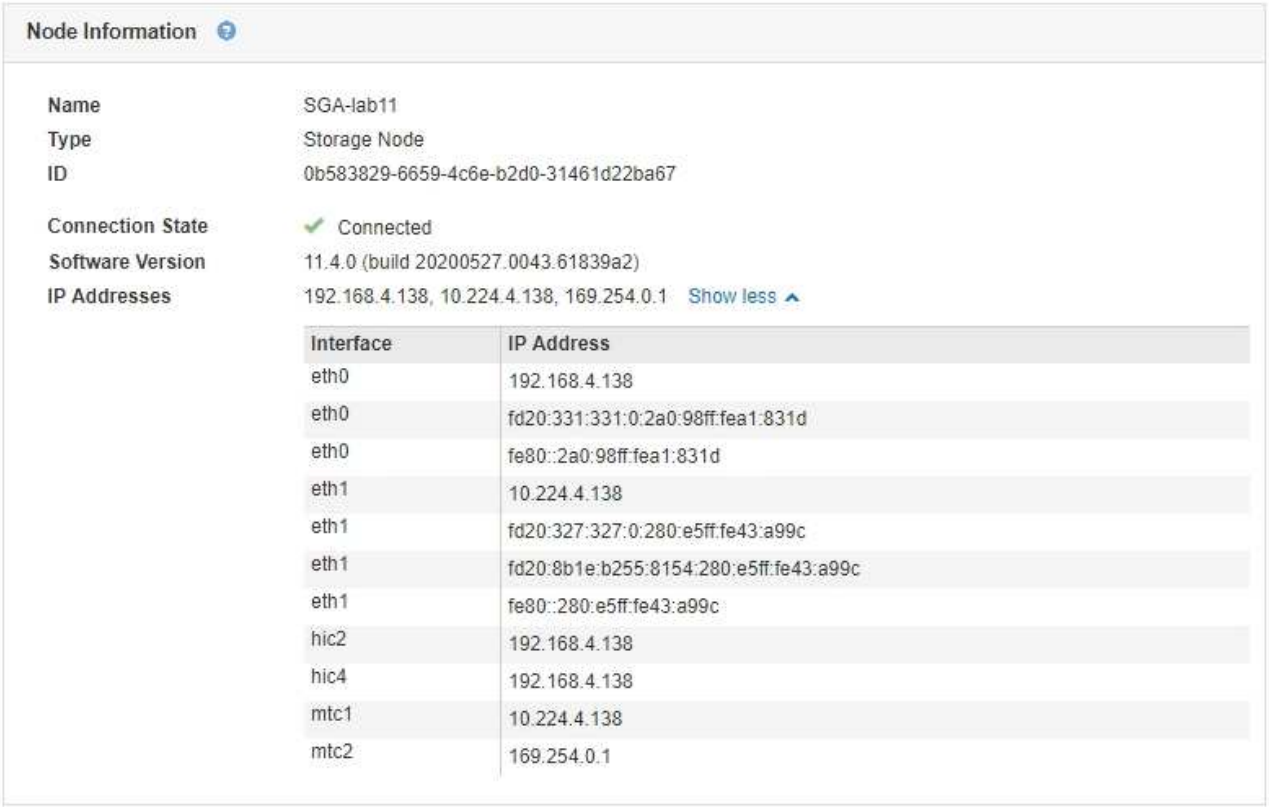
firmware do controlador, recursos de rede, interfaces de rede, endereços de rede e receber e transmitir dados.

Passos

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

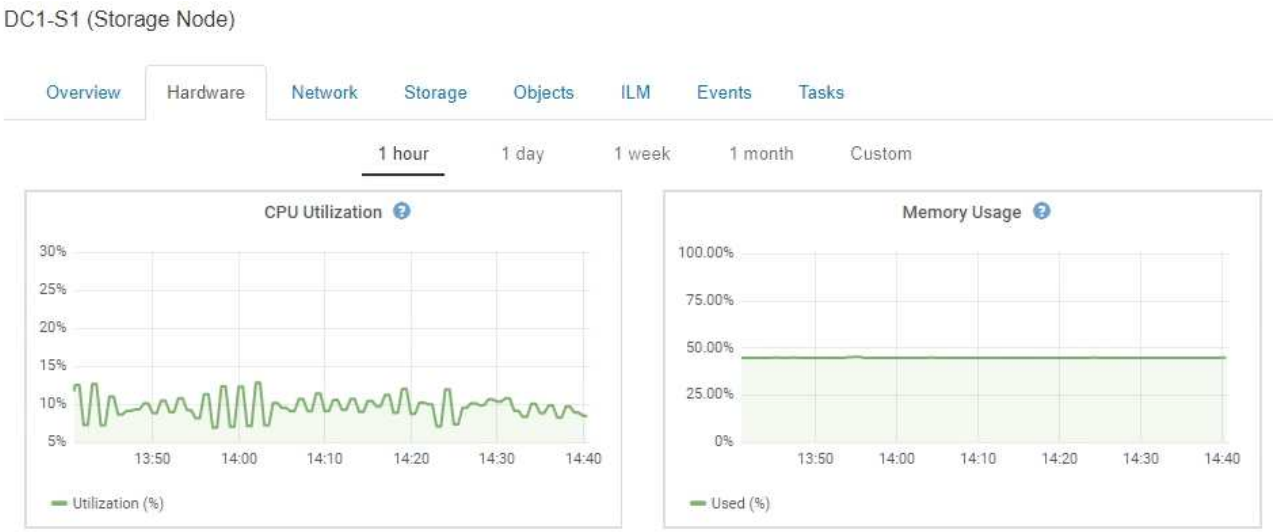
   A tabela informações do nó na guia Visão geral exibe a ID e o nome do nó, o tipo de nó, a versão do software instalada e os endereços IP associados ao nó. A coluna Interface contém o nome da interface, da seguinte forma:

   - **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, que pode ser ligada ou ligada à rede de administração do StorageGRID (eth1).



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

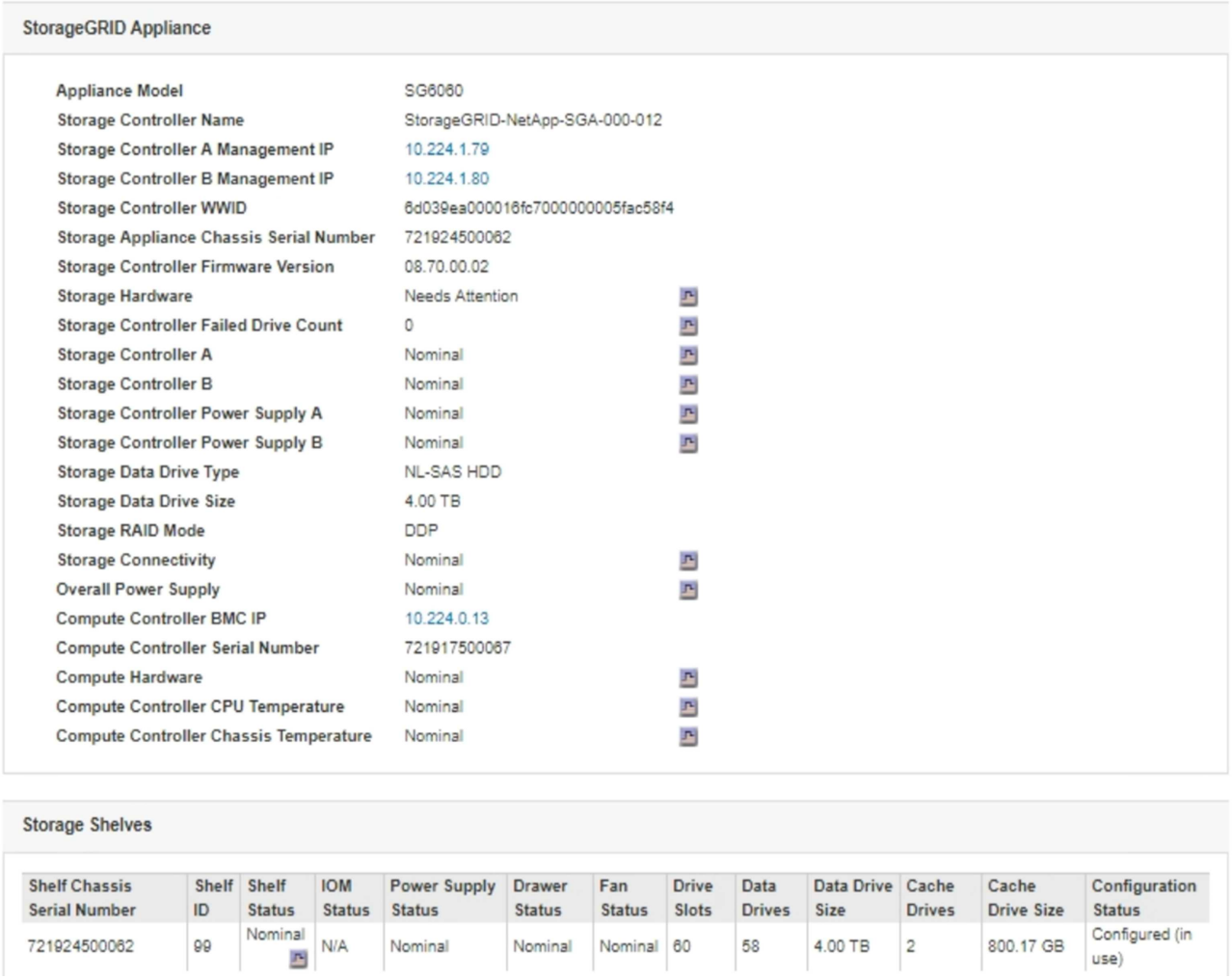
   a. Visualize os gráficos de utilização da CPU e memória para determinar as percentagens de utilização da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico ou gráfico. Você pode exibir as informações disponíveis para intervalos 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 BMC IP do controlador de computação e 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 software SANtricity.
Nome do controlador de armazenamento	O nome deste dispositivo StorageGRID mostrado no software SANtricity.
Controlador de armazenamento Um IP de gerenciamento	Endereço IP da porta de gerenciamento 1 no controlador de armazenamento A. você usa esse IP para acessar o software SANtricity para solucionar problemas de armazenamento.
IP de gerenciamento do controlador de armazenamento B.	Endereço IP da porta de gerenciamento 1 no controlador de storage B. você usa esse IP para acessar o software SANtricity para solucionar problemas de storage. Alguns modelos de aparelhos não têm um controlador de armazenamento B..

Campo na mesa do aparelho	Descrição
WWID do controlador de armazenamento	O identificador mundial do controlador de storage mostrado no software SANtricity.
Número de série do chassis do dispositivo de armazenamento	O número de série do chassis do aparelho.
Versão do firmware do controlador de armazenamento	A versão do firmware no controlador de armazenamento para este dispositivo.
Hardware de armazenamento	O status geral do hardware do controlador de storage. Se o Gerenciador de sistema do SANtricity relatar um status de precisa de atenção para o hardware de storage, o sistema StorageGRID também informará esse valor. Se o status for "precisa de atenção", primeiro verifique o controlador de armazenamento usando o software SANtricity. Em seguida, certifique-se de que não existem outros alarmes que se apliquem ao controlador de computação.
Falha na contagem de unidades do controlador de armazenamento	O número de unidades que não são ideais.
Controlador de armazenamento A	O status do controlador de armazenamento A..
Controlador de armazenamento B	O estado do controlador de armazenamento B. alguns modelos de aparelhos não têm um controlador de armazenamento B.
Fonte de alimentação A do controlador de armazenamento	O estado da fonte de Alimentação A para o controlador de armazenamento.
Fonte de alimentação B do controlador de armazenamento	O estado da fonte de alimentação B para o controlador de armazenamento.
Tipo de unidade de dados de armazenamento	O tipo de unidades no dispositivo, como HDD (unidade de disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de dados de armazenamento	Capacidade total, incluindo todas as unidades de dados do dispositivo.
Modo RAID de armazenamento	O modo RAID configurado para o dispositivo.
Conetividade de armazenamento	O estado de conetividade de storage.

Campo na mesa do aparelho	Descrição
Fonte de alimentação geral	O estado de todas as fontes de alimentação do aparelho.
IP do controlador de computação BMC	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 storage separados.
Temperatura da CPU do controlador de computação	O status da temperatura da CPU do controlador de computação.
Temperatura do chassi do controlador de computação	O status da temperatura do controlador de computação.

+

Coluna na tabela prateleiras de armazenamento	Descrição
Número de série do chassi da prateleira	O número de série do chassi do compartimento de armazenamento.
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 ao SG6060.
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.

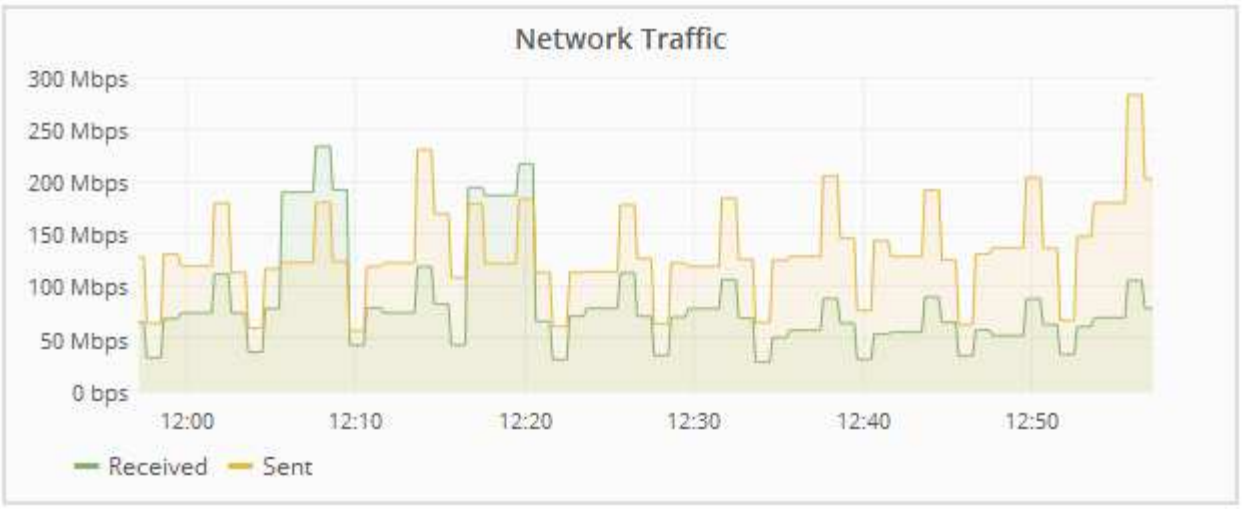
Coluna na tabela prateleiras de armazenamento	Descrição
Estado da fonte de alimentação	O status geral das fontes de alimentação para o compartimento de armazenamento.
Estado da gaveta	O estado das gavetas na prateleira de arrumação. N/A se a prateleira não contiver gavetas.
Estado da ventoinha	O status geral dos ventiladores de resfriamento na prateleira de armazenamento.
Ranhuras da unidade	O número total de slots de unidade no compartimento de armazenamento.
Unidades de dados	O número de unidades no compartimento de storage usadas para o storage de dados.
Tamanho da unidade de dados	O tamanho efetivo de uma unidade de dados no compartimento de storage.
Unidades de cache	O número de unidades no compartimento de armazenamento que são usadas como cache.
Tamanho da unidade de cache	O tamanho da menor unidade de cache no compartimento de armazenamento. Normalmente, as unidades de cache têm o mesmo tamanho.
Estado da configuração	O status de configuração do compartimento de storage.

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

   Se um status não for "nominal", revise os alertas atuais. Você também pode usar o Gerenciador de sistema do SANtricity para saber mais sobre alguns desses valores de hardware. Consulte as instruções para instalar e manter o seu aparelho.

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

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



a. Reveja a secção interfaces de rede.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	Up

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

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

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

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	25	25
Agregado	LACP	10	40
Fixo	LACP	10	20
Fixo	Ativo/Backup	10	10

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

b. Reveja a secção Comunicação de rede.

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

Network Communication

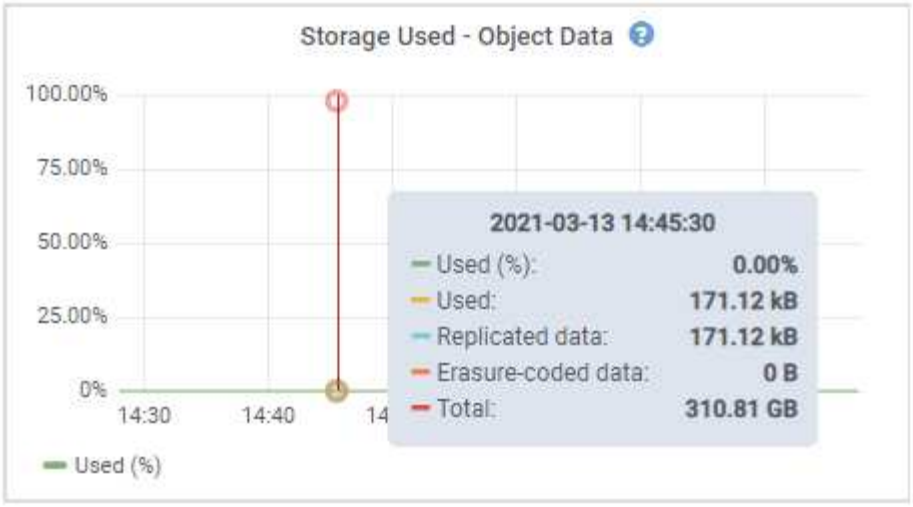
Receive

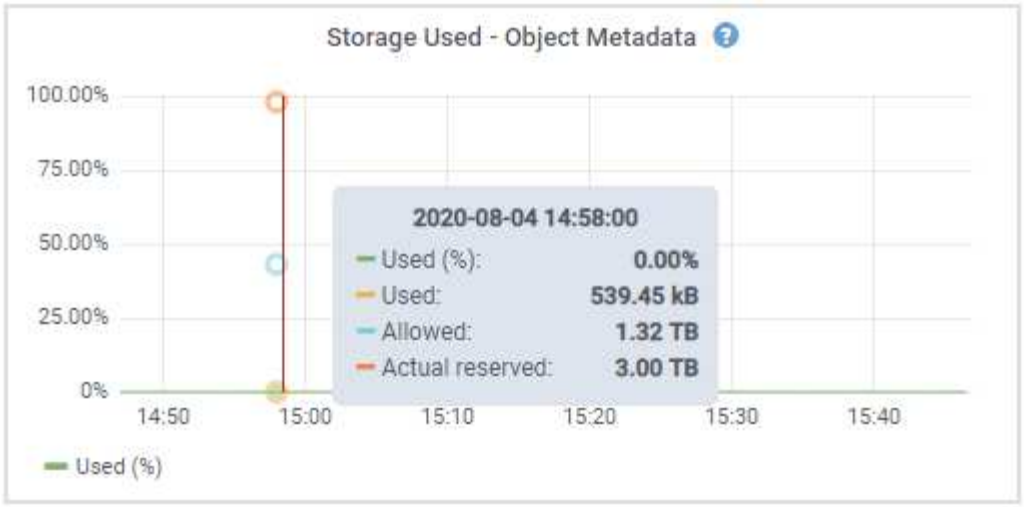
Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

6. 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.

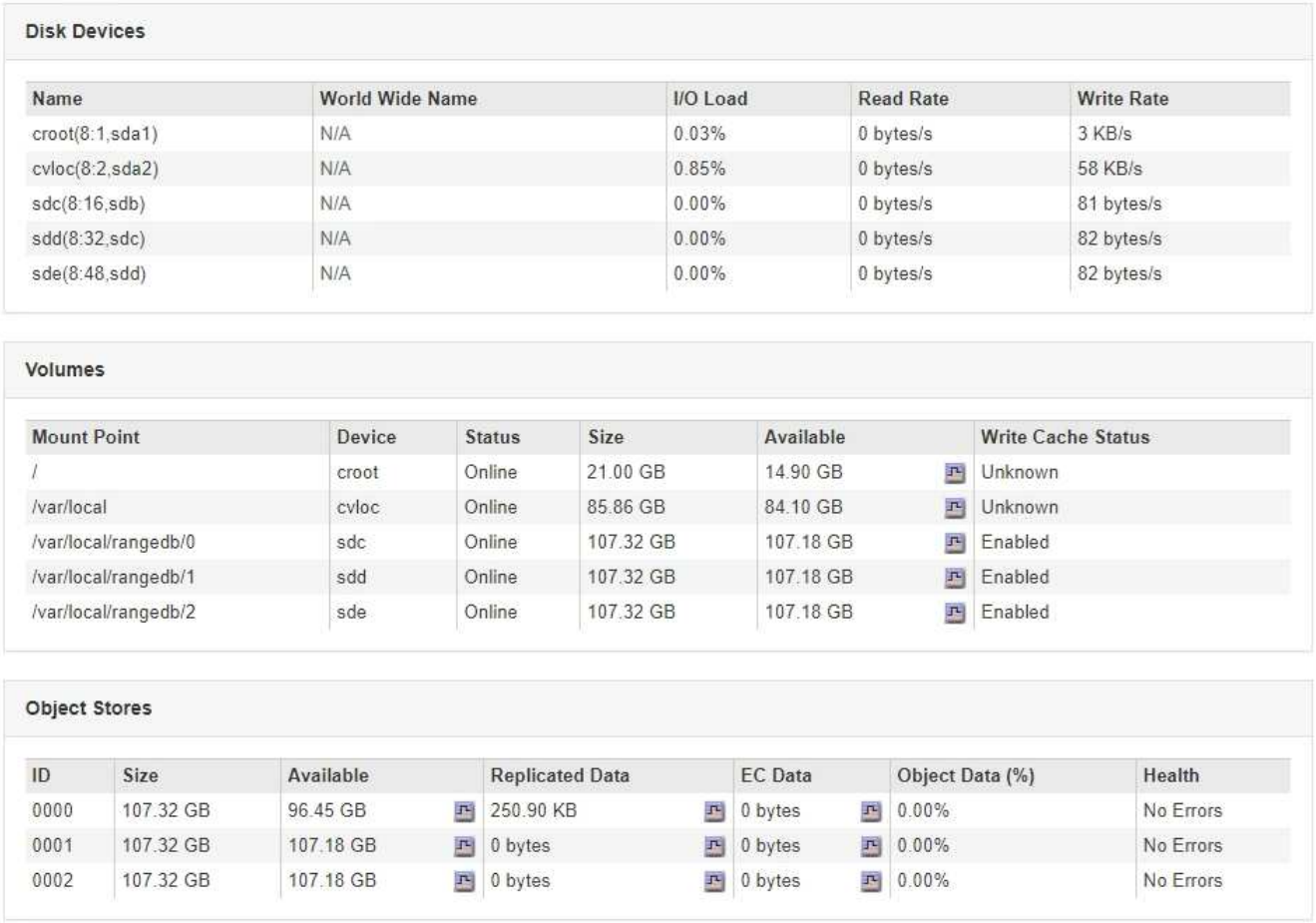




a. Role para baixo para ver as quantidades de armazenamento disponível para cada volume e armazenamento de objetos.

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

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



Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Informações relacionadas

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

Exibindo a guia Gerenciador de sistema do SANtricity

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

A guia Gerenciador de sistema do SANtricity é exibida para os nós de dispositivos de storage.

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

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

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

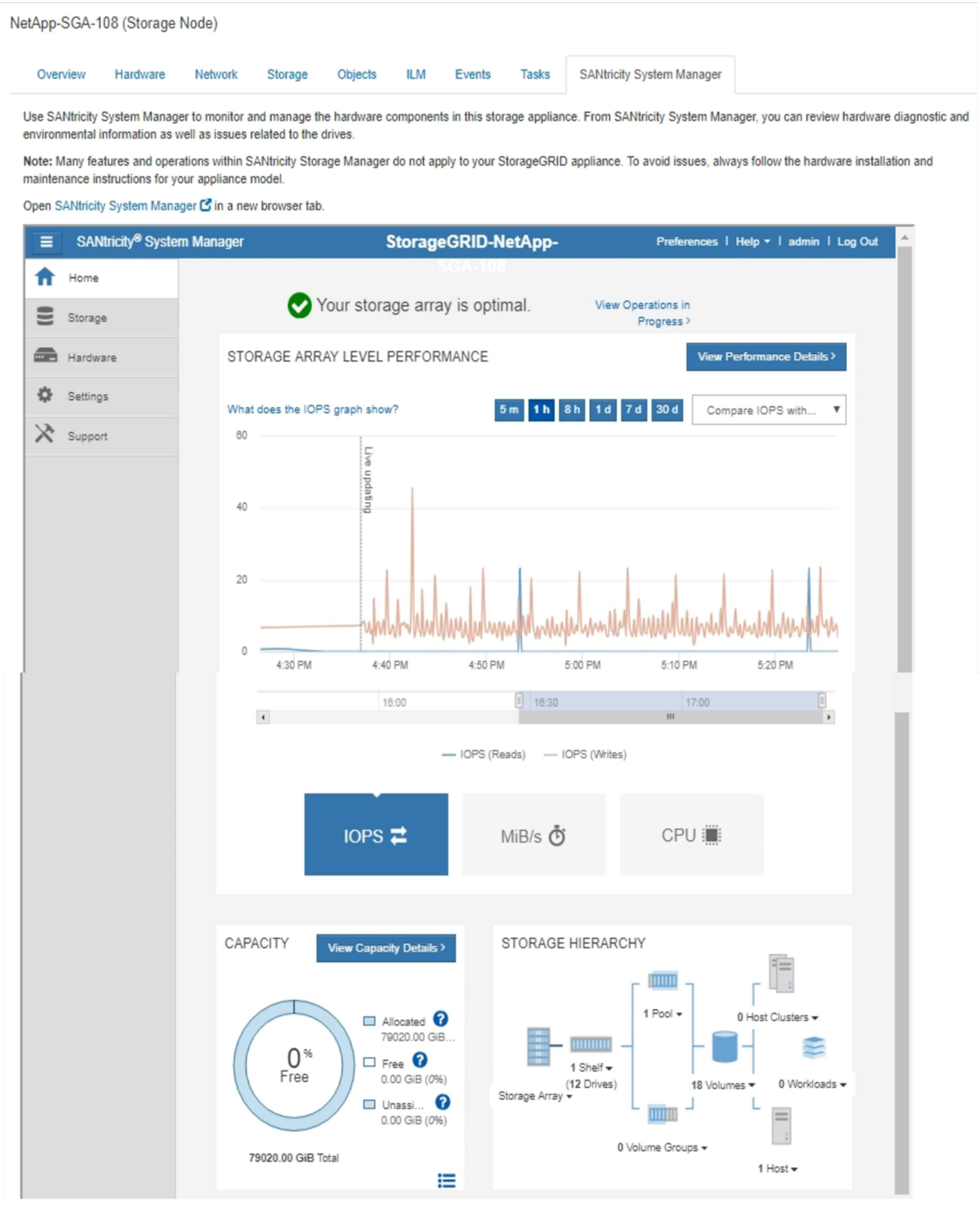
"Administrar o StorageGRID"

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

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

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

O separador apresenta a página inicial do Gestor do sistema SANtricity



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

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

gráfico.

Para obter mais detalhes sobre como visualizar as informações acessíveis a partir do separador Gestor do sistema do SANtricity, consulte as informações no "Centro de Documentação de sistemas NetApp e-Series"

Exibindo informações sobre nós de administração do dispositivo e 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 usado para um nó de administrador ou um 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 tabela informações do nó na guia Visão geral exibe a ID e o nome do nó, o tipo de nó, a versão do software instalada e os endereços IP associados ao nó. A coluna Interface contém o nome da interface, 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, que pode ser ligada ou ligada à rede de administração do StorageGRID (eth1).

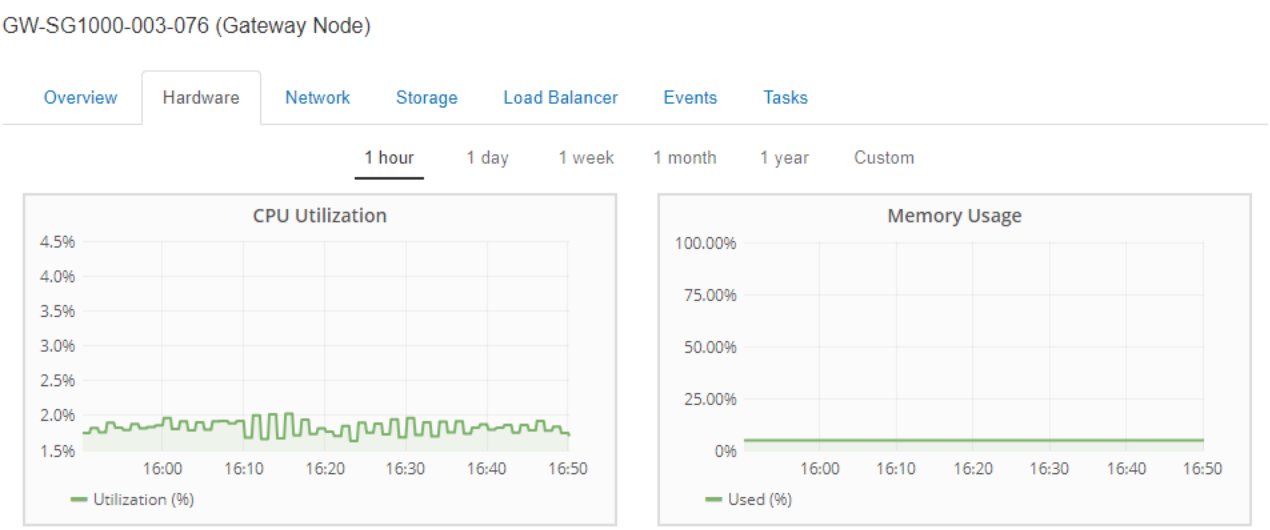
Node Information

ID	46702fe0-2bca-4097-8f61-f3fe6b22ed75
Name	GW-SG1000-003-076
Type	Gateway Node
Software Version	11.3.0 (build 20190708.2304.71ba19a)
IP Addresses	169.254.0.1, 172.16.3.76, 10.224.3.76, 47.47.3.76 Show less

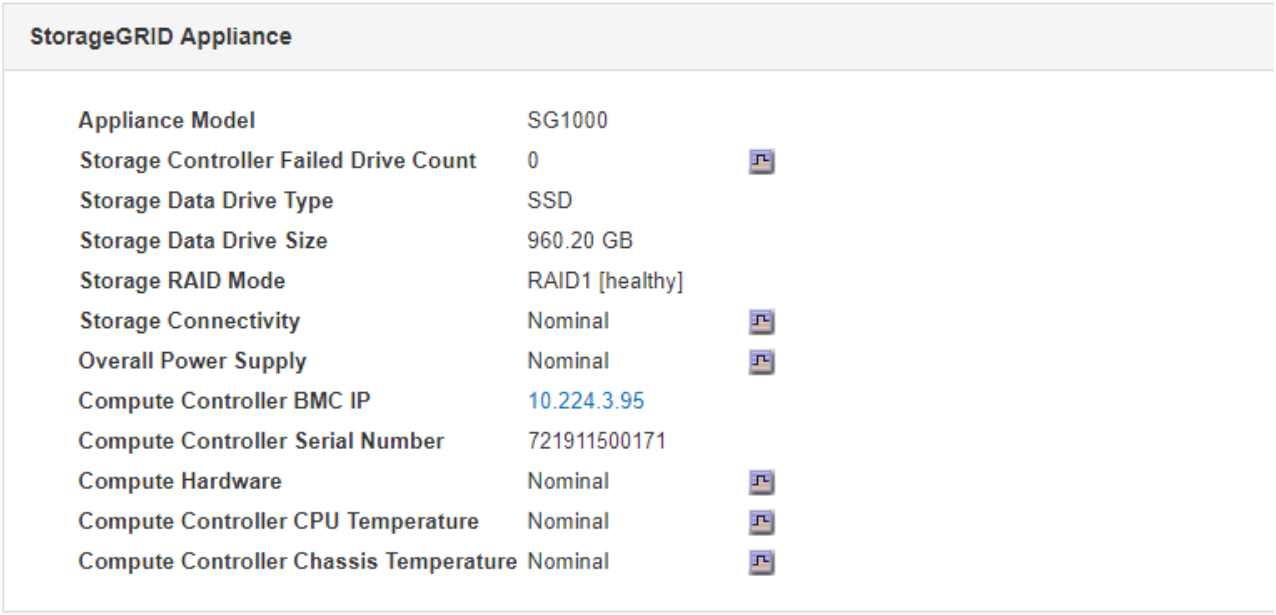
Interface	IP Address
adllb	fe80::c020:17ff:fe59:1cf3
adlli	169.254.0.1
adlli	fd20:327:327:0:408f:84ff:fe80:a9
adlli	fd20:8b1e:b255:8154:408f:84ff:fe80:a9
adlli	fe80::408f:84ff:fe80:a9
eth0	172.16.3.76
eth0	fd20:328:328:0:9a03:9bff:fe98:a272
eth0	fe80::9a03:9bff:fe98:a272
eth1	10.224.3.76
eth1	fd20:327:327:0:b6a9:fcff:fe08:4e49
eth1	fd20:8b1e:b255:8154:b6a9:fcff:fe08:4e49
eth1	fe80::b6a9:fcff:fe08:4e49
eth2	47.47.3.76
eth2	fd20:332:332:0:9a03:9bff:fe98:a272
eth2	fe80::9a03:9bff:fe98:a272
hic1	47.47.3.76
hic2	47.47.3.76
hic3	47.47.3.76
hic4	47.47.3.76
mtc1	10.224.3.76
mtc2	10.224.3.76

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.
Falha na contagem de unidades do controlador de armazenamento	O número de unidades que não são ideais.
Tipo de unidade de dados de armazenamento	O tipo de unidades no dispositivo, como HDD (unidade de disco rígido) ou SSD (unidade de estado sólido).

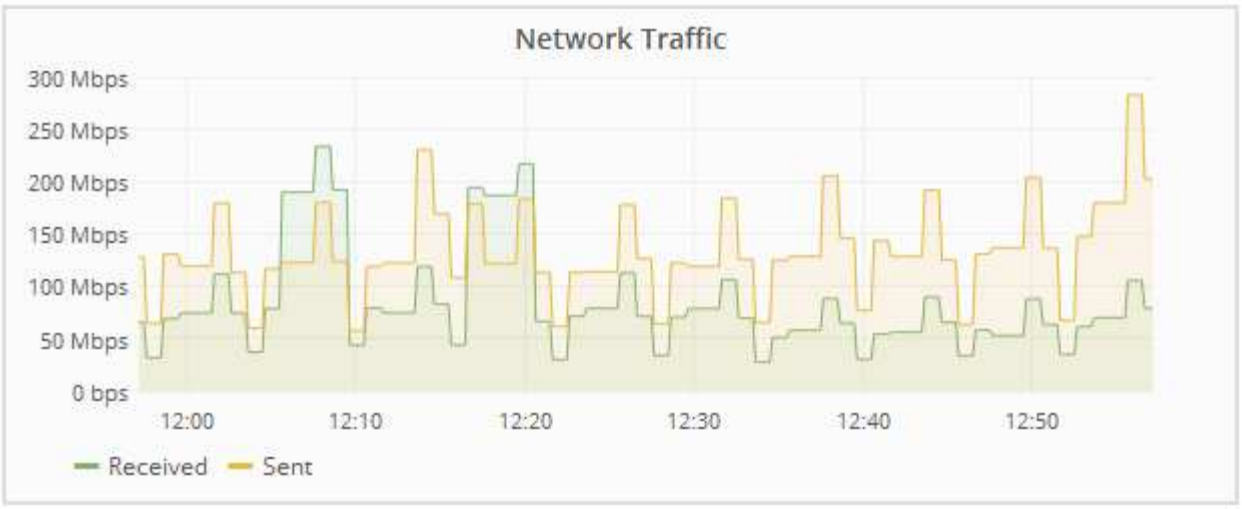
Campo na mesa do aparelho	Descrição
Tamanho da unidade de dados de armazenamento	Capacidade total, incluindo todas as unidades de dados do dispositivo.
Modo RAID de armazenamento	O modo RAID do dispositivo.
Fonte de alimentação geral	O estado de todas as fontes de alimentação no aparelho.
IP do controlador de computação BMC	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. Confirme se todos os Estados são ""nominais"".

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

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

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



a. Reveja a secção interfaces de rede.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
adllb	C2:20:17:59:1C:F3	10 Gigabit	Full	Off	Up
adlli	42:8F:84:80:00:A9	10 Gigabit	Full	Off	Up
eth0	98:03:9B:98:A2:72	400 Gigabit	Full	Off	Up
eth1	B4:A9:FC:08:4E:49	10 Gigabit	Full	Off	Up
eth2	98:03:9B:98:A2:72	400 Gigabit	Full	Off	Up
hic1	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic2	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic3	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic4	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
mtc1	B4:A9:FC:08:4E:49	Gigabit	Full	On	Up
mtc2	B4:A9:FC:08:4E:49	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

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

b. Reveja a secção Comunicação de rede.

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

Network Communication

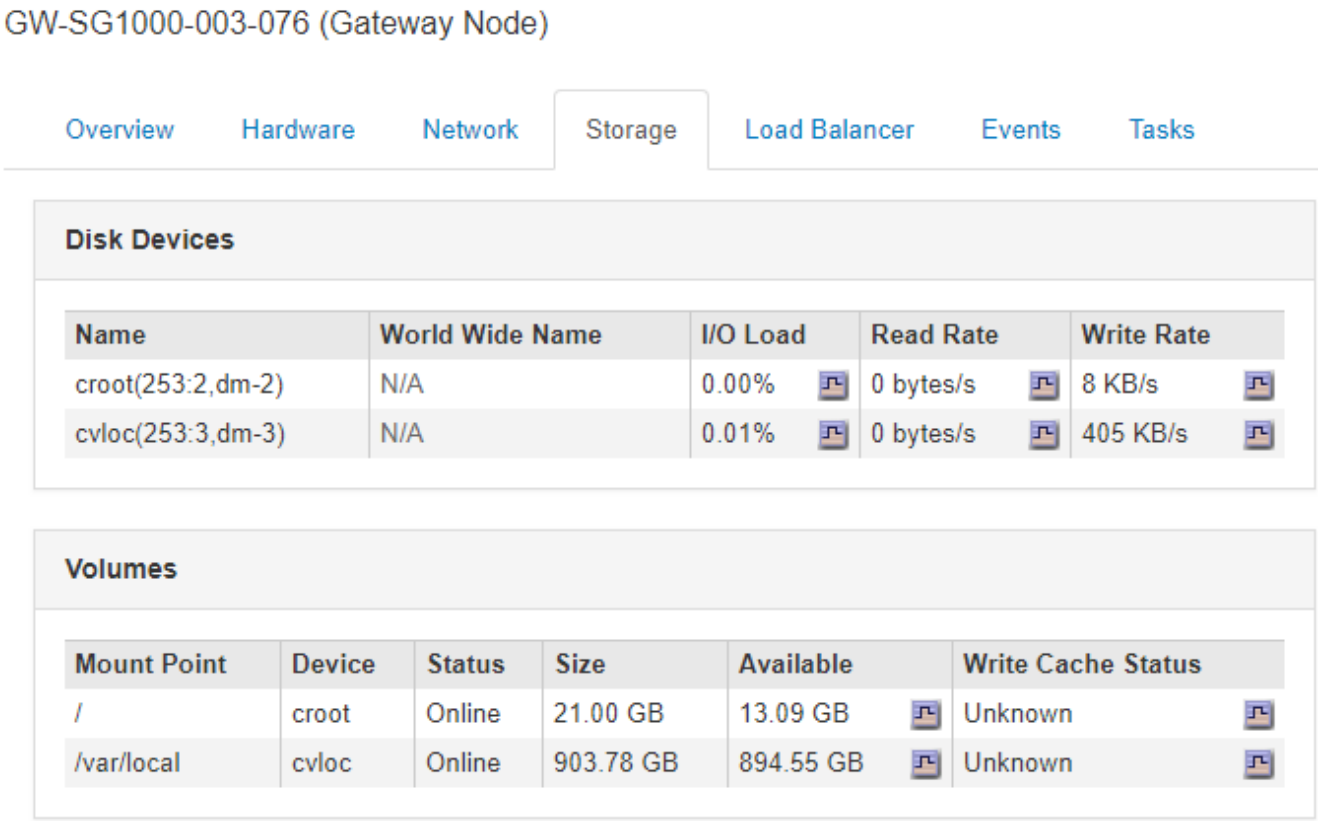
Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

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



Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

Informações que você deve monitorar regularmente

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

Um sistema ocupado gera grandes quantidades de informações. Esta secção fornece orientações sobre as informações mais importantes a monitorizar de forma contínua. Esta secção contém as seguintes subsecções:

- "Monitoramento da integridade do sistema"
- "Monitoramento da capacidade de armazenamento"
- "Monitoramento do gerenciamento do ciclo de vida das informações"
- "Monitoramento de desempenho, rede e recursos do sistema"
- "Monitorar a atividade do locatário"
- "Monitoramento da capacidade de arquivamento"
- "Monitoramento de operações de balanceamento de carga"
- "Aplicar hotfixes ou atualizar software, se necessário"

O que monitorar	Frequência
Os dados de integridade do sistema mostrados no painel do Grid Manager DashboardNote se alguma coisa mudou do dia anterior.	Diariamente
Taxa à qual a capacidade de metadados e objetos do nó de storage está sendo consumida	Semanalmente
Operações de gerenciamento do ciclo de vida das informações	Semanalmente
Desempenho, rede e recursos do sistema: • Latência da consulta • Conetividade e rede • Recursos em nível de nó	Semanalmente
Atividade do locatário	Semanalmente
Capacidade do sistema de armazenamento de arquivos externo	Semanalmente
Operações de balanceamento de carga	Após a configuração inicial e após quaisquer alterações de configuração
Disponibilidade de hotfixes de software e atualizações de software	Mensalmente

Monitoramento da integridade do sistema

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

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

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

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

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

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

Link	Indica
Detalhes da grelha	Aparece se algum nó estiver desconetado (estado de conexão desconhecido ou administrativamente inativo). Clique no link ou clique no ícone azul ou cinza para determinar que nó ou nós são afetados.
Alertas atuais	Aparece se algum alerta estiver ativo no momento. Clique no link ou clique em **Crítica**, **Principal** ou **menor** para ver os detalhes na página **Alertas atual**.
Alertas resolvidos recentemente	Aparece se quaisquer alertas acionados na semana passada estiverem agora resolvidos. Clique no link para ver os detalhes na página **Alertas resolvido**.
Alarmes legados	Aparece se algum alarme (sistema legado) estiver ativo no momento. Clique no link para ver os detalhes na página **suporte Alarmes (legado) Alarmes atuais**. **Nota:** enquanto o sistema de alarme antigo continua a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.
Licença	É apresentado se existir um problema com a licença de software para este sistema StorageGRID. Clique no link para ver os detalhes na página **Manutenção sistema Licença**.

Informações relacionadas

"Administrar o StorageGRID"

"Configurar notificações por e-mail para alertas"

"Utilizar a monitorização SNMP"

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Os nós podem ter um de três estados de conexão:

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

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

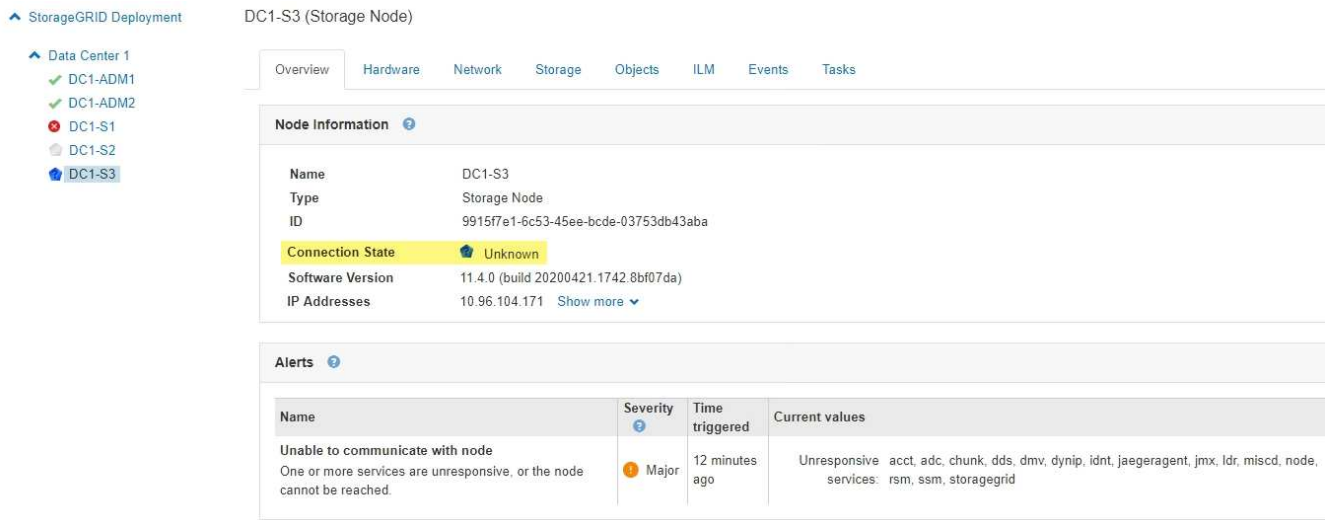
- **Não conetado - administrativamente para baixo** : o nó não está conetado à grade por um motivo esperado. Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.
- **Conectado** : o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

Passos

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

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

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



2. Se um nó tiver um ícone azul, siga estas etapas:
   a. Selecione cada alerta na tabela e siga as ações recomendadas.

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

   b. Se você não conseguir colocar o nó novamente on-line, entre em Contato com o suporte técnico.
3. Se um nó tiver um ícone cinza, siga estas etapas:

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

   a. Revise a seção Alertas e determine se algum alerta está afetando esse nó.
   b. Se um ou mais alertas estiverem ativos, selecione cada alerta na tabela e siga as ações recomendadas.
   c. Se você não conseguir colocar o nó novamente on-line, entre em Contato com o suporte técnico.

Informações relacionadas

"Referência de alertas"

"Manter recuperar"

Visualização de alertas atuais

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

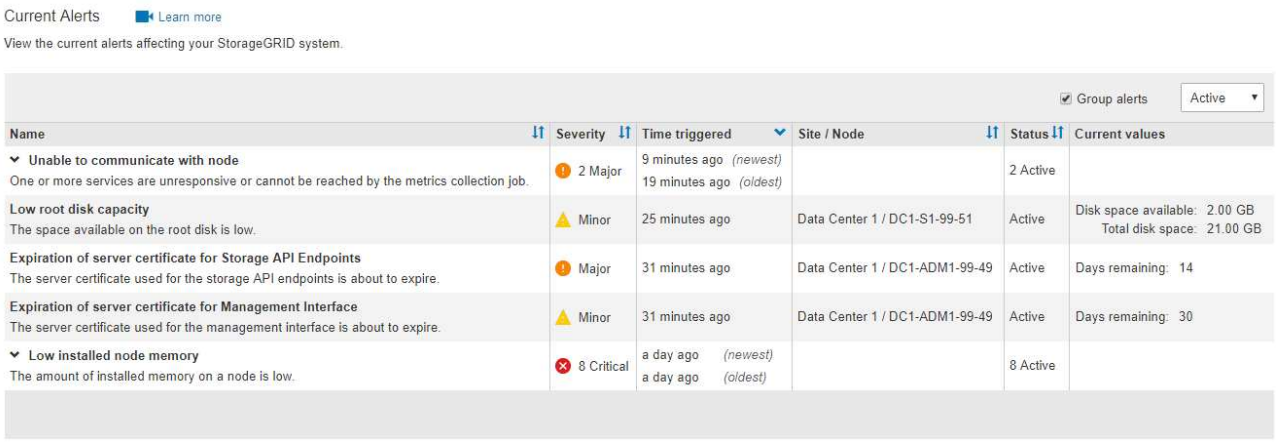
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Se um ou mais alertas estiverem ativos, execute um dos seguintes procedimentos:
   - No painel Saúde do Painel, clique no ícone de alerta ou clique em **alertas atuais**. (Um ícone de alerta e o link **alertas atuais** aparecem somente se pelo menos um alerta estiver ativo.)
   - Selecione **Alertas atual**.

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



Por padrão, os alertas são exibidos da seguinte forma:

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

  A página Alertas atuais é atualizada a cada dois minutos.

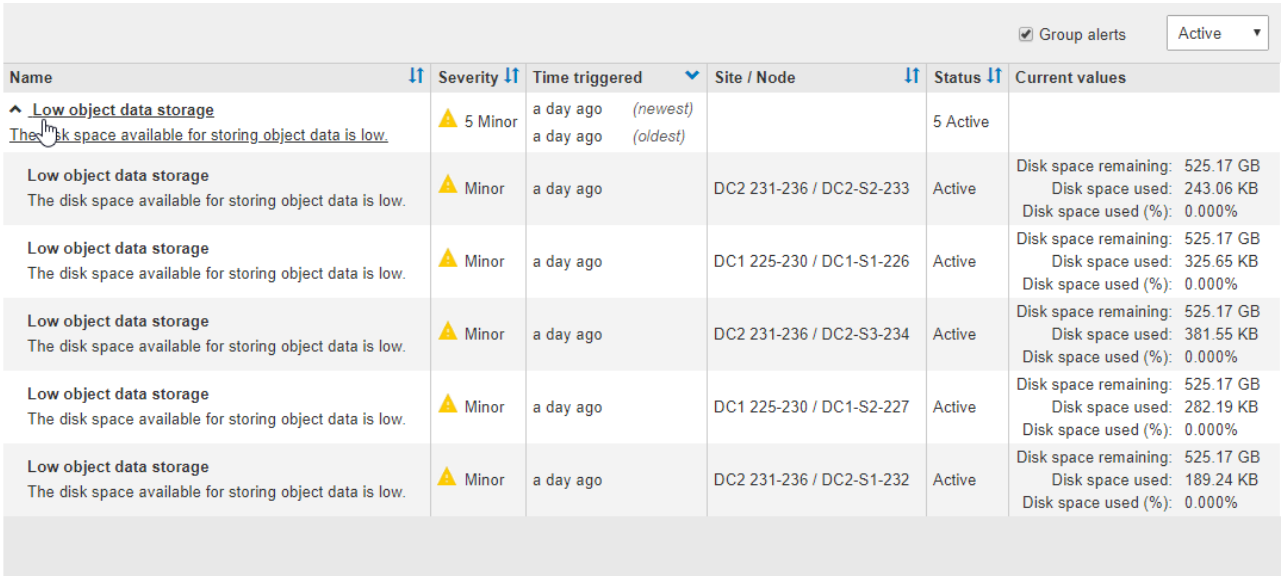
2. Reveja as informações na tabela.

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

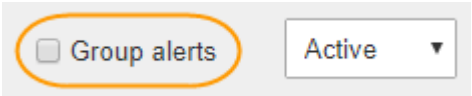
Cabeçalho da coluna	Descrição
Gravidade	A gravidade do alerta. Se vários alertas forem agrupados, a linha de título mostrará quantas instâncias desse alerta estão ocorrendo em cada gravidade. • **Crítico** : existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. 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. • **Minor** : o sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.
Tempo acionado	Há quanto tempo o alerta foi acionado. Se vários alertas forem agrupados, a linha de título mostrará horas para a instância mais recente do alerta (*newest*) e a instância mais antiga do alerta (*older*).
Local/nó	O nome do site e do nó onde o alerta está ocorrendo. Se vários alertas forem agrupados, os nomes do site e do nó não serão exibidos na linha de título.
Estado	Se o alerta está ativo ou foi silenciado. Se vários alertas forem agrupados e **todos os alertas** estiverem selecionados na lista suspensa, a linha de título mostrará quantas instâncias desse alerta estão ativas e quantas instâncias foram silenciadas.

Cabeçalho da coluna	Descrição
Valores atuais	O valor atual da métrica que fez com que o alerta fosse acionado. Para alguns alertas, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta **armazenamento de dados de objeto baixo** incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado. **Nota:** se vários alertas estiverem agrupados, os valores atuais não serão exibidos na linha de título.

3. Para expandir e recolher grupos de alertas:
   - Para mostrar os alertas individuais em um grupo, clique no cursor para baixo no cabeçalho ou clique no nome do grupo.
   - Para ocultar os alertas individuais em um grupo, clique no cursor para cima no cabeçalho ou clique no nome do grupo.



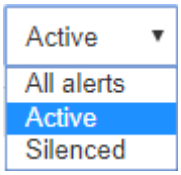
4. Para exibir alertas individuais em vez de grupos de alertas, desmarque a caixa de seleção **alertas de grupo** na parte superior da tabela.



5. Para classificar alertas ou grupos de alertas, clique nas setas para cima/para baixo em cada cabeçalho de coluna.
   - Quando **alertas de grupo** é selecionado, tanto os grupos de alerta quanto os alertas individuais dentro de cada grupo são classificados. Por exemplo, você pode querer classificar os alertas em um grupo por **tempo disparado** para encontrar a instância mais recente de um alerta específico.
   - Quando **Alerta de grupo** não está selecionado, toda a lista de alertas é classificada. Por exemplo, você pode querer classificar todos os alertas por **nó/Site** para ver todos os alertas que afetam um nó

específico.

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



   - Selecione **todos os alertas** para visualizar todos os alertas atuais (alertas ativos e silenciados).
   - Selecione **Ativo** para exibir somente os alertas atuais ativos.
   - Selecione **silenciado** para visualizar apenas os alertas atuais que foram silenciados.

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

   É apresentada uma caixa de diálogo para o alerta. Consulte as instruções para visualizar um alerta específico.

Informações relacionadas

"Visualizar um alerta específico"

"Silenciar notificações de alerta"

Visualização de alertas resolvidos

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

O que você vai precisar

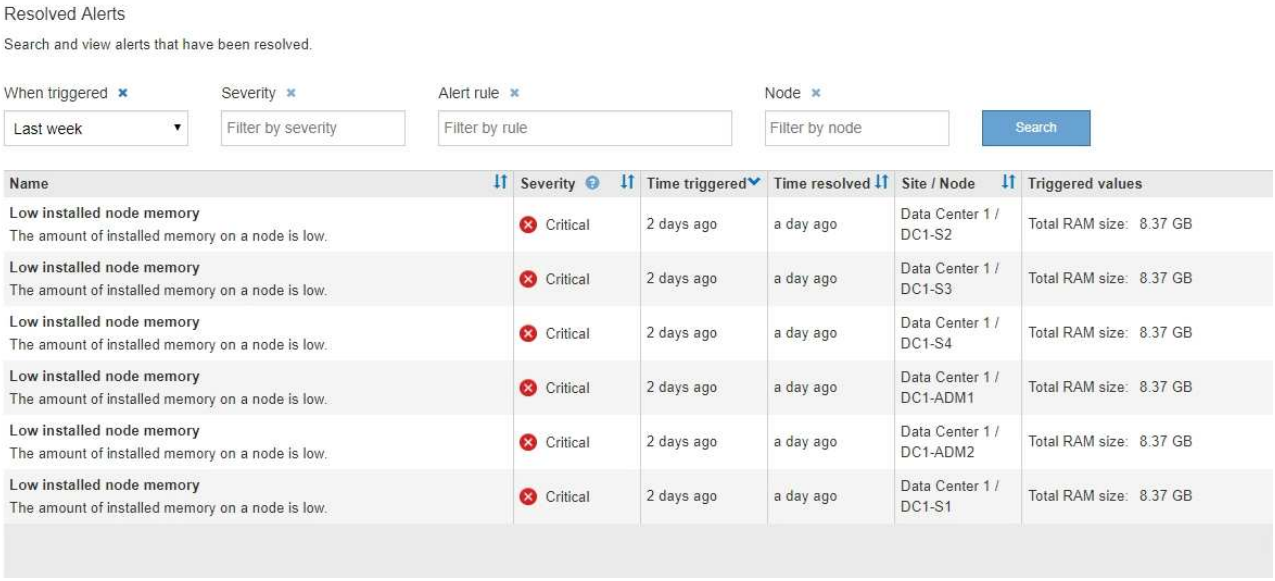
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Para exibir alertas resolvidos, siga um destes procedimentos:
   - No painel Saúde do Painel, clique em **alertas resolvidos recentemente**.

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

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



2. Reveja as informações na tabela.

Cabeçalho da coluna	Descrição
Nome	O nome do alerta e sua descrição.
Gravidade	A gravidade do alerta. • **Crítico**: existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido. • **Major**: existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não pare a operação normal de um nó ou serviço StorageGRID. • **Minor**: o sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.
Tempo acionado	Há quanto tempo o alerta foi acionado.
Tempo resolvido	Há quanto tempo o alerta foi resolvido.

Cabeçalho da coluna	Descrição
Local/nó	O nome do site e do nó onde o alerta ocorreu.
Valores acionados	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta **armazenamento de dados de objeto baixo** incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado.

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

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

4. Opcionalmente, filtre a lista de alertas resolvidos usando os menus suspensos na parte superior da tabela.
   a. Selecione um período de tempo no menu suspenso **When Triggered** para mostrar alertas resolvidos com base em quanto tempo atrás eles foram acionados.

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

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

   b. Selecione uma ou mais severidades no menu suspenso **gravidade** para filtrar os alertas resolvidos de uma gravidade específica.
   c. Selecione uma ou mais regras de alerta padrão ou personalizadas no menu suspenso **regra de alerta** para filtrar os alertas resolvidos relacionados a uma regra de alerta específica.
   d. Selecione um ou mais nós no menu suspenso **Node** para filtrar os alertas resolvidos relacionados a um nó específico.
   e. Clique em **pesquisar**.
5. Para exibir detalhes de um alerta resolvido específico, selecione o alerta na tabela.

   É apresentada uma caixa de diálogo para o alerta. Consulte as instruções para visualizar um alerta específico.

Informações relacionadas

"Visualizar um alerta específico"

Visualizar um alerta específico

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

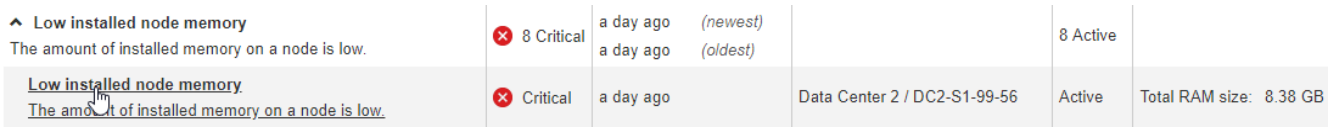
Passos

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

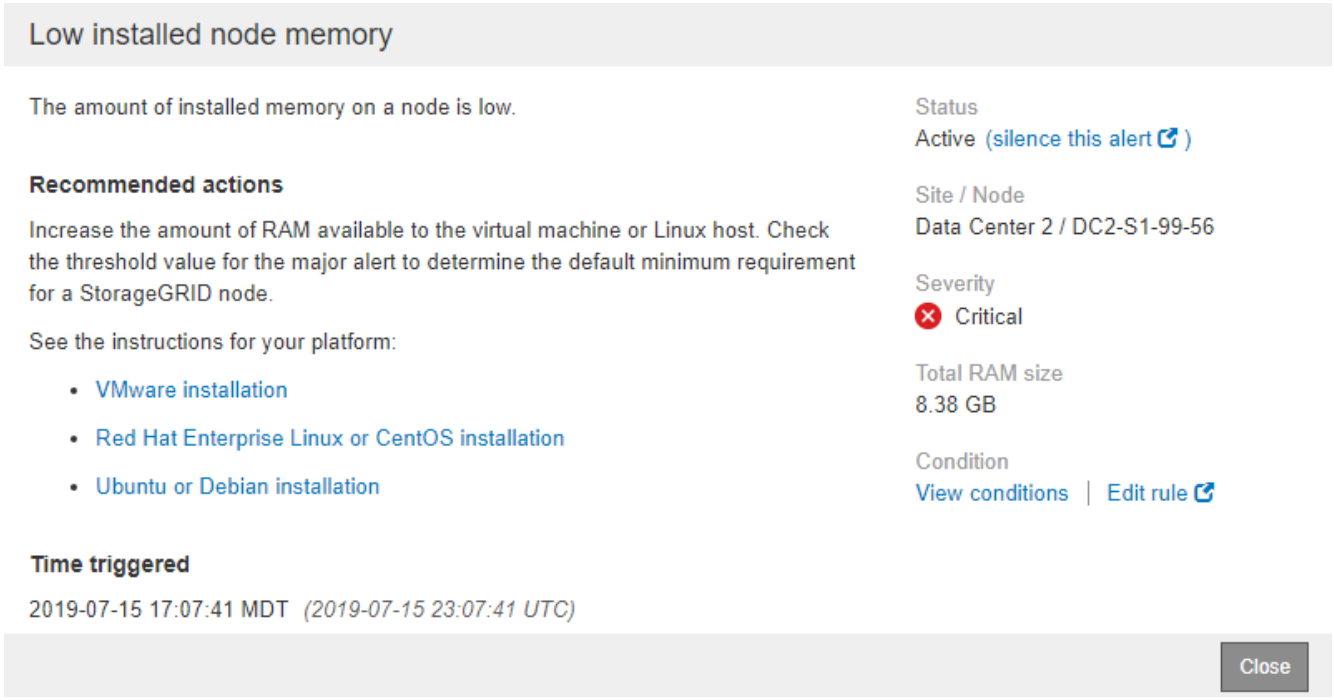
Cabeçalho da coluna	Descrição
Alerta atual	• No painel Saúde no Painel, clique no link **alertas atuais**. Este link aparece somente se pelo menos um alerta estiver ativo no momento. Este link fica oculto se não houver alertas atuais ou se todos os alertas atuais tiverem sido silenciados. • Selecione **Alertas atual**. • Na página **nós**, selecione a guia **Visão geral** para um nó que tenha um ícone de alerta. Em seguida, na seção Alertas, clique no nome do alerta.
Alerta resolvido	• No painel Saúde do Painel, clique no link **alertas resolvidos recentemente**. (Este link aparece somente se um ou mais alertas foram acionados na semana passada e agora estão resolvidos. Este link fica oculto se nenhum alerta foi acionado e resolvido na última semana.) • Selecione **Alertas resolvido**.

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

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



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



3. Reveja os detalhes do alerta.

Informações	Descrição
title	O nome do alerta.
primeiro parágrafo	A descrição do alerta.
Ações recomendadas	As ações recomendadas para este alerta.
Tempo acionado	A data e a hora em que o alerta foi acionado na sua hora local e em UTC.
Tempo resolvido	Apenas para alertas resolvidos, a data e a hora em que o alerta foi resolvido na sua hora local e na UTC.
Estado	O estado do alerta: Ativo, silenciado ou resolvido.
Local/nó	O nome do site e do nó afetados pelo alerta.

Informações	Descrição
Gravidade	A gravidade do alerta. • **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.
valores de dados	O valor atual da métrica para este alerta. Para alguns alertas, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta **armazenamento de metadados baixo** incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado.

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

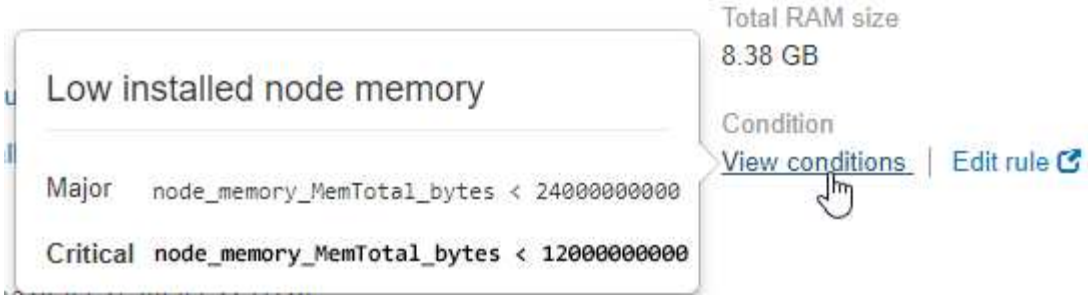
   Você deve ter a permissão Gerenciar Alertas ou acesso root para silenciar uma regra de alerta.

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

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

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

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



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

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

   Você deve ter a permissão Gerenciar Alertas ou acesso root para editar uma regra de alerta.

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

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

Informações relacionadas

"Silenciar notificações de alerta"

"Editar uma regra de alerta"

Visualização de alarmes legados

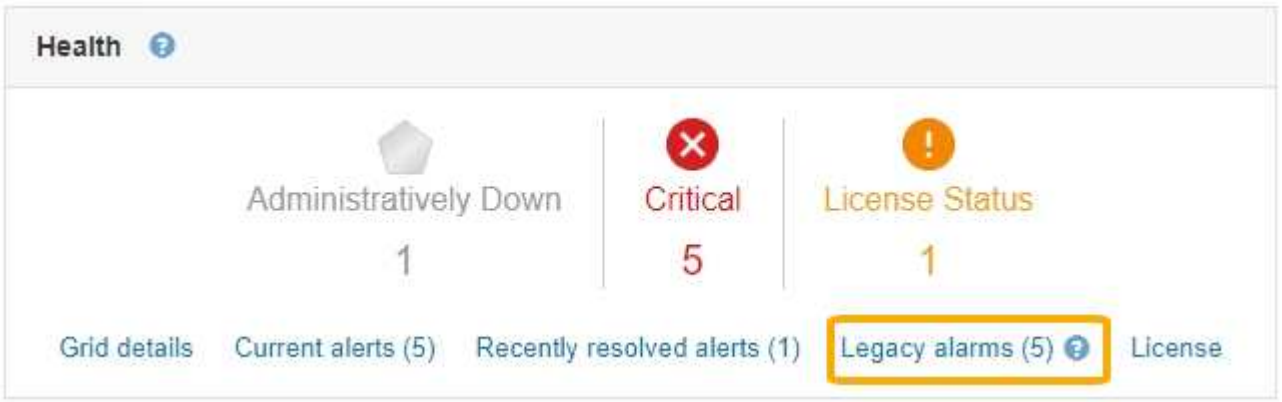
Os alarmes (sistema legado) são acionados quando os atributos do sistema atingem os valores de limite de alarme. Pode visualizar os alarmes atualmente ativos a partir do Painel de instrumentos ou da página Alarmes atuais.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Se um ou mais alarmes herdados estiverem ativos no momento, o painel Saúde no Painel inclui um link **Alarmes herdados**. O número entre parênteses indica quantos alarmes estão ativos no momento.



A contagem de **Legacy Alarms** no Dashboard é incrementada sempre que um alarme legado é acionado. Esta contagem é incrementada mesmo que tenha desativado as notificações por e-mail de alarme. Normalmente, pode ignorar este número (uma vez que os alertas fornecem uma melhor visualização do sistema) ou pode visualizar os alarmes que estão atualmente ativos.

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

Passos

1. Para exibir os alarmes legados que estão atualmente ativos, execute um dos seguintes procedimentos:
   - No painel Saúde no Painel, clique em **Legacy Alarms**. Este link aparece somente se pelo menos um alarme estiver ativo no momento.
   - Selecione **suporte Alarmes (legado) Alarmes atuais**. A página Alarmes atuais é exibida.

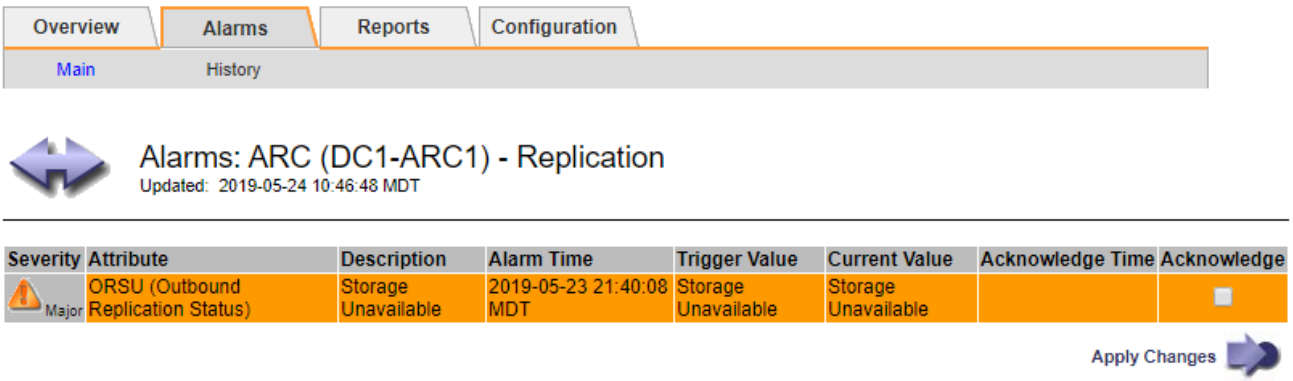
O ícone de alarme indica a gravidade de cada alarme, da seguinte forma:

Ícone	Cor	Gravidade do alarme	Significado
	Amarelo	Aviso	O nó está conetado à grade, mas existe uma condição incomum que não afeta as operações normais.
	Laranja claro	Menor	O nó está conetado à grade, mas existe uma condição anormal que pode afetar a operação no futuro. Você deve investigar para evitar o escalonamento.

Ícone	Cor	Gravidade do alarme	Significado
	Laranja escuro	Maior	O nó está conetado à grade, mas existe uma condição anormal que afeta atualmente a operação. Isso requer atenção imediata para evitar o escalonamento.
	Vermelho	Crítico	O nó está conetado à grade, mas existe uma condição anormal que parou as operações normais. Você deve resolver o problema imediatamente.

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

   A guia Alarmes para o serviço selecionado é exibida (**suporte Ferramentas topologia de Grade *Grid Node Service* Alarmes**).



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

Informações relacionadas

"Referência de alarmes (sistema legado)"

"Reconhecer alarmes atuais (sistema legado)"

"Desativar alarmes (sistema legado)"

Monitoramento da capacidade de armazenamento

Você deve monitorar o espaço utilizável total disponível nos nós de storage 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 visualizar as informações de capacidade de storage de toda a grade, de cada local e de cada nó de storage em seu sistema StorageGRID.

Informações relacionadas

"Visualizar o separador armazenamento"

Monitoramento da capacidade de armazenamento para toda a grade

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

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

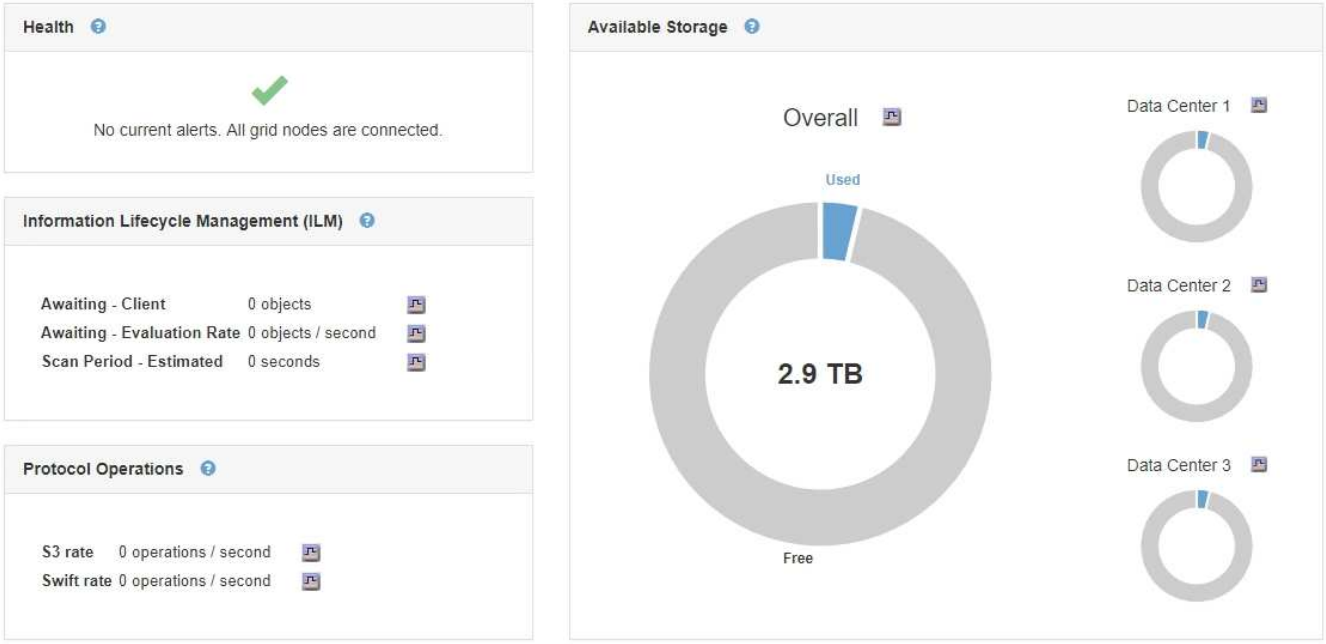
Sobre esta tarefa

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

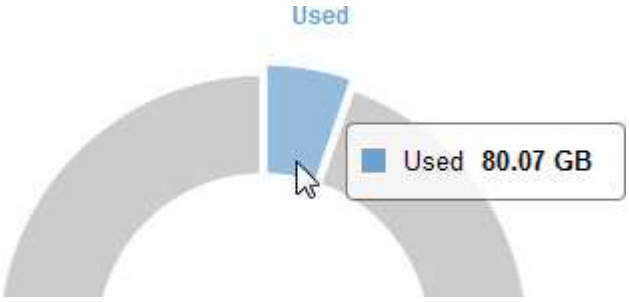
Passos

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

      O resumo não inclui Mídia de arquivamento.



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



b. Para grades de vários locais, revise o gráfico de cada data center.

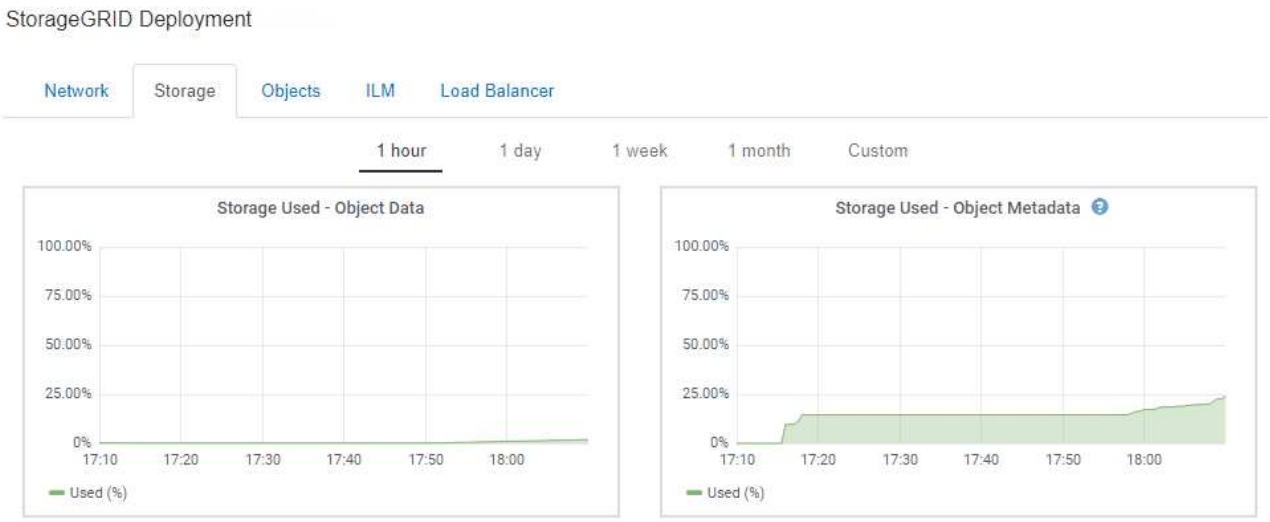
c. Clique no ícone do gráfico para o gráfico geral ou para um data center individual para exibir um gráfico que mostra o uso da capacidade ao longo do tempo.

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

2. Determine quanto storage foi usado e quanto storage permanece disponível para dados de objetos e metadados de objetos.

   a. Selecione **nós**.

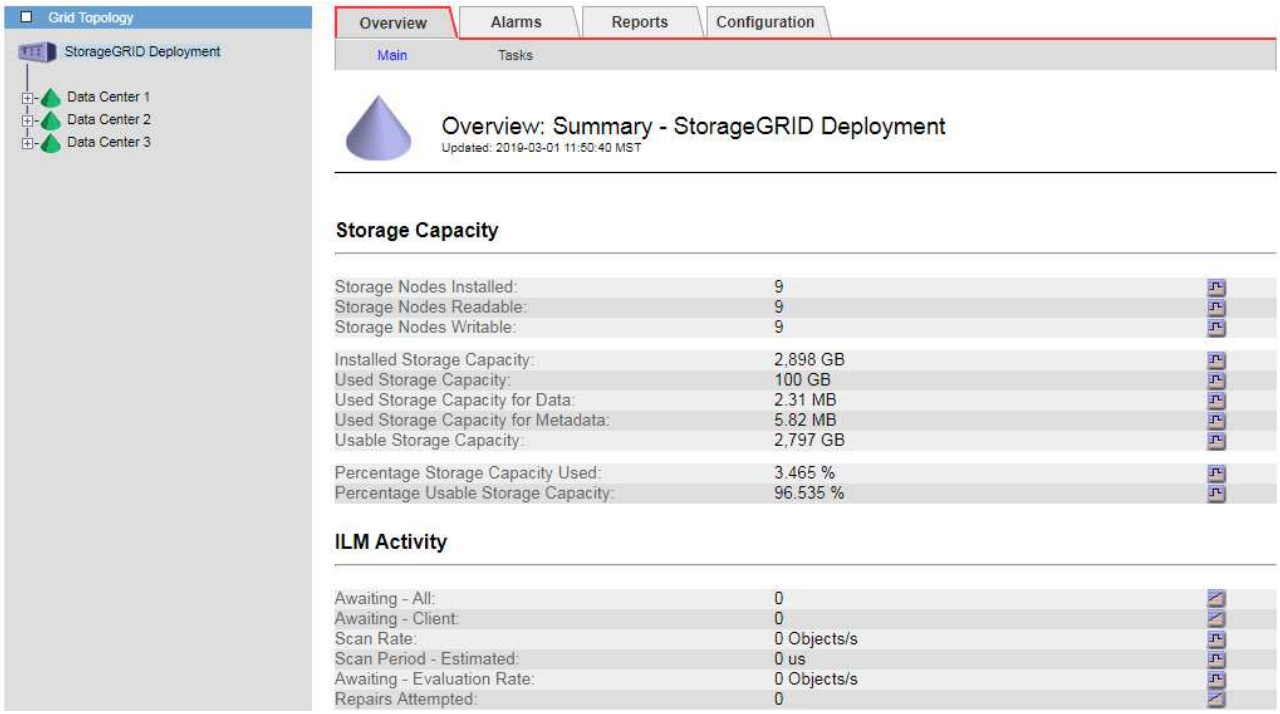
   b. Selecione ***grid* Storage**.



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

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

3. Conforme orientação do suporte técnico, veja detalhes adicionais sobre a capacidade de storage da sua grade.
   a. Selecione **Support** > **Tools** > **Grid Topology**.
   b. Selecione ***grid* Visão geral Principal**.



4. 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 as instruções para expandir o StorageGRID.

Informações relacionadas

"Expanda sua grade"

Monitoramento da capacidade de storage para cada nó de storage

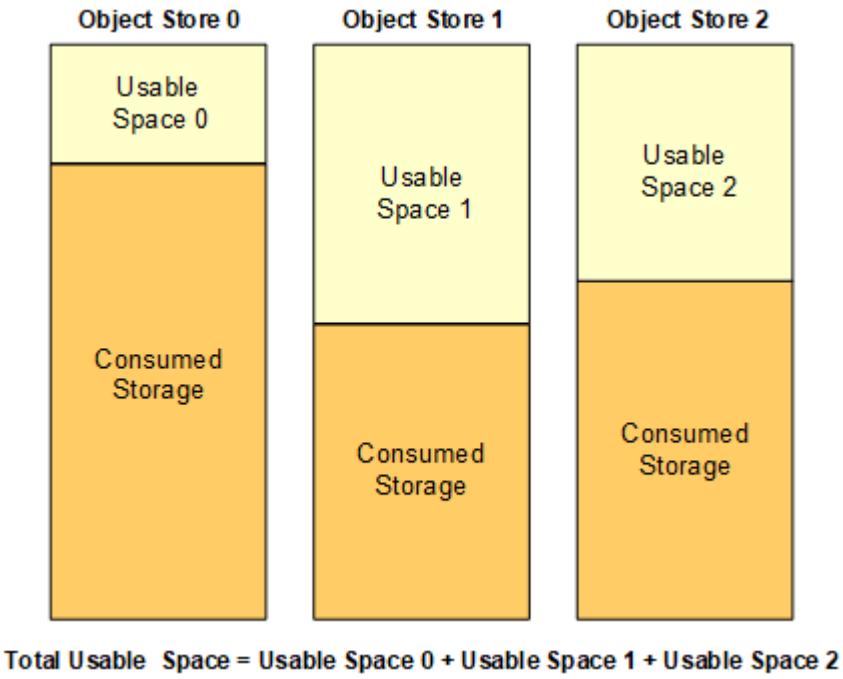
Você deve monitorar o espaço utilizável total para cada nó de storage para garantir que o nó tenha espaço suficiente para novos dados de objeto.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

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

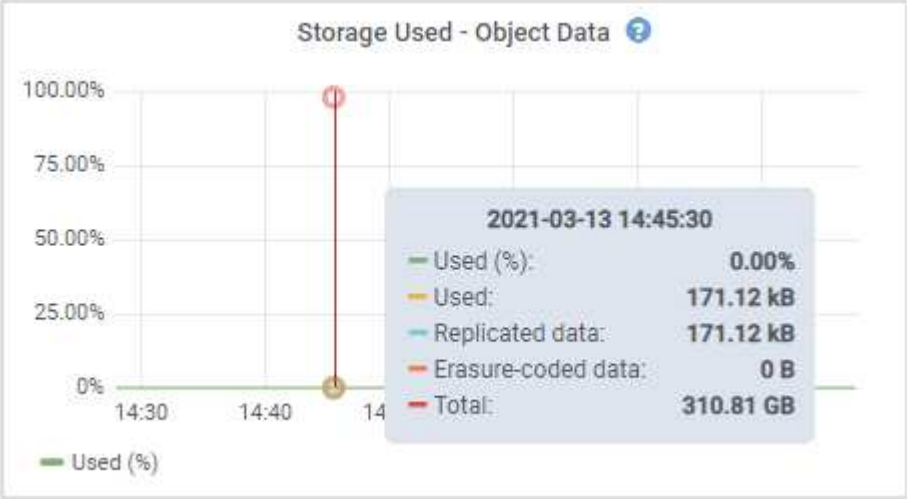
1. Selecione **nós *Storage Node* Storage**.

   Os gráficos e tabelas para o nó aparecem.

2. Passe o cursor sobre o gráfico Storage Used - Object Data (armazenamento usado - dados do objeto).

   São apresentados os seguintes valores:

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



3. Reveja os valores disponíveis nas tabelas volumes e Object Stores, 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	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 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 as instruções para expandir o StorageGRID.

   O alerta **armazenamento de dados de objeto baixo** e o alarme de estado de armazenamento legado (SSTS) são acionados quando o espaço insuficiente permanece para armazenar dados de objeto em um nó de armazenamento.

Informações relacionadas

"Administrar o StorageGRID"

"Solução de problemas do alerta de armazenamento de dados de objetos baixos"

"Expanda sua grade"

Monitoramento da capacidade dos metadados de objetos para cada nó de storage

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

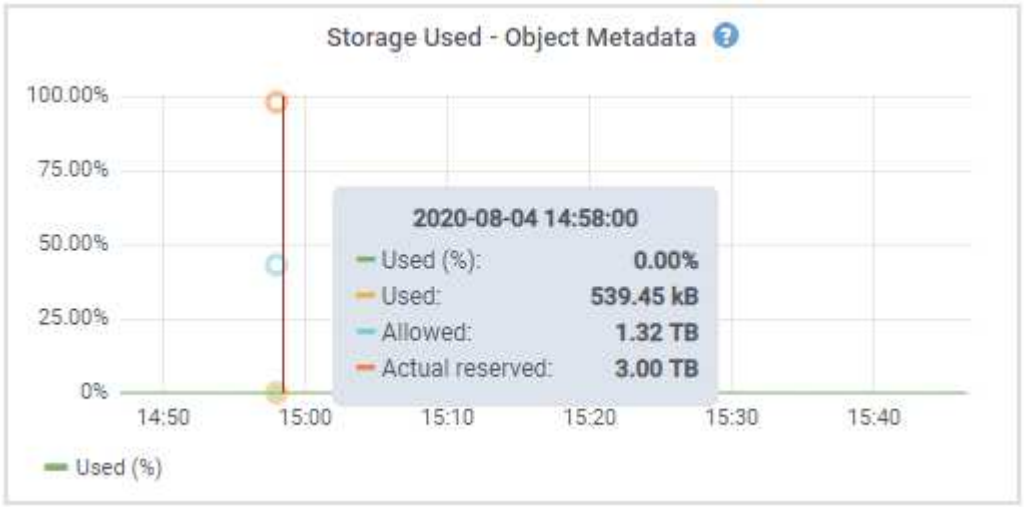
O StorageGRID mantém três cópias de metadados de objetos em cada local para fornecer redundância e proteger os metadados de objetos da perda. As três cópias são distribuídas uniformemente por todos os nós de storage em cada local, usando o espaço reservado para metadados no volume de storage 0 de cada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

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

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

Passos

1. Selecione **nós *Storage Node* Storage**.
2. Passe o cursor sobre o gráfico Storage Used - Object Metadata (armazenamento usado - metadados de objetos) para ver os valores de um tempo específico.



Valor	Descrição	Métrica Prometheus
Usado (%)	A porcentagem do espaço de metadados permitido que foi usado neste nó de storage.	`storagegrid_storage_utilization_metadata_bytes/ storagegrid_storage_utilization_metadata_allowed_bytes`
Usado	Os bytes do espaço de metadados permitido que foram usados neste nó de armazenamento.	`storagegrid_storage_utilization_metadata_bytes`
Permitido	O espaço permitido para metadados de objetos neste nó de storage. Para saber como este valor é determinado para cada nó de armazenamento, consulte as instruções para administrar o StorageGRID.	`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 as instruções para administrar o StorageGRID.	`storagegrid_storage_utilization_metadata_reserved_bytes`

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 as instruções para expandir um sistema StorageGRID.

Informações relacionadas

"Solução de problemas do alerta de armazenamento de metadados baixos"

"Administrar o StorageGRID"

"Expanda sua grade"

Monitoramento do gerenciamento do ciclo de vida das informações

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

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

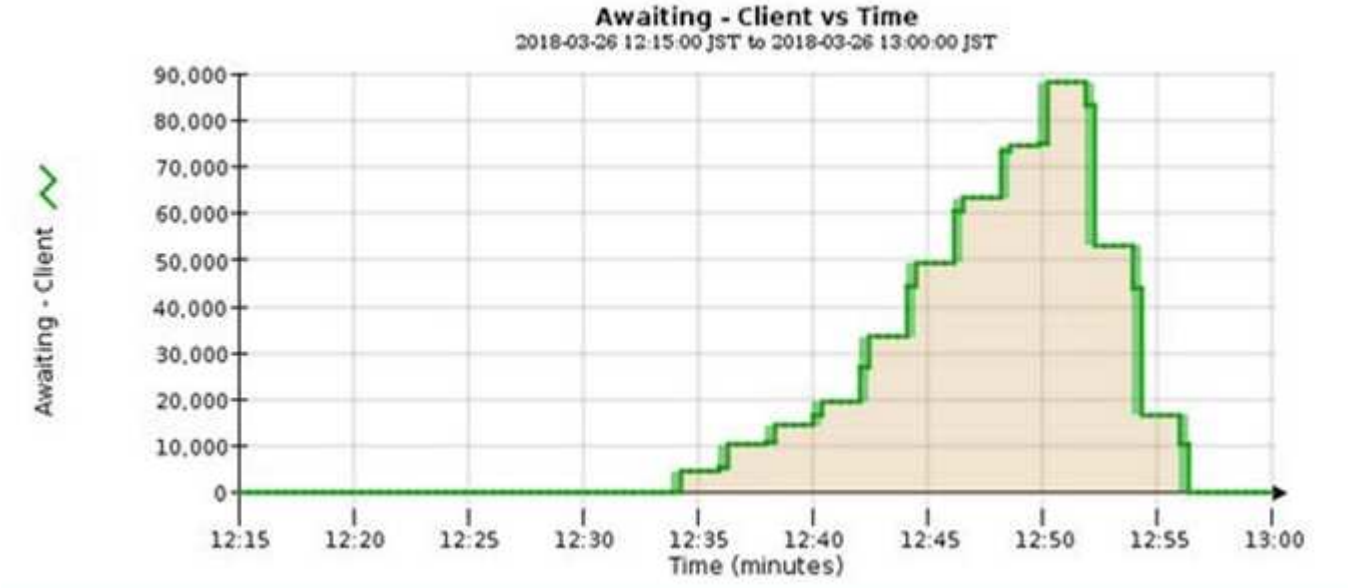
O sistema StorageGRID gerencia objetos aplicando a política ILM ativa. A política ILM e as regras ILM associadas determinam quantas cópias são feitas, o tipo de cópias que são criadas, onde as cópias são colocadas e o tempo de retenção de cada cópia.

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

Para traçar este atributo:

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

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



Picos temporários no gráfico de aguardando - o cliente deve ser esperado. Mas se o valor mostrado no gráfico

continuar a aumentar e nunca declinar, a grade requer mais recursos para operar com eficiência: Mais nós de storage ou, se a política ILM colocar objetos em locais remotos, mais largura de banda da rede.

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

Passos

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

   A secção fila ILM está incluída apenas para a grelha. 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.

Monitoramento de desempenho, rede e recursos do sistema

Você deve monitorar o desempenho, a rede e os recursos do sistema para determinar se o StorageGRID pode lidar com sua carga atual e garantir que o desempenho do cliente não diminua ao longo do tempo.

Ações do cliente, como armazenar, recuperar ou excluir objetos, criam consultas para o banco de dados distribuído da grade de metadados de objetos. Você deve monitorar tendências na latência da consulta para garantir que os recursos da grade sejam adequados para a carga atual.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

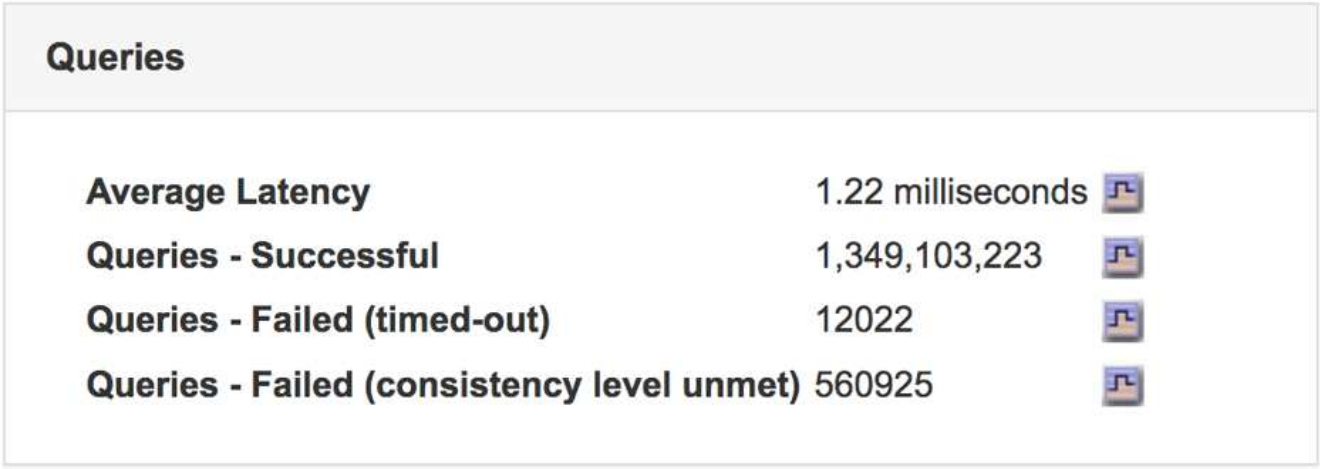
Aumentos temporários na latência de consulta são normais e podem ser causados por um aumento súbito nas solicitações de ingestão. As consultas falhadas também são normais e podem resultar de problemas de rede transitórios ou de nós que estão temporariamente indisponíveis. No entanto, se o tempo médio para realizar uma consulta aumentar, o desempenho geral da grade diminui.

Se você notar que a latência da consulta está aumentando com o tempo, considere adicionar nós de storage adicionais em um procedimento de expansão para atender a futuras cargas de trabalho.

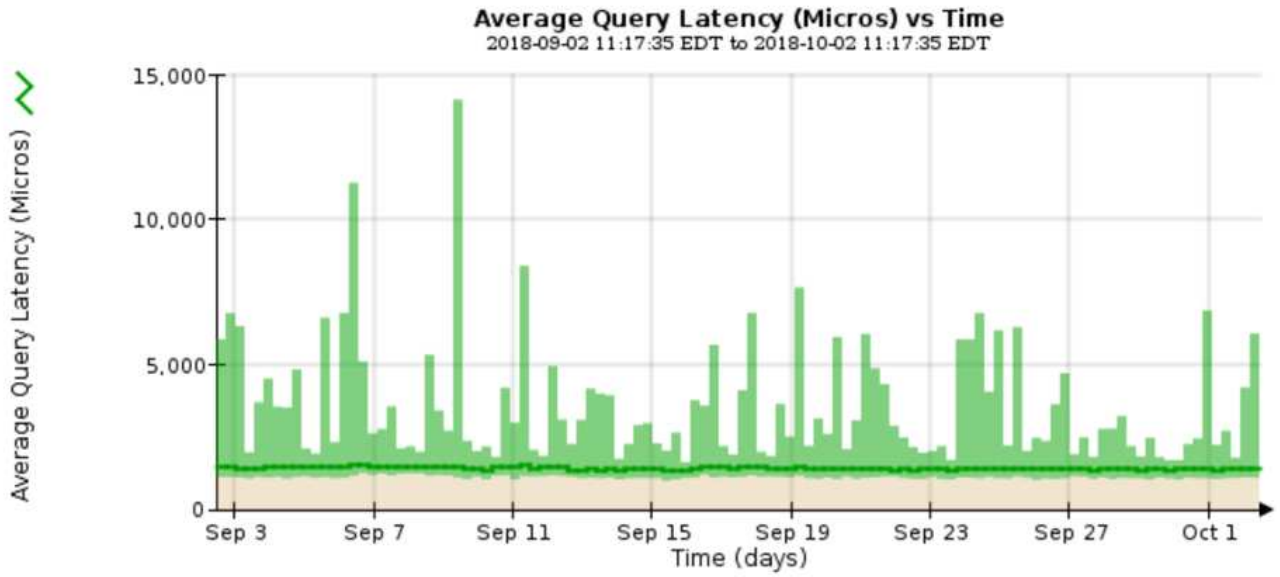
O alerta **alta latência para consultas de metadados** é acionado se o tempo médio para consultas for muito longo.

Passos

1. Selecione **nós *Storage Node* Objects**.
2. Role para baixo até a tabela consultas e exiba o valor da latência média.



3. Clique no ícone do gráfico para traçar o valor ao longo do tempo.



O gráfico de exemplo mostra picos na latência da consulta durante a operação normal da grade.

Informações relacionadas

"Expanda sua grade"

Monitoramento de conexões de rede e desempenho

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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 simplesmente a baixo desempenho de ingestão e backlogs de ILM.

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

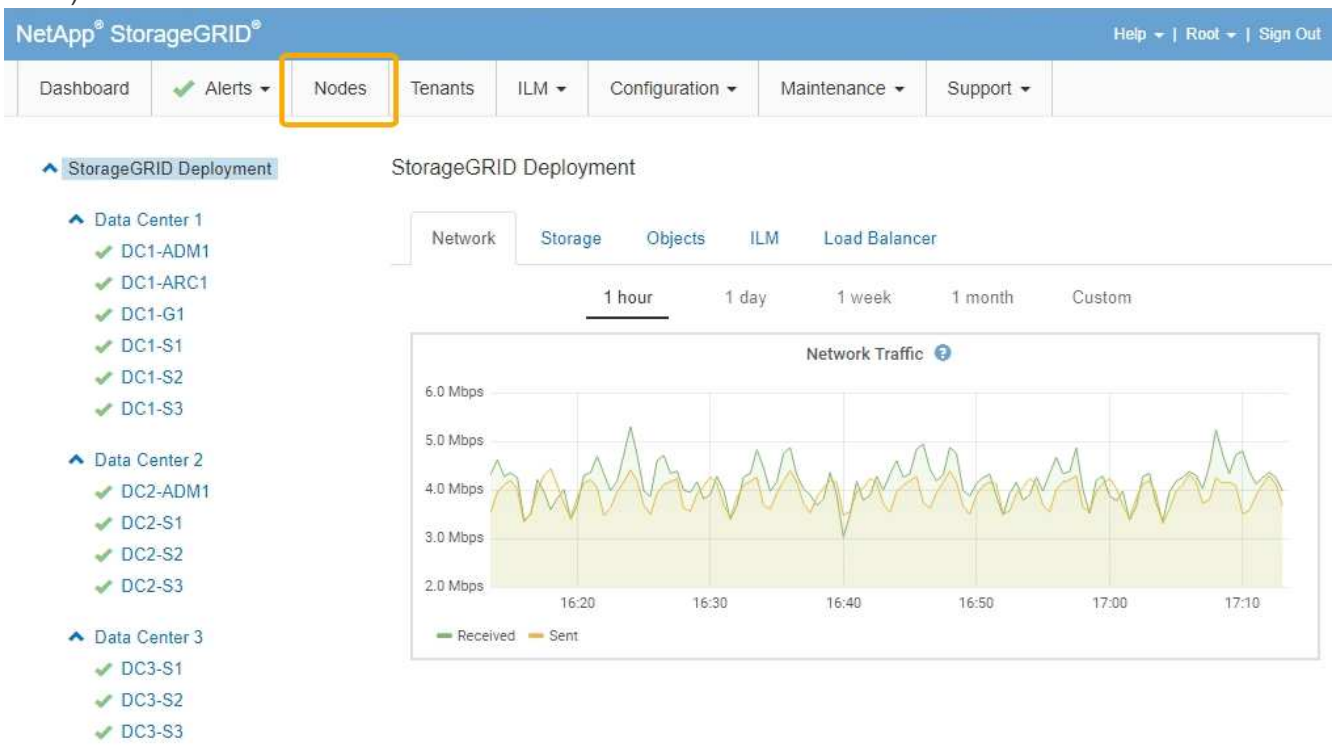
Além disso, considere criar políticas de classificação de tráfego de rede para fornecer monitoramento e limitação para o tráfego relacionado a locatários específicos, buckets, sub-redes ou pontos de extremidade do balanceador de carga. Consulte as instruções para administrar o StorageGRID.

Passos

1. Selecione **nós**.

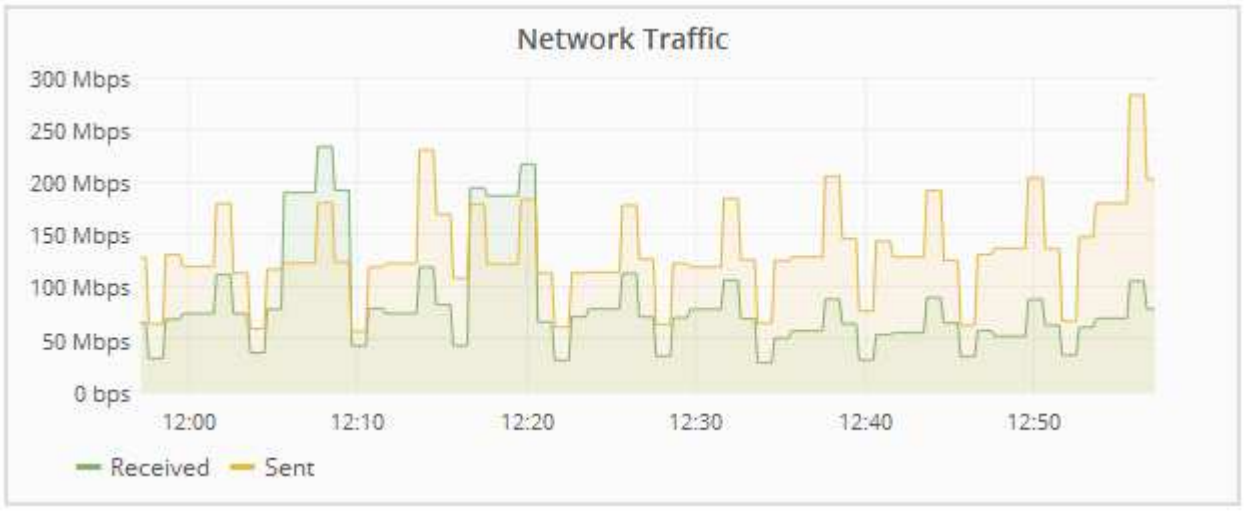
   A página nós é exibida. Os ícones de nó indicam rapidamente quais nós estão conetados (ícone de marca

de seleção verde) e quais nós estão desconetados (ícones azul ou cinza).



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

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



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

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	Up

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.

Network Communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

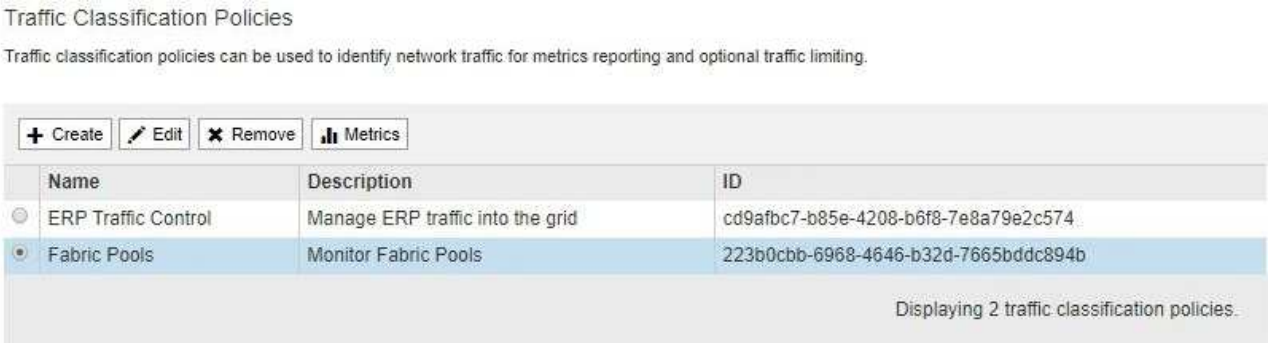
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

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

   a. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

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



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

c. Reveja os gráficos para compreender o tráfego de rede associado à política.

   Se uma política de classificação de tráfego for projetada para limitar o tráfego de rede, analise a frequência com que o tráfego é limitado e decida se a política continua atendendo às suas necessidades. De tempos em tempos, ajuste cada política de classificação de tráfego conforme necessário.

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

Informações relacionadas

"Visualizar o separador rede"

"Monitorização dos estados de ligação do nó"

"Administrar o StorageGRID"

Monitoramento de recursos no nível do nó

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

O que você vai precisar

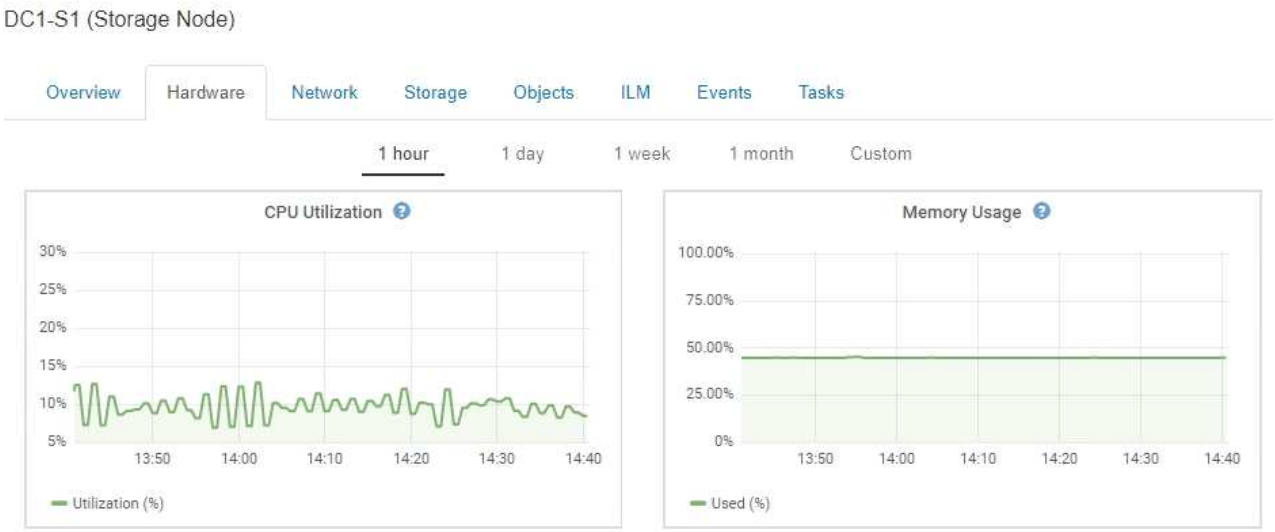
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

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

Passos

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



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

d. Se o nó estiver hospedado em um dispositivo de armazenamento ou em um dispositivo de serviços, role para baixo para exibir as tabelas de componentes. O status de todos os componentes deve ser "nominal". Investigue componentes que tenham qualquer outro status.

Informações relacionadas

"Exibição de informações sobre os nós de storage do dispositivo"

"Exibindo informações sobre nós de administração do dispositivo e nós de gateway"

Monitorar a atividade do locatário

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root ou Administrador.

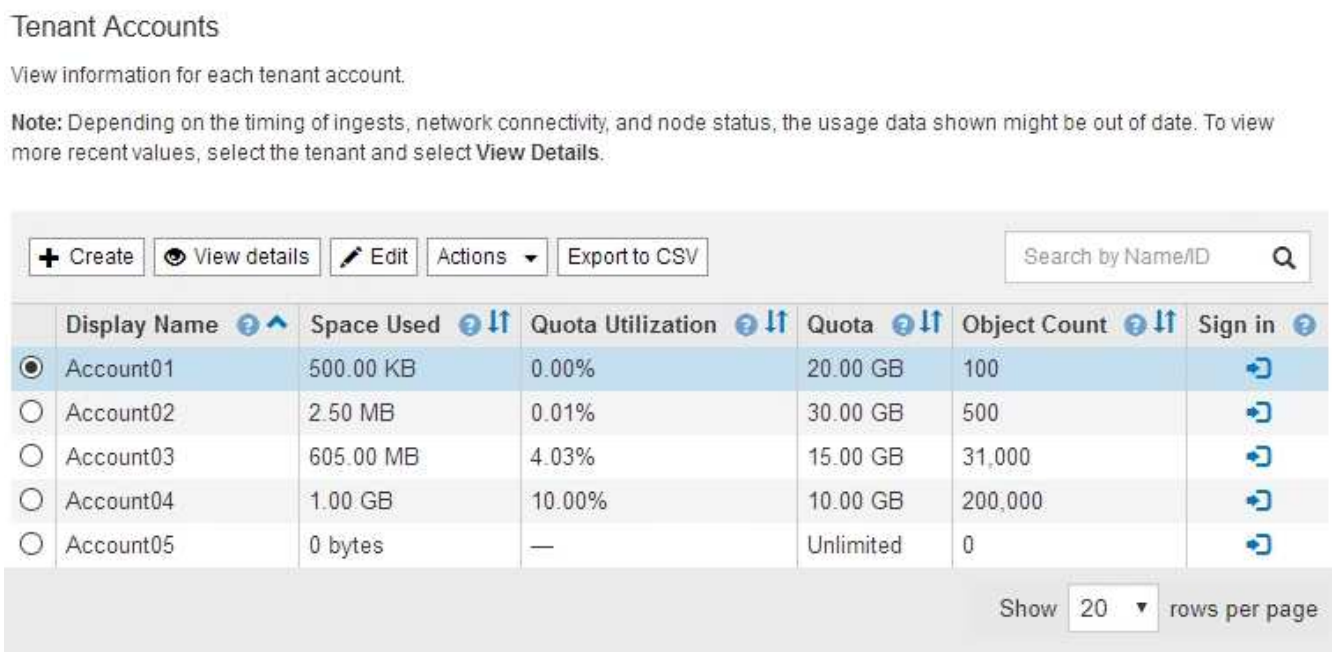
Sobre esta tarefa

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

Passos

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

   O espaço usado, a utilização da cota, a cota e a contagem de objetos são listados para cada locatário. Se uma cota não for definida para um locatário, o campo de utilização da cota contém um traço (--) e o campo de cota indica "ilimitado".



Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Use a caixa de pesquisa para procurar uma conta de locatário por nome de exibição ou ID de locatário.

Você pode entrar em uma conta de locatário selecionando o link na coluna **entrar** da tabela.

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

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

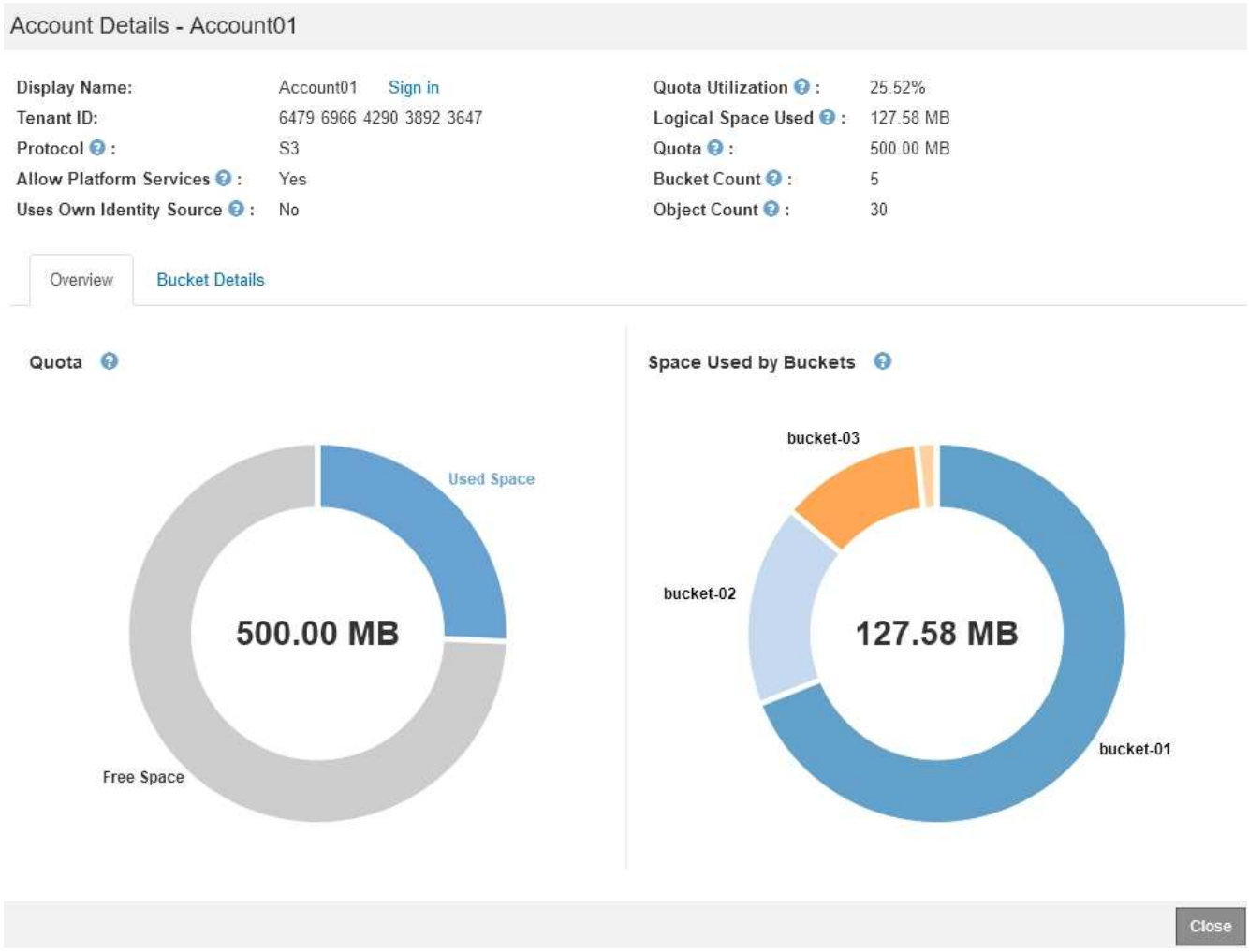
   O conteúdo de um arquivo .csv se parece com o seguinte exemplo:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
56243391454153665591	Account01	500000	0	20000000000	100	S3
82457136581801590515	Account02	2500000	0.01	30000000000	500	S3
04489086912300179118	Account03	605000000	4.03	15000000000	31000	S3
26417581662098345719	Account04	1000000000	10	10000000000	200000	S3
78472447501213318575	Account05	0			0	S3

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

3. Para exibir detalhes de um locatário específico, incluindo gráficos de uso, selecione a conta do locatário na página Contas do locatário e selecione **Exibir detalhes**.

   A página Detalhes da conta aparece e mostra informações resumidas, um gráfico que representa a quantidade de cota usada e restante, e um gráfico que representa a quantidade de dados de objeto em buckets (S3) ou contentores (Swift).



- **Quota**

  Se uma cota foi definida para esse locatário, o gráfico **quota** mostra quanto dessa cota esse locatário usou e quanto ainda está disponível. Se nenhuma cota foi definida, o locatário tem uma cota ilimitada e uma mensagem informativa é exibida. 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 segmento de espaço usado para ver o número de objetos armazenados e o total de bytes usados. Você pode colocar o cursor sobre o segmento de espaço livre para ver quantos bytes de cota de armazenamento estão disponíveis.

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

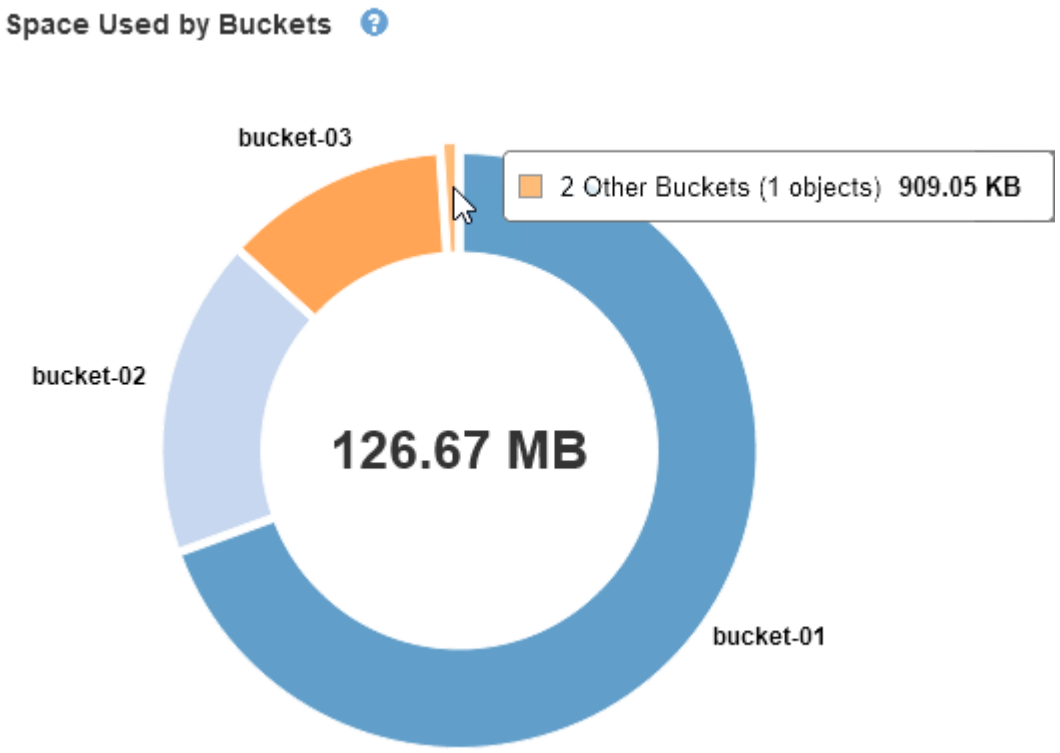
  > A utilização da cota de um locatário indica a quantidade total de dados de objeto que o locatário carregou para o StorageGRID (tamanho lógico). A utilização da cota não representa o espaço usado para armazenar cópias desses objetos e seus metadados (tamanho físico).

Você pode ativar o alerta **Alto uso da cota do locatário** para determinar se os locatários estão consumindo suas cotas. Se ativado, esse alerta é acionado quando um locatário usou 90% de sua cota. Para obter mais informações, consulte a referência de alertas.

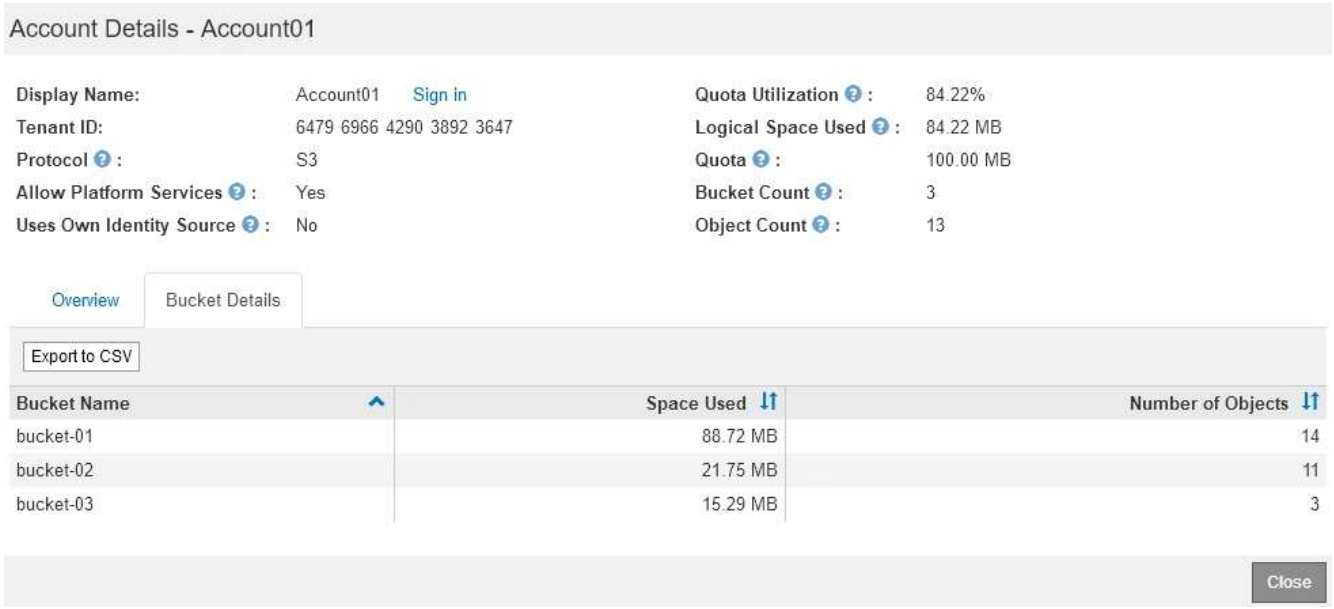
- **Espaço utilizado**

  O gráfico **espaço usado por baldes** (S3) ou **espaço usado por contentores** (Swift) mostra os maiores baldes para o inquilino. O espaço utilizado é a quantidade total de dados de objetos no intervalo. Esse valor não representa o espaço de storage necessário para cópias do ILM e metadados de objetos.

  Se o locatário tiver mais de nove buckets ou contentores, eles serão combinados em um segmento chamado outro. Alguns segmentos de gráfico podem ser muito pequenos para incluir um rótulo. Você pode colocar o cursor sobre qualquer um dos segmentos para ver o rótulo e obter mais informações, incluindo o número de objetos armazenados e o total de bytes para cada bucket ou contentor.



4. Selecione **Detalhes do balde** (S3) ou **Detalhes do contentor** (Swift) para visualizar uma lista do espaço usado e o número de objetos para cada um dos baldes ou contentores do locatário.



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

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

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

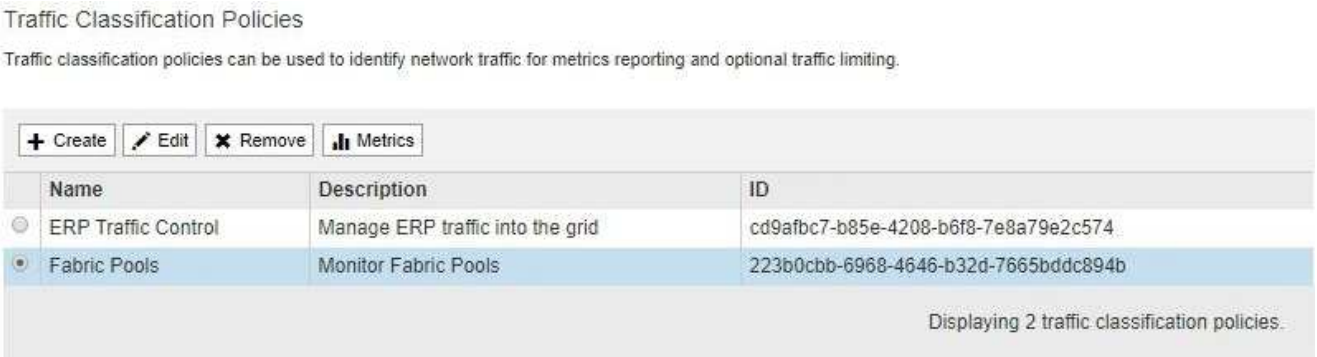
Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

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

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

   a. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

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



   a. Revise a lista de políticas para identificar as que se aplicam a um locatário específico.

   b. Para exibir métricas associadas a uma política, selecione o botão de opção à esquerda da política e clique em **métricas**.

c. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustar a política.

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

7. Opcionalmente, use o log de auditoria para monitoramento mais granular das atividades de um locatário.

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

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

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

8. Opcionalmente, use as métricas Prometheus para relatar a atividade do locatário:
   - No Gerenciador de Grade, selecione **suporte Ferramentas métricas**. 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.

   - Selecione **Ajuda Documentação da API**. Você pode usar as métricas na seção métricas da API de gerenciamento de grade para criar regras de alerta personalizadas e painéis para a atividade do locatário.

Informações relacionadas

"Referência de alertas"

"Rever registos de auditoria"

"Administrar o StorageGRID"

"Revisão das métricas de suporte"

Monitoramento da capacidade de arquivamento

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

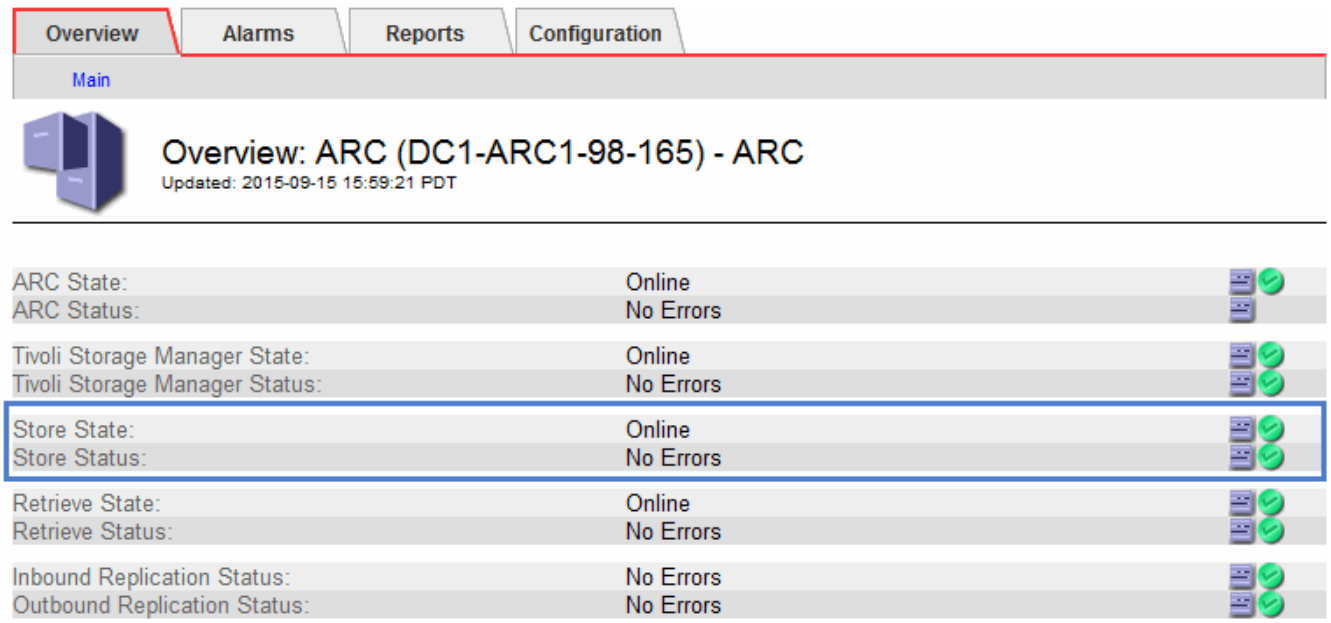
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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

Passos

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



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

Informações relacionadas

"Administrar o StorageGRID"

Monitoramento de operações de balanceamento de carga

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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

O serviço CLB está obsoleto.

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

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

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

Passos

1. Se os clientes S3 ou Swift se conetarem usando o serviço Load Balancer, verifique se os nós Admin ou os nós de Gateway estão distribuindo ativamente o tráfego como você espera:
   a. Selecione **nós**.
   b. Selecione um nó de gateway ou nó de administrador.
   c. Na guia **Visão geral**, verifique se uma interface de nó está em um grupo de HA e se a interface de nó tem a função de Mestre.

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

   d. Para cada nó que deve estar distribuindo ativamente solicitações de cliente, selecione a guia **Load Balancer**.
   e. Revise o gráfico de tráfego de solicitação do Load Balancer para a última semana para garantir que o nó esteja distribuindo solicitações ativamente.

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

   f. Revise o gráfico da taxa de solicitação de entrada do Load Balancer da última semana para analisar a taxa de transferência de objetos do nó.
   g. Repita estas etapas para cada nó de administrador ou nó de gateway no sistema StorageGRID.
   h. Opcionalmente, use políticas de classificação de tráfego para exibir uma discriminação mais detalhada do tráfego que está sendo servido pelo serviço Load Balancer.
2. Se os clientes S3 ou Swift se conetarem usando o serviço CLB (obsoleto), execute as seguintes verificações:
   a. Selecione **nós**.
   b. Selecione um nó de gateway.
   c. Na guia **Visão geral**, verifique se uma interface de nó está em um grupo HA e se a interface de nó tem a função de Mestre.

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

d. Para cada nó de gateway que deve estar distribuindo ativamente solicitações de cliente, selecione **suporte Ferramentas topologia de grade**.

e. Selecione ***Gateway Node* CLB HTTP Overview Main**.

f. Revise o número de **sessões de entrada - estabelecidas** para verificar se o Gateway Node tem lidado ativamente com solicitações.

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

a. Selecione ***Storage Node* LDR HTTP**.

b. Reveja o número de **sessões de entrada atualmente estabelecidas**.

c. Repita para cada nó de armazenamento na grade.

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

Informações relacionadas

"Administrar o StorageGRID"

"Exibindo a guia Load Balancer"

Aplicar hotfixes ou atualizar software, se necessário

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

Sobre esta tarefa

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

Passos

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

"NetApp Downloads: StorageGRID"

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

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

3. Reveja as alterações incluídas na atualização:

a. Selecione a versão no menu suspenso e clique em **Go**.

b. Inicie sessão utilizando o nome de utilizador e a palavra-passe da sua conta NetApp.

c. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.

É apresentada a página de transferências para a versão selecionada.

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

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

5. Se decidir que é necessária uma atualização de software, localize as instruções antes de prosseguir.
   - Para uma nova versão de software, siga cuidadosamente as instruções para atualizar o StorageGRID.
   - Para obter um hotfix, localize o procedimento de hotfix nas instruções de recuperação e manutenção

Informações relacionadas

"Atualizar o software"

"Manter recuperar"

Gerenciamento de alertas e alarmes

O sistema de alerta StorageGRID foi concebido para o informar sobre problemas operacionais que requerem a sua atenção. Conforme necessário, você também pode usar o sistema de alarme legado para monitorar seu sistema. Esta secção contém as seguintes subsecções:

- "Comparação de alertas e alarmes"
- "Gerenciamento de alertas"
- "Gerenciamento de alarmes (sistema legado)"

O StorageGRID inclui dois sistemas para informá-lo sobre problemas.

Sistema de alerta

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

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

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

Sistema de alarme legado

O sistema de alarme é suportado, mas é considerado um sistema legado. Como alertas, os alarmes são acionados em níveis específicos de gravidade quando os atributos atingem valores de limite definidos. No entanto, ao contrário dos alertas, muitos alarmes são acionados para eventos que você pode ignorar com

segurança, o que pode resultar em um número excessivo de notificações de e-mail ou SNMP.

Quando um alarme é acionado, ocorrem as seguintes acões:

- A contagem de alarmes legados no Dashboard é incrementada.
- O alarme aparece na página **suporte Alarmes (legado) Alarmes atuais**.
- Uma notificação por e-mail é enviada, supondo que você tenha configurado um servidor SMTP e configurado uma ou mais listas de e-mail.
- Uma notificação SNMP pode ser enviada, supondo que você tenha configurado o agente SNMP do StorageGRID. (As notificações SNMP não são enviadas para todos os alarmes ou gravidades de alarme.)

Comparação de alertas e alarmes

Há uma série de semelhanças entre o sistema de alerta e o sistema de alarme legado, mas o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

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

	Alertas	**Alarmes (sistema legado)**
Como posso ver quais alertas ou alarmes estão ativos?	• Clique no link **Current alerts** (alertas atuais*) no Dashboard. • Clique no alerta na página **nós Visão geral**. • Selecione **Alertas atual**. "Visualização de alertas atuais"	• Clique no link **Legacy Alarms** no Painel. • Selecione **suporte Alarmes (legado) Alarmes atuais**. "Visualização de alarmes legados"
O que faz com que um alerta ou um alerta seja acionado?	Os alertas são acionados quando uma expressão Prometheus em uma regra de alerta é avaliada como verdadeira para a condição e duração específicas do gatilho. "Visualizar regras de alerta"	Os alarmes são acionados quando um atributo StorageGRID atinge um valor limite. "Lógica de acionamento de alarme (sistema legado)"
Se um alerta ou alarme for acionado, como resolvo o problema subjacente?	As ações recomendadas para um alerta estão incluídas nas notificações por e-mail e estão disponíveis nas páginas Alertas no Gerenciador de Grade. Conforme necessário, informações adicionais são fornecidas na documentação do StorageGRID. "Referência de alertas"	Você pode aprender sobre um alarme clicando no nome do atributo ou pode procurar um código de alarme na documentação do StorageGRID. "Referência de alarmes (sistema legado)"

	Alertas	Alarmes (sistema legado)
Onde posso ver uma lista de alertas ou alarmes resolvidos?	• Clique no link **alertas resolvidos recentemente** no Dashboard. • Selecione **Alertas resolvido**. "Visualização de alertas resolvidos"	Selecione **suporte Alarmes (legado) Alarmes históricos**. "Revisão de alarmes históricos e frequência de alarmes (sistema legado)"
Onde posso gerir as definições?	Selecione **Alertas**. Em seguida, use as opções no menu Alertas. "Gerenciamento de alertas"	Selecione **suporte**. Em seguida, use as opções na seção **Alarmes (legacy)** do menu. "Gerenciamento de alarmes (sistema legado)"
Quais permissões do grupo de usuários eu preciso?	• Qualquer pessoa que possa entrar no Gerenciador de Grade pode exibir alertas atuais e resolvidos. • Você deve ter a permissão Gerenciar Alertas para gerenciar silêncios, notificações de alerta e regras de alerta. "Administrar o StorageGRID"	• Qualquer pessoa que possa entrar no Gerenciador de Grade pode exibir alarmes legados. • Você deve ter a permissão reconhecer alarmes para reconhecer alarmes. • Você deve ter as permissões Configuração da Página de topologia de Grade e outras permissões de Configuração de Grade para gerenciar alarmes globais e notificações por e-mail. "Administrar o StorageGRID"
Como faço para gerenciar notificações por e-mail?	Selecione **Alertas Configuração de e-mail**. **Nota:** como os alarmes e alertas são sistemas independentes, a configuração de e-mail usada para notificações de alarme e AutoSupport não é usada para notificações de alerta. No entanto, você pode usar o mesmo servidor de e-mail para todas as notificações. "Gerenciando notificações de alerta"	Selecione **suporte Alarmes (legado) Configuração de e-mail legado**. "Configurar notificações para alarmes (sistema legado)"

	Alertas	Alarmes (sistema legado)
Como faço para gerenciar notificações SNMP?	Selecione **Configuração Monitoramento Agente SNMP**. "Utilizar a monitorização SNMP"	Selecione **Configuração Monitoramento Agente SNMP**. "Utilizar a monitorização SNMP" **Nota**: As notificações SNMP não são enviadas para cada alarme ou gravidade do alarme. "Alarmes que geram notificações SNMP (sistema legado)"
Como posso controlar quem recebe notificações?	1. Selecione **Alertas Configuração de e-mail**. 2. Na seção **destinatários**, insira um endereço de e-mail para cada lista de e-mail ou pessoa que deve receber um e-mail quando ocorrer um alerta. "Configurar notificações por e-mail para alertas"	1. Selecione **suporte Alarmes (legado) Configuração de e-mail legado**. 2. Criando uma lista de discussão. 3. Selecione **notificações**. 4. Selecione a lista de discussão. "Criando listas de discussão para notificações de alarme (sistema legado)" "Configurar notificações por e-mail para alarmes (sistema legado)"
Quais nós de administrador enviam notificações?	Um único nó Admin (o "'remetente preferido'"). "Administrar o StorageGRID"	Um único nó Admin (o "'remetente preferido'"). "Administrar o StorageGRID"
Como faço para suprimir algumas notificações?	1. Selecione **Alertas silêncios**. 2. Selecione a regra de alerta que deseja silenciar. 3. Especifique uma duração para o silêncio. 4. Selecione a gravidade do alerta que deseja silenciar. 5. Selecione para aplicar o silêncio a toda a grade, a um único local ou a um único nó. **Nota**: Se você ativou o agente SNMP, os silêncios também suprimem traps SNMP e informam. "Silenciar notificações de alerta"	1. Selecione **suporte Alarmes (legado) Configuração de e-mail legado**. 2. Selecione **notificações**. 3. Selecione uma lista de discussão e selecione **suprimir**. "Suprimir notificações de alarme para uma lista de correio (sistema legado)"

	Alertas	Alarmes (sistema legado)
Como faço para suprimir todas as notificações?	Selecione **Alertas silêncios**.em seguida, selecione **todas as regras**. **Nota**: Se você ativou o agente SNMP, os silêncios também suprimem traps SNMP e informam. "Silenciar notificações de alerta"	1. Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**. 2. Marque a caixa de seleção **notificação suprimir tudo**. **Nota**: A supressão de notificações por e-mail em todo o sistema também suprime os e-mails do AutoSupport acionados por eventos. "Suprimindo o sistema de notificações por e-mail"
Como posso personalizar as condições e os gatilhos?	1. Selecione **Alertas regras de alerta**. 2. Selecione uma regra padrão para editar ou selecione **criar regra personalizada**. "Editar uma regra de alerta" "Criando regras de alerta personalizadas"	1. Selecione **suporte Alarmes (legado) Alarmes globais**. 2. Crie um alarme personalizado global para substituir um alarme padrão ou para monitorar um atributo que não tenha um alarme padrão. "Criação de alarmes personalizados globais (sistema legado)"
Como posso desativar um alerta individual ou um alarme?	1. Selecione **Alertas regras de alerta**. 2. Selecione a regra e clique em **Editar regra**. 3. Desmarque a caixa de seleção **Enabled**. "Desativar uma regra de alerta"	1. Selecione **suporte Alarmes (legado) Alarmes globais**. 2. Selecione a regra e clique no ícone Editar. 3. Desmarque a caixa de seleção **Enabled**. "Desativar um alarme predefinido (sistema legado)" "Desativar alarmes personalizados globais (sistema legado)"

Gerenciamento de alertas

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

Informações relacionadas

"Visualização de alertas atuais"

"Visualização de alertas resolvidos"

"Visualizar um alerta específico"

"Referência de alertas"

Quais são os 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.

- O sistema de alerta se concentra em problemas acionáveis no sistema. Ao contrário de alguns alarmes no sistema legado, os alertas são acionados para eventos que exigem sua atenção imediata, não para eventos que podem ser ignorados com segurança.
- A página Alertas atuais fornece uma interface amigável para visualizar problemas atuais. Você pode classificar a lista por alertas individuais e grupos de alertas. Por exemplo, talvez você queira classificar todos os alertas por nó/site para ver quais alertas estão afetando um nó específico. Ou, talvez você queira classificar os alertas em um grupo por tempo acionado para encontrar a instância mais recente de um alerta específico.
- A página Alertas resolvidos fornece informações semelhantes às da página Alertas atuais, mas permite pesquisar e visualizar um histórico dos alertas que foram resolvidos, incluindo quando o alerta foi acionado e quando foi resolvido.
- Vários alertas do mesmo tipo são agrupados em um e-mail para reduzir o número de notificações. Além disso, vários alertas do mesmo tipo são exibidos como um grupo na página Alertas. Você pode expandir e recolher grupos de alerta para mostrar ou ocultar os alertas individuais. Por exemplo, se vários nós relatarem o alerta **não é possível se comunicar com o nó** aproximadamente ao mesmo tempo, somente um email é enviado e o alerta é mostrado como um grupo na página Alertas.
- Os alertas usam nomes e descrições intuitivas para ajudá-lo a entender rapidamente o problema. As notificações de alerta incluem detalhes sobre o nó e o site afetado, a gravidade do alerta, o tempo em que a regra de alerta foi acionada e o valor atual das métricas relacionadas ao alerta.
- As notificações de e-mails de alerta e as listagens de alerta nas páginas Alertas atuais e alertas resolvidos fornecem ações recomendadas para resolver um alerta. Essas ações recomendadas geralmente incluem links diretos para o centro de documentação do StorageGRID para facilitar a localização e o acesso a procedimentos de solução de problemas mais detalhados.
- Se você precisar suprimir temporariamente as notificações de um alerta em um ou mais níveis de gravidade, poderá silenciar facilmente uma regra de alerta específica por uma duração especificada e para toda a grade, um único local ou um único nó. Você também pode silenciar todas as regras de alerta, por exemplo, durante um procedimento de manutenção planejado, como uma atualização de software.
- Você pode editar as regras de alerta padrão conforme necessário. Você pode desativar completamente uma regra de alerta ou alterar suas condições de ativação e duração.
- Você pode criar regras de alerta personalizadas para direcionar as condições específicas que são relevantes para a sua situação e para fornecer suas próprias ações recomendadas. Para definir as condições para um alerta personalizado, você cria expressões usando as métricas Prometheus disponíveis na seção métricas da API de Gerenciamento de Grade.

Gerenciando regras de alerta

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

personalizadas.

Visualizar regras de alerta

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

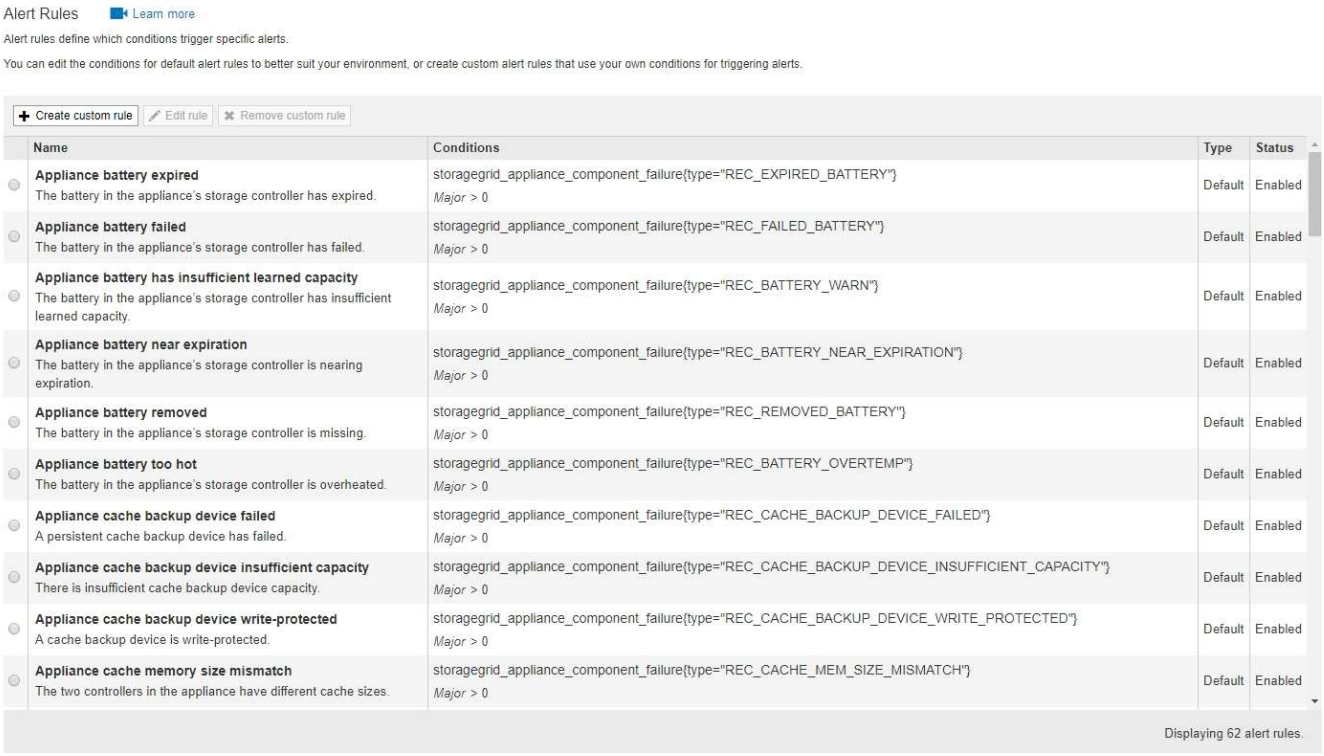
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Gerenciar Alertas ou acesso root.

Passos

1. Selecione **Alertas regras de alerta**.

   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.

Cabeçalho da coluna	Descrição
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.

Informações relacionadas

"Referência de alertas"

Criando regras de alerta personalizadas

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Gerenciar Alertas ou acesso root.

Sobre esta tarefa

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

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

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

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

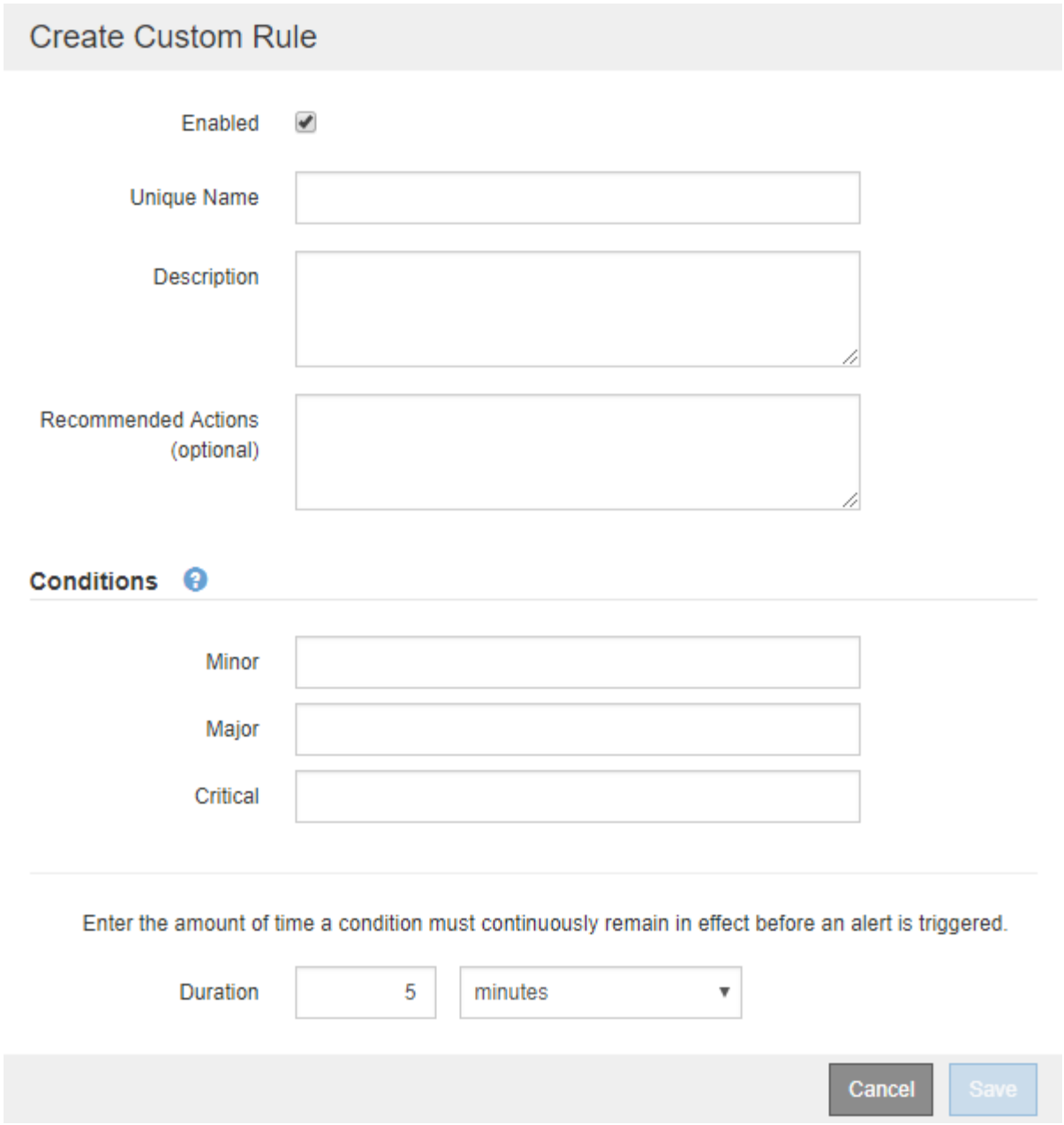
Passos

1. Selecione **Alertas regras de alerta**.

   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.

   Para ver as métricas disponíveis e testar expressões Prometheus, clique no ícone de ajuda e siga o link para a seção métricas da API de Gerenciamento de Grade.

   Para saber mais sobre como usar a API de gerenciamento de grade, consulte as instruções para administrar o StorageGRID. Para obter detalhes sobre a sintaxe das consultas Prometheus, consulte a documentação do Prometheus.

   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
   ```

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. Clique em **Salvar**.

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

Informações relacionadas

"Administrar o StorageGRID"

"Métricas de Prometheus comumente usadas"

"Prometheus: Noções básicas de consulta"

Editar uma regra de alerta

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Gerenciar Alertas ou acesso root.

Sobre esta tarefa

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

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

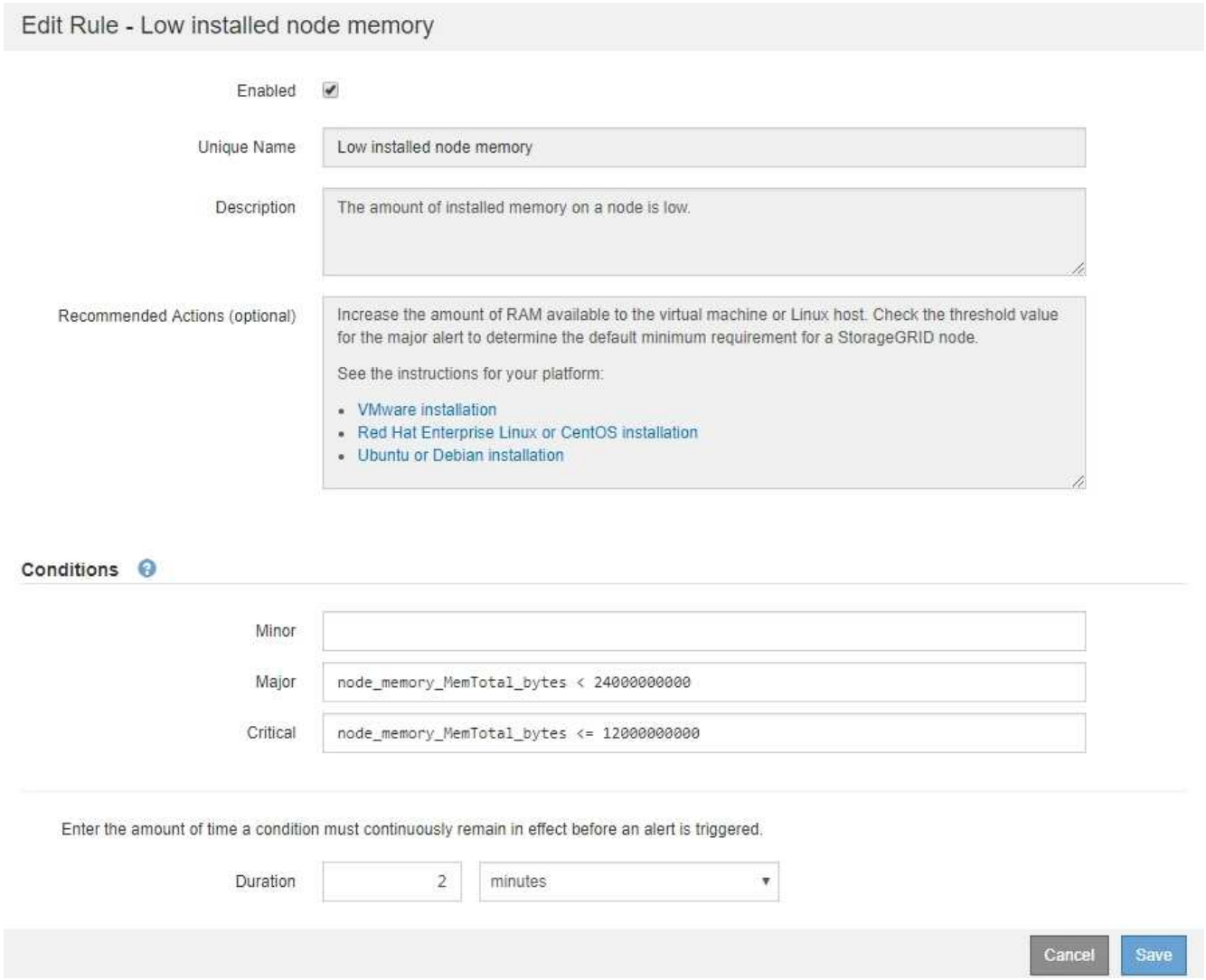
Passos

1. Selecione **Alertas regras de alerta**.

   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.

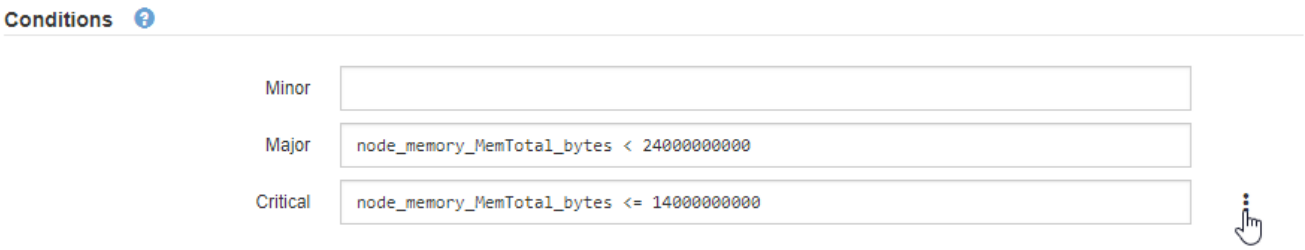
5. Para regras de alerta personalizadas, atualize as seguintes informações conforme necessário.

   > 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, clique nos 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.

Para ver as métricas disponíveis e testar expressões Prometheus, clique no ícone de ajuda e siga o link para a seção métricas da API de Gerenciamento de Grade.

Para saber mais sobre como usar a API de gerenciamento de grade, consulte as instruções para administrar o StorageGRID. Para obter detalhes sobre a sintaxe das consultas Prometheus, consulte a documentação do Prometheus.

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. Clique em **Salvar**.

   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**.

Informações relacionadas

"Administrar o StorageGRID"

"Métricas de Prometheus comumente usadas"

"Prometheus: Noções básicas de consulta"

Desativar uma regra de alerta

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Gerenciar Alertas ou acesso root.

Sobre esta tarefa

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

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

Passos

1. Selecione **Alertas regras de alerta**.

   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. Clique em **Salvar**.

   Disabled aparece na coluna **Status**.

Removendo uma regra de alerta personalizada

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Gerenciar Alertas ou acesso root.

Passos

1. Selecione **Alertas regras de alerta**.

   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. Clique em **Remover regra personalizada**.

   É apresentada uma caixa de diálogo de confirmação.

4. Clique em **OK** para remover a regra de alerta.

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

Gerenciando notificações de alerta

Quando um alerta é acionado, o StorageGRID pode enviar notificações por e-mail e notificações (traps) de Protocolo de Gerenciamento de rede simples (SNMP).

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.

Sobre esta tarefa

Você pode usar a opção **Configuração Monitoramento Agente SNMP** 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, consulte a seção para usar o monitoramento SNMP.

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. As notificações de alerta são enviadas por qualquer nó Admin configurado para ser o remetente preferido. Por padrão, o nó de administração principal é selecionado. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

> Notificações de intercetação e informação também são enviadas quando certos alarmes (sistema legado) são acionados em níveis de gravidade especificados ou superiores; no entanto, as notificações SNMP não são enviadas para cada alarme ou para cada gravidade de alarme.

Informações relacionadas

"Utilizar a monitorização SNMP"

"Silenciar notificações de alerta"

"Administrar o StorageGRID"

"Alarmes que geram notificações SNMP (sistema legado)"

Configurar notificações por e-mail para alertas

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Gerenciar Alertas ou acesso root.

O que você vai precisar

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

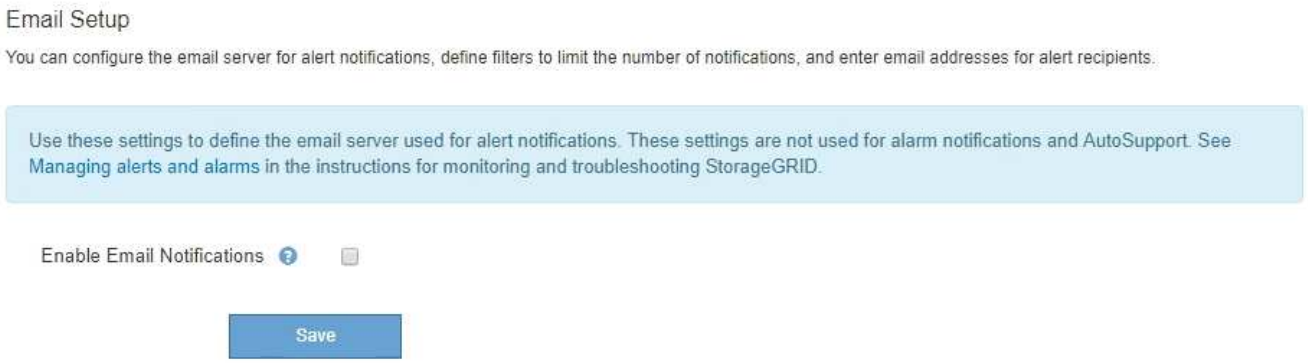
Se sua implantação do StorageGRID incluir vários nós de administração, você poderá selecionar qual nó de

administração deve ser o remetente preferido das notificações de alerta. O mesmo ""remetente preferido"" também é usado para notificações de alarme e mensagens AutoSupport. Por padrão, o nó de administração principal é selecionado. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

Passos

1. Selecione **Alertas Configuração de 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. Você também deve exigir TLS e fornecer um certificado de CA.

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.

      Clique no ícone de mais ✚para adicionar destinatários.

5. Na seção Transport Layer Security (TLS), marque a caixa de seleção **Require TLS** se a Transport Layer Security (TLS) for necessária para comunicações com o servidor SMTP.

   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 clique em **Procurar** e selecione o arquivo.

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

   b. Marque a caixa de seleção **Enviar certificado de cliente** se o servidor de e-mail SMTP exigir que os remetentes de e-mail forneçam certificados de cliente para autenticação.

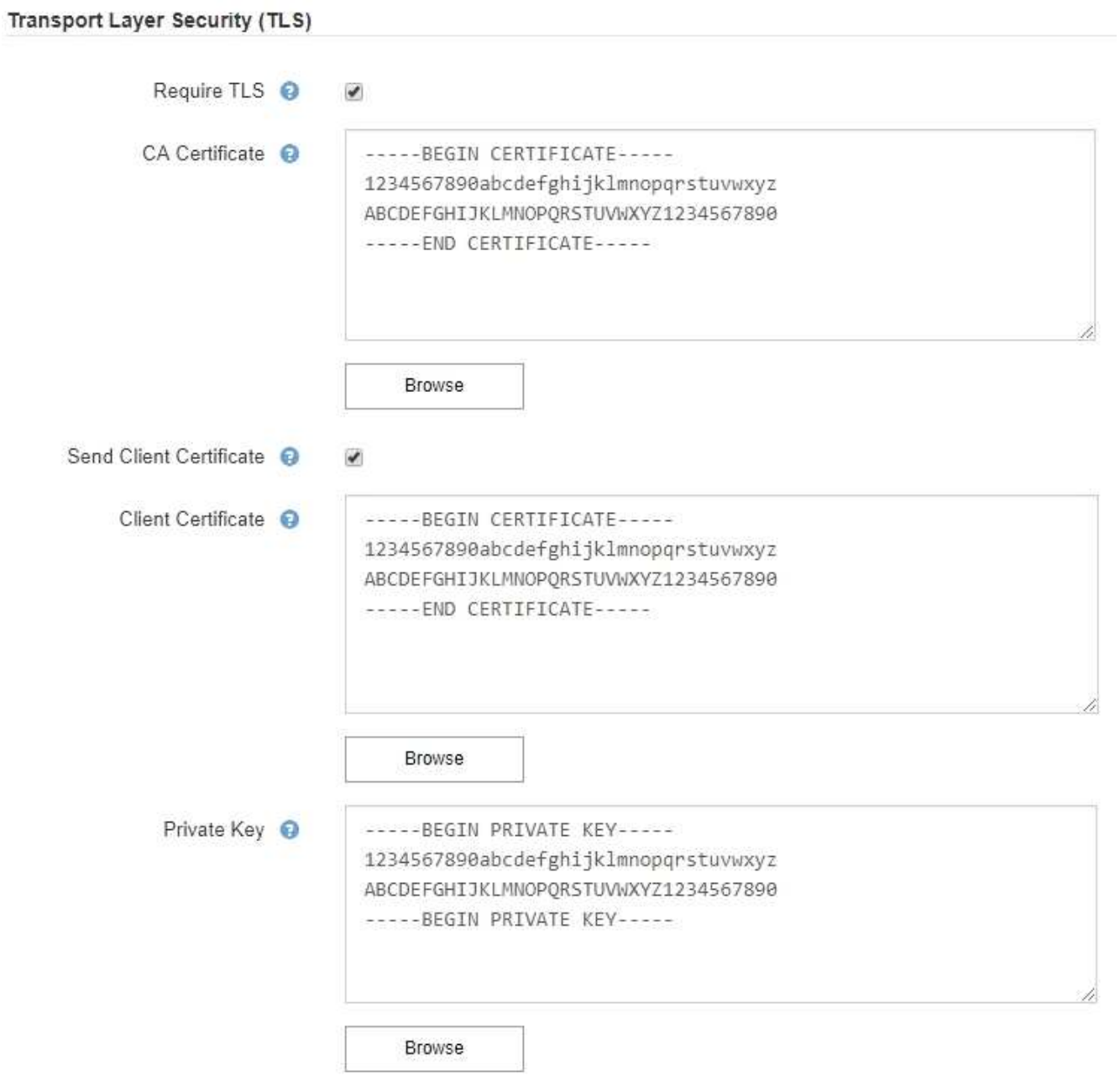
   c. No campo **Client Certificate**, forneça o certificado de cliente codificado em PEM para enviar para o servidor SMTP.

      Você pode copiar e colar o conteúdo neste campo, ou clique em **Procurar** e selecione 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 clique em **Procurar** e selecione o arquivo.

Se você precisar editar a configuração do e-mail, clique no ícone de lápis para atualizar esse 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.

Gravidade	Descrição
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. Clique em **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 notificações de alarme e mensagens AutoSupport, onde todos os nós de administração enviam o e-mail de teste.

8. Clique em **Salvar**.

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

   As configurações de e-mail são salvas.

Informações relacionadas

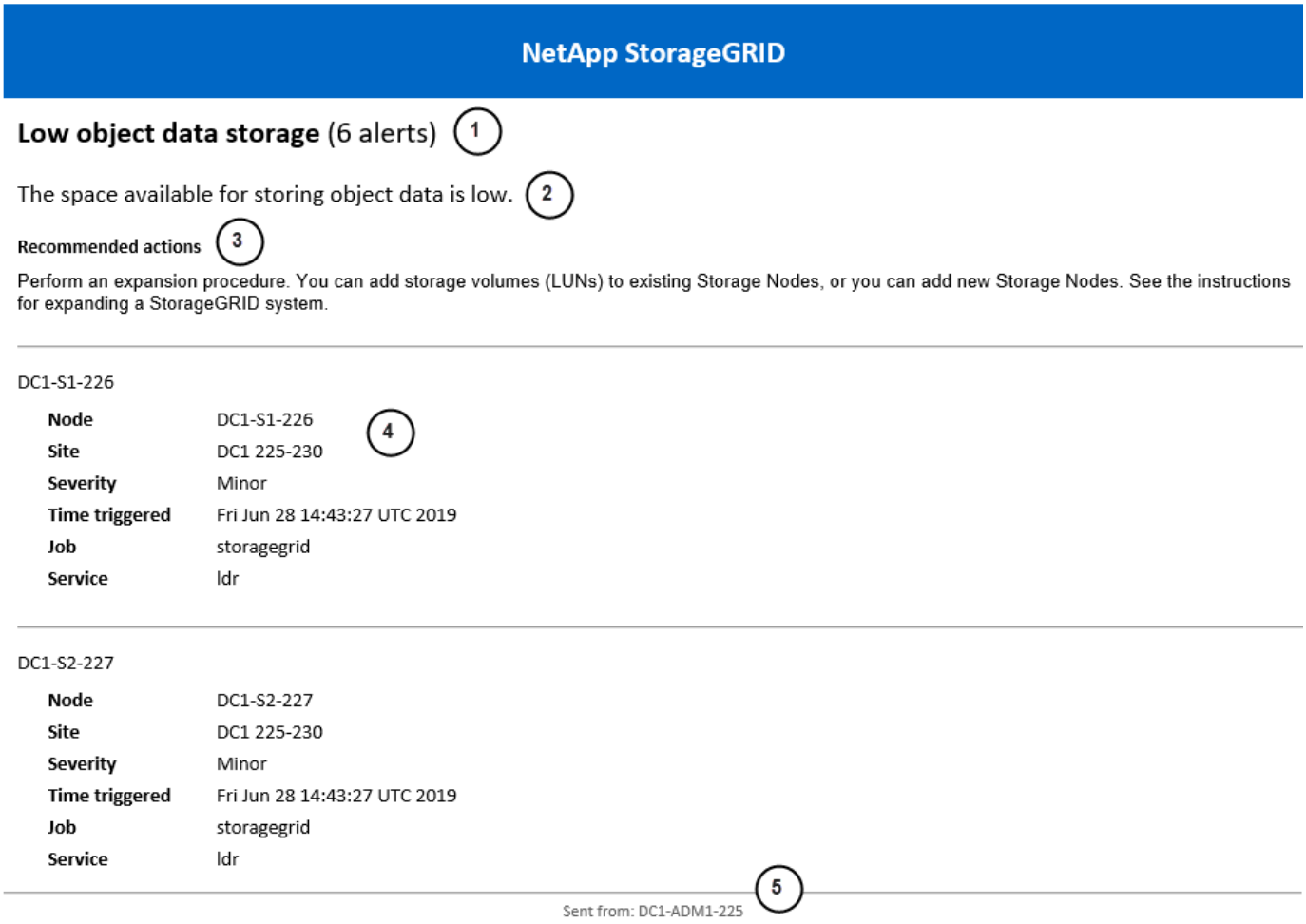
"Solução de problemas de notificações por e-mail de alerta"

"Manter recuperar"

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.

As notificações por e-mail incluem as seguintes informações:



	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.

Informações relacionadas

"Silenciar notificações de alerta"

Como o StorageGRID agrupa alertas em notificações por e-mail

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.

Comportamento	Exemplo
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.

Solução de problemas de notificações por e-mail de alerta

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Gerenciar Alertas ou acesso root.

Passos

1. Verifique as suas definições.
   a. Selecione **Alertas Configuração de e-mail**.
   b. Verifique se as configurações do servidor de e-mail (SMTP) estão corretas.
   c. Verifique se você especificou endereços de e-mail válidos para os destinatários.
2. Verifique 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.

Informações relacionadas

"Coletando arquivos de log e dados do sistema"

Silenciar notificações de alerta

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Gerenciar Alertas ou acesso root.

Sobre esta tarefa

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

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

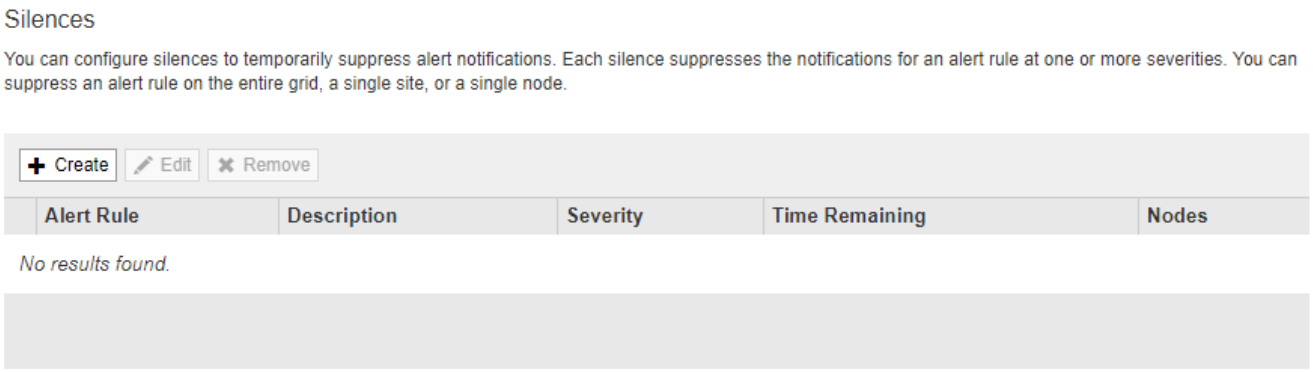
Tenha cuidado ao decidir silenciar uma regra de alerta. Se você silenciar um alerta, talvez não detete um problema subjacente até que ele impeça que uma operação crítica seja concluída.

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

Passos

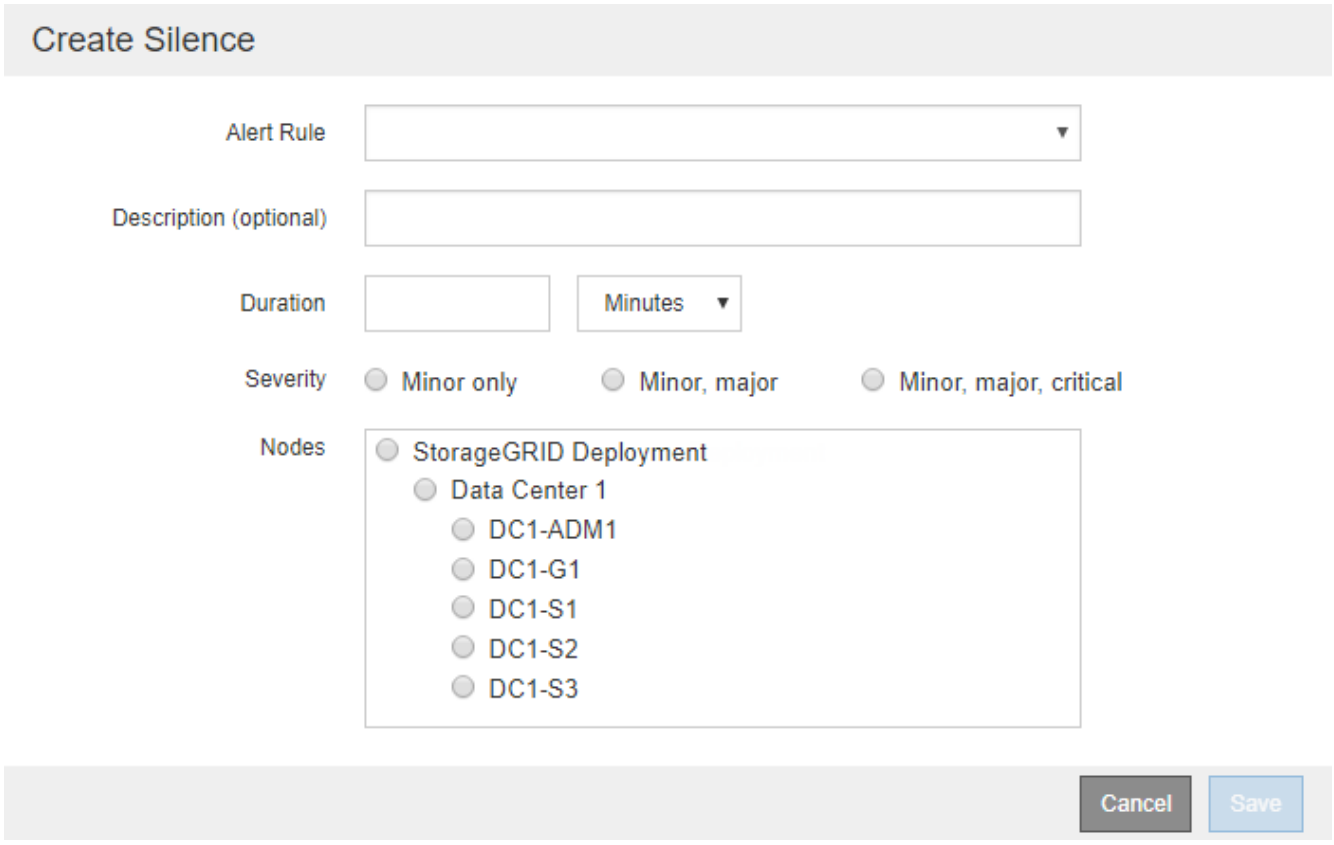
1. Selecione **Alertas silêncios**.

   É apresentada a página silêncios.



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.
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. Clique em **Salvar**.
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. Clique em **Editar**. d. Altere a descrição, a quantidade de tempo restante, as severidades selecionadas ou o nó afetado. e. Clique em **Salvar**.

Opção	Descrição
Remova um silêncio	a. Selecione **Alertas silêncios**. b. Na tabela, selecione o botão de opção para o silêncio que deseja remover. c. Clique em **Remover**. d. Clique em **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

"Configurando o agente SNMP"

Gerenciamento de alarmes (sistema legado)

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

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

Informações relacionadas

"Referência de alarmes (sistema legado)"

"Visualização de alarmes legados"

"Administrar o StorageGRID"

Classes de alarme (sistema legado)

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

Alarmes predefinidos

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

Alarmes personalizados globais

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

Informações relacionadas

"Visualizar alarmes predefinidos (sistema legado)"

"Desativar um alarme predefinido (sistema legado)"

"Criação de alarmes personalizados globais (sistema legado)"

"Desativar alarmes personalizados globais (sistema legado)"

Lógica de acionamento de alarme (sistema legado)

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

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

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

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

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

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

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

Exemplo de acionamento de alarmes

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

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

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

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

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

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

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

Alarmes da mesma gravidade

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

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

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

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	Under 5(	=	5000		
☑	SSM	UMEM (Available Memory)	Minor	under10(	<=	1000		

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

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

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	under10(	<=	1000		
☑	SSM	UMEM (Available Memory)	Minor	Under 5(	=	5000		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions

Apply Changes

Notificações

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

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

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

de alarme mostre o valor de gatilho como 2,0.

Novos serviços

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

Alarmes e tabelas

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

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

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

Volumes

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

Reconhecer alarmes atuais (sistema legado)

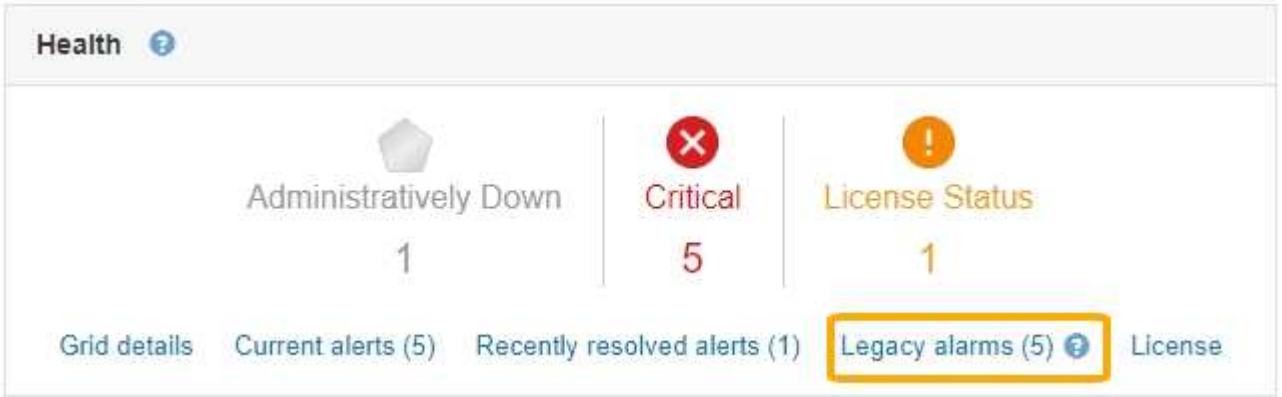
Os alarmes herdados são acionados quando os atributos do sistema atingem os valores de limite de alarme. Se você quiser reduzir ou limpar a contagem de alarmes legados no Dashboard, você pode reconhecer os alarmes.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão reconhecer Alarmes.

Sobre esta tarefa

Se um alarme do sistema legado estiver ativo no momento, o painel Saúde no Painel inclui um link **Alarmes Legacy**. O número entre parênteses indica quantos alarmes legados estão ativos atualmente.



Como o sistema de alarme antigo continua a ser suportado, o número de alarmes herdados mostrados no Dashboard é incrementado sempre que um novo alarme ocorre. Essa contagem é incrementada mesmo que as notificações de e-mail não estejam mais sendo enviadas para alarmes. Normalmente, você pode ignorar esse número (uma vez que os alertas fornecem uma melhor visualização do sistema), ou você pode reconhecer os alarmes.

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

Quando você reconhece um alarme, ele não é mais incluído na contagem de alarmes herdados, a menos que o alarme seja acionado no próximo nível de gravidade ou seja resolvido e ocorra novamente.

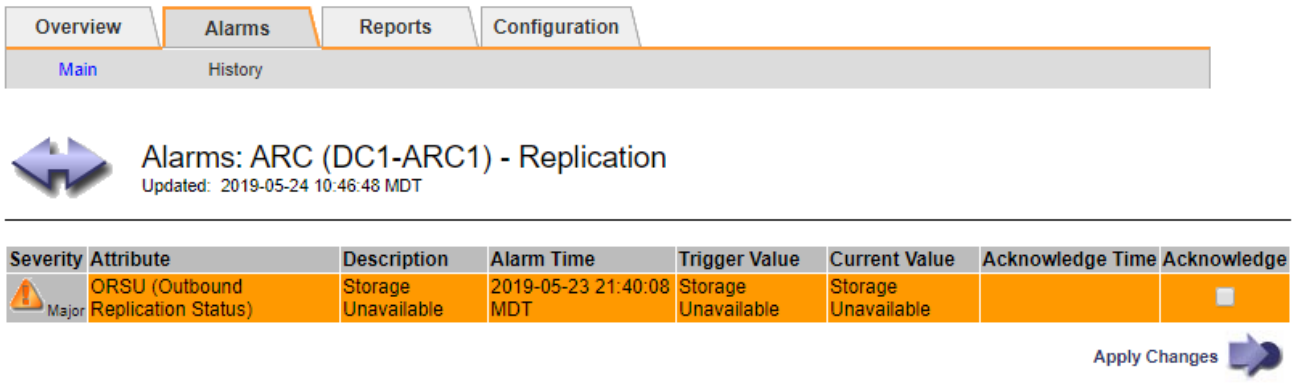
> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Passos

1. Para ver o alarme, proceda de uma das seguintes formas:
   - No painel Saúde no Painel, clique em **Legacy Alarms**. Este link aparece somente se pelo menos um alarme estiver ativo no momento.
   - Selecione **suporte Alarmes (legado) Alarmes atuais**. A página Alarmes atuais é exibida.

2. Clique no nome do serviço na tabela.

   A guia Alarmes para o serviço selecionado é exibida (**suporte Ferramentas topologia de Grade *Grid Node Service* Alarmes**).



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

   O alarme não aparece mais no Painel de instrumentos ou na página Alarmes atuais.

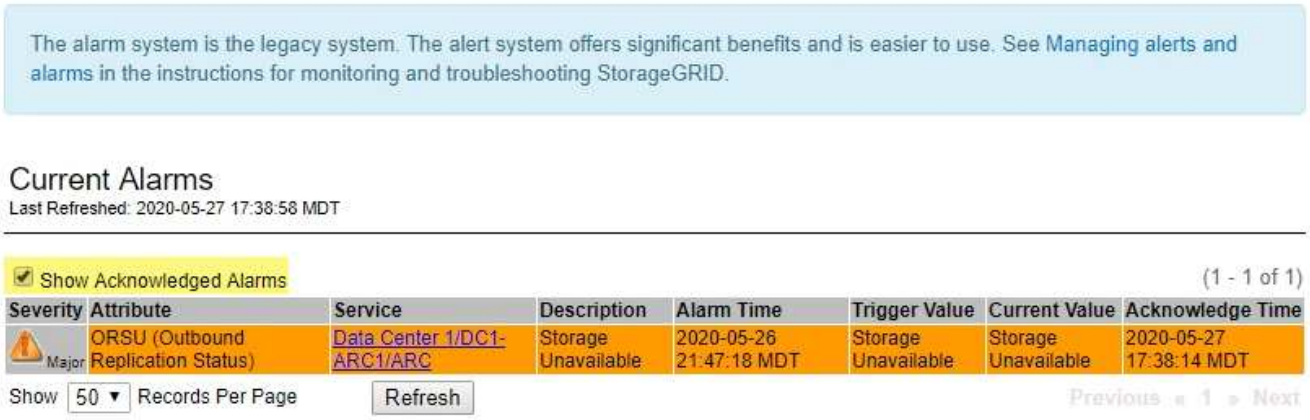
   > Quando você reconhece um alarme, a confirmação não é copiada para outros nós de administração. Por esse motivo, se você exibir o Dashboard de outro nó Admin, poderá continuar a ver o alarme ativo.

4. Conforme necessário, visualize os alarmes reconhecidos.

   a. Selecione **suporte Alarmes (legado) Alarmes atuais**.

   b. Selecione **Mostrar alarmes confirmados**.

      São apresentados quaisquer alarmes reconhecidos.



Informações relacionadas

"Referência de alarmes (sistema legado)"

Visualizar alarmes predefinidos (sistema legado)

Pode ver a lista de todos os alarmes herdados predefinidos.

O que você vai precisar

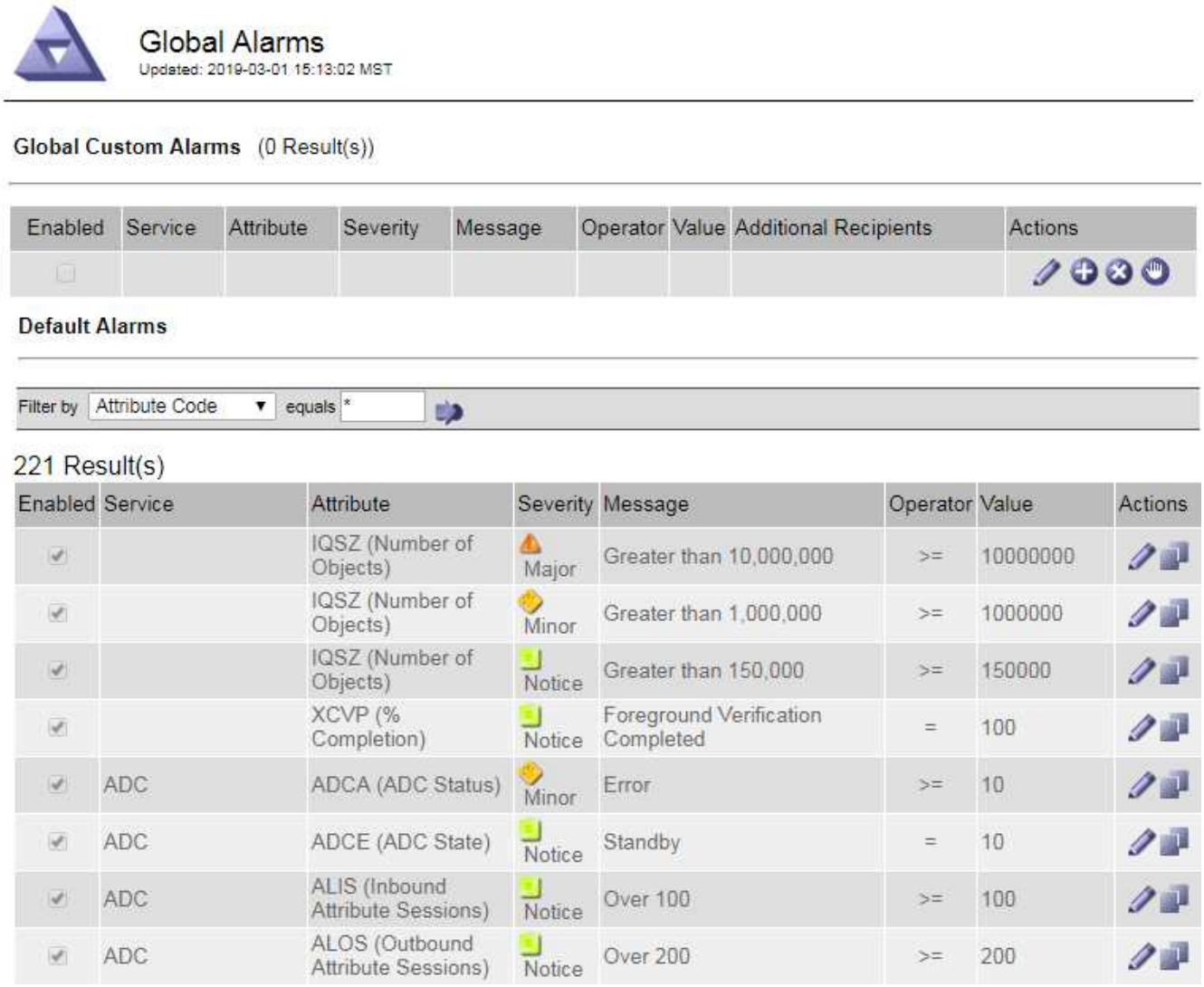
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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

Passos

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

   Todos os alarmes predefinidos estão listados.



Revisão de alarmes históricos e frequência de alarmes (sistema legado)

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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

Passos

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

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

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

Informações relacionadas

"Referência de alarmes (sistema legado)"

Criação de alarmes personalizados globais (sistema legado)

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

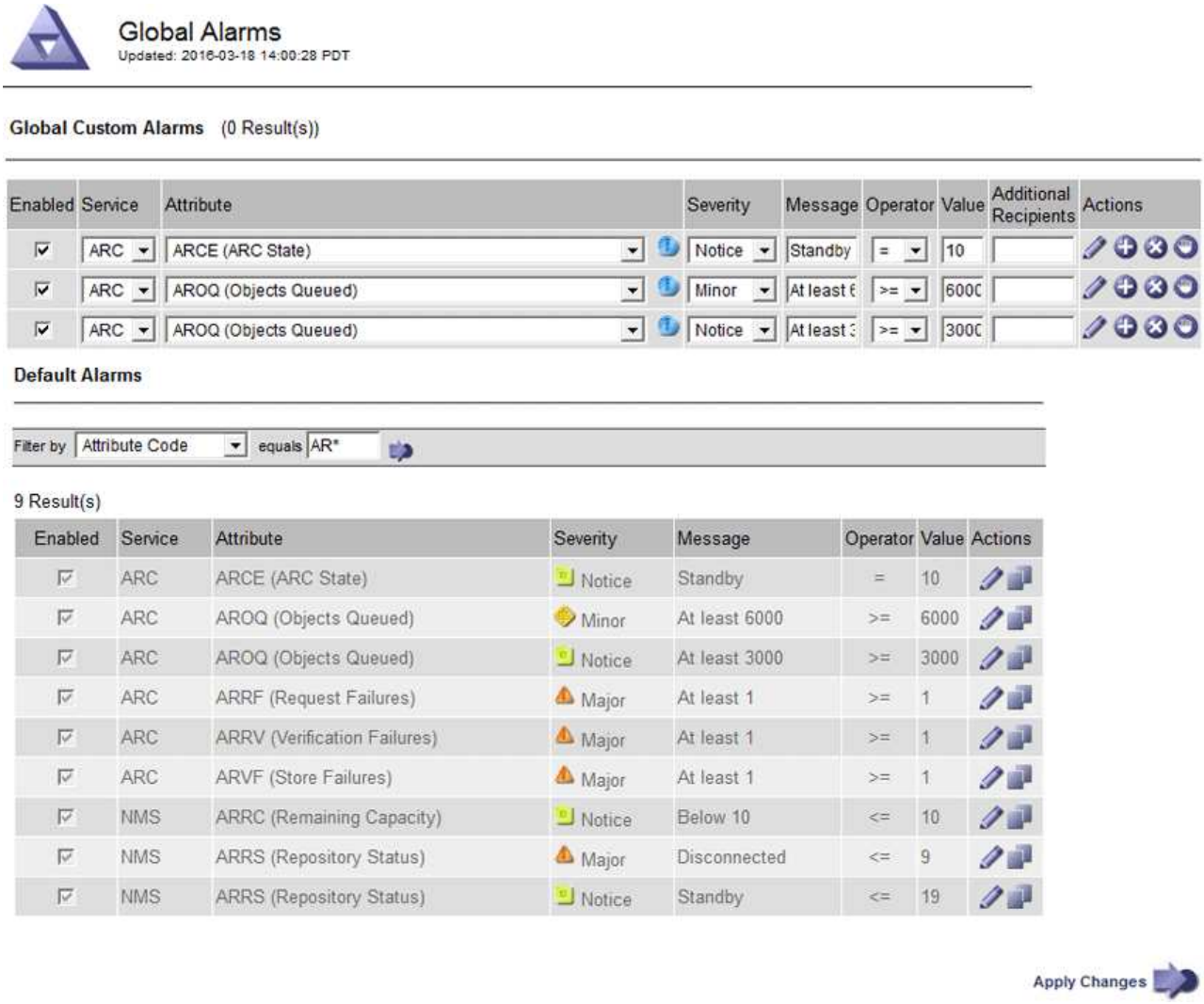
> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

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

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

Passos

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



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

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

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

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

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

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

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

4. Clique em **aplicar alterações**.

Informações relacionadas

"Configuração das configurações do servidor de e-mail para alarmes (sistema legado)"

Desativar alarmes (sistema legado)

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

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

Desativar um alarme predefinido (sistema legado)

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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

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

Passos

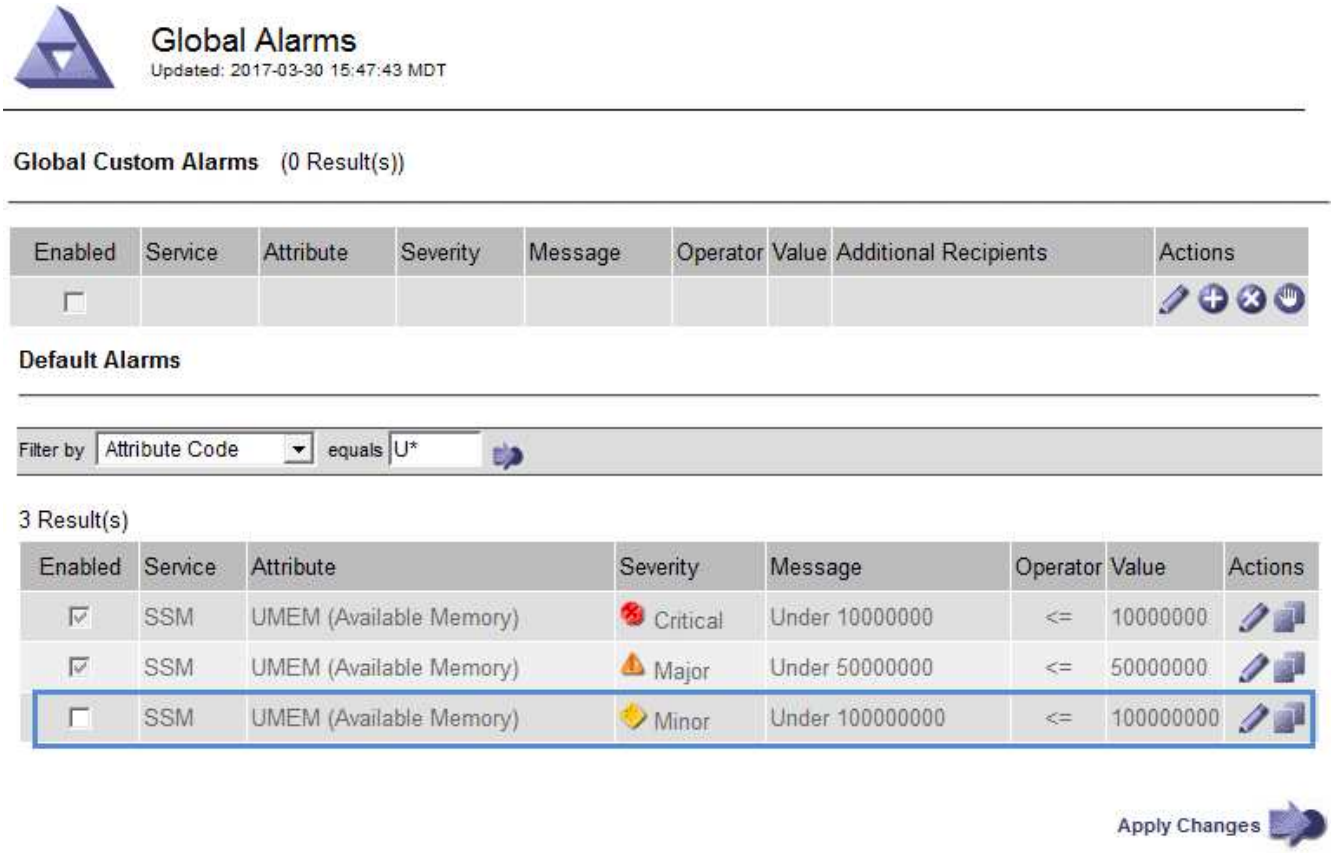
1. Selecione **suporte Alarmes (legado) Alarmes globais**.
2. Procure o alarme predefinido para desativar.
   a. Na seção Alarmes padrão, selecione **Filtrar por Código de Atributo** ou **Nome do Atributo**.
   b. Digite uma string de pesquisa.

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

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

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

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



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

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

   O alarme predefinido está desativado.

Desativar alarmes personalizados globais (sistema legado)

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

O que você vai precisar

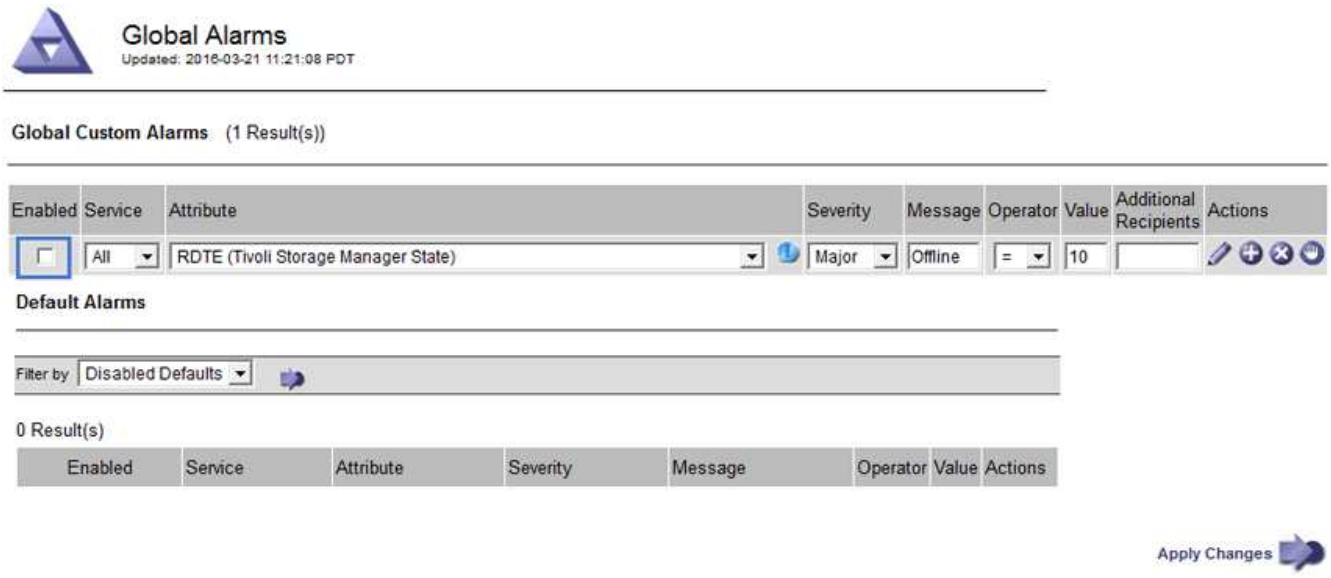
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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

Passos

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



4. Clique em **aplicar alterações**.

   O alarme personalizado global está desativado.

Apagar alarmes acionados (sistema legado)

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

O que você vai precisar

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

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

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

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

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

   O alarme é apagado.

Informações relacionadas

"Desativar alarmes (sistema legado)"

Configurar notificações para alarmes (sistema legado)

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

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

Informações relacionadas

"Utilizar a monitorização SNMP"

Tipos de notificações de alarme (sistema legado)

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

Notificações de nível de gravidade

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

- Aviso
- Menor
- Maior
- Crítico

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

Notificações do estado do serviço

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

- Desconhecido
- Administrativamente para baixo

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

Informações relacionadas

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

Configuração das configurações do servidor de e-mail para alarmes (sistema legado)

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

não pode receber e-mail.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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

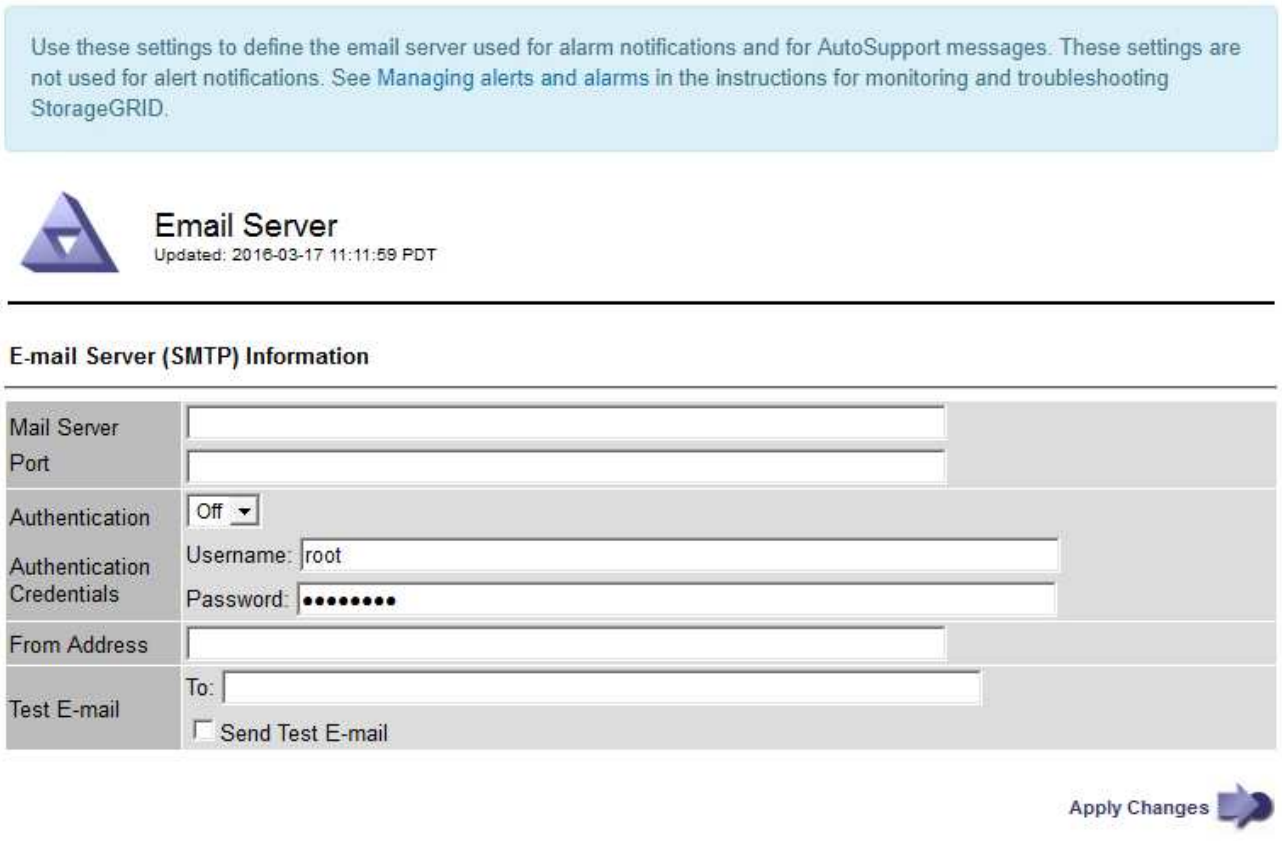
> Se você usar SMTP como protocolo para mensagens AutoSupport, talvez você já tenha configurado um servidor de email SMTP. O mesmo servidor SMTP é usado para notificações de e-mail de alarme, para que você possa ignorar este procedimento. Consulte as instruções para administrar o StorageGRID.

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

Passos

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

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



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

Item	Descrição
Servidor de correio	Endereço IP do servidor de correio SMTP. Você pode inserir um nome de host em vez de um endereço IP se tiver configurado as configurações de DNS anteriormente no nó Admin.
Porta	Número da porta para aceder ao servidor de correio SMTP.
Autenticação	Permite a autenticação do servidor de correio SMTP. Por padrão, a autenticação está desativada.
Credenciais de autenticação	Nome de utilizador e palavra-passe do servidor de correio SMTP. Se a Autenticação estiver definida como ativada, um nome de usuário e senha para acessar o servidor de e-mail SMTP devem ser fornecidos.

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

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

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

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

Informações relacionadas

"Administrar o StorageGRID"

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

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

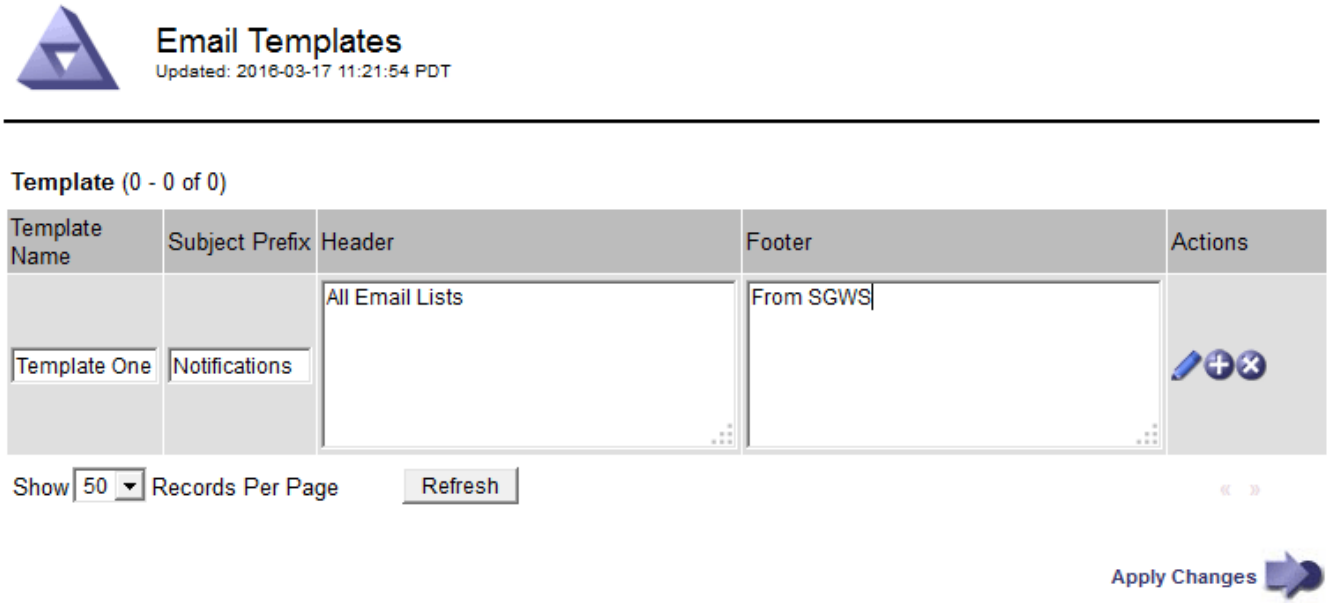
Sobre esta tarefa

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

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

Passos

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



4. Na nova linha, adicione o seguinte:

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

Item	Descrição
Rodapé	Opcional. Texto de rodapé que aparece no final do corpo da mensagem de e-mail. O texto do rodapé pode ser usado para fechar a mensagem de e-mail com informações de lembrete, como um número de telefone de Contato ou um link para um site da Web.

5. Clique em **aplicar alterações**.

   Um novo modelo para notificações é adicionado.

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

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

O que você vai precisar

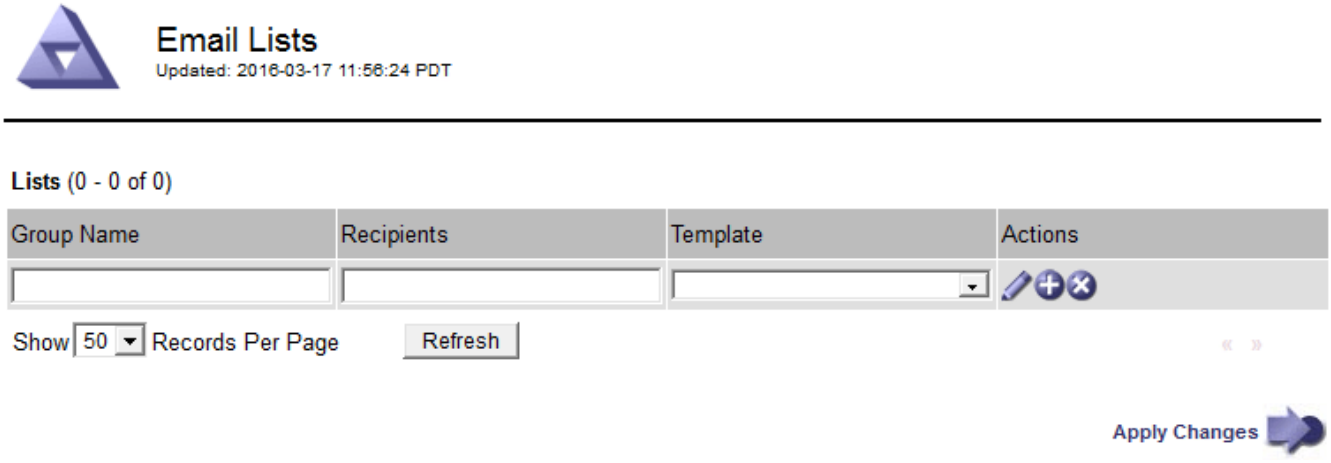
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Se você quiser especificar um modelo de e-mail para a lista de e-mail (cabeçalho personalizado, rodapé e linha de assunto), você já deve ter criado o modelo.

Sobre esta tarefa

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

Passos

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



4. Na nova linha, adicione o seguinte:

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

5. Clique em **aplicar alterações**.

   Uma nova lista de discussão é criada.

Informações relacionadas

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

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

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter configurado uma lista de e-mail.

Sobre esta tarefa

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

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

Passos

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

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

Informações relacionadas

"Criando listas de discussão para notificações de alarme (sistema legado)"

"Tipos de notificações de alarme (sistema legado)"

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

Você pode suprimir notificações de alarme para uma lista de discussão quando não quiser mais que a lista de discussão receba notificações sobre alarmes. Por exemplo, você pode querer suprimir notificações sobre alarmes legados depois de fazer a transição para o uso de notificações por e-mail de alerta.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

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

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

Passos

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

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

Suprimindo o sistema de notificações por e-mail

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

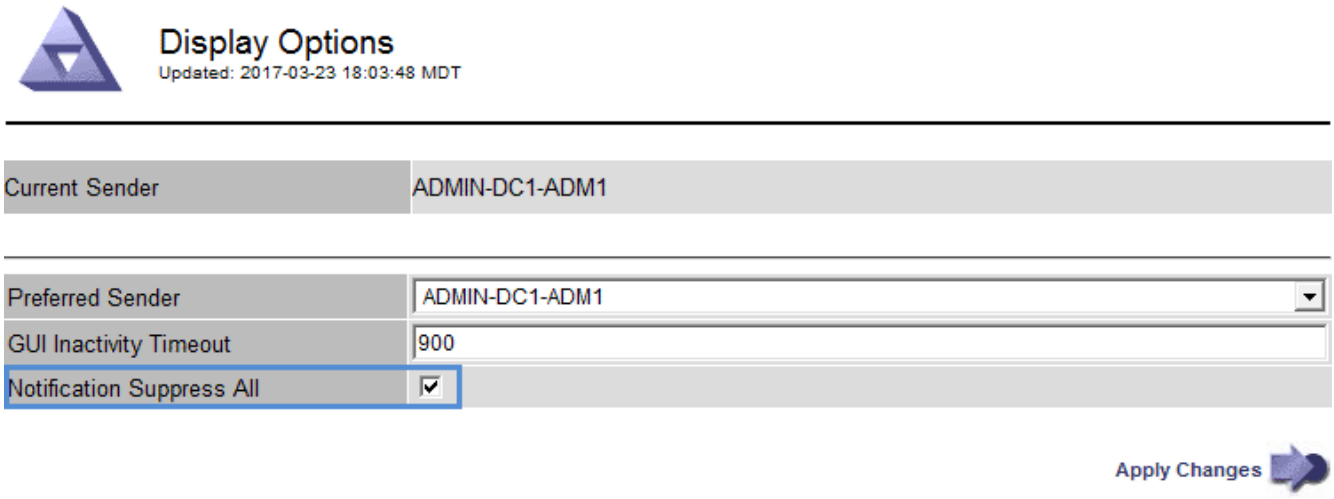
Sobre esta tarefa

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

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

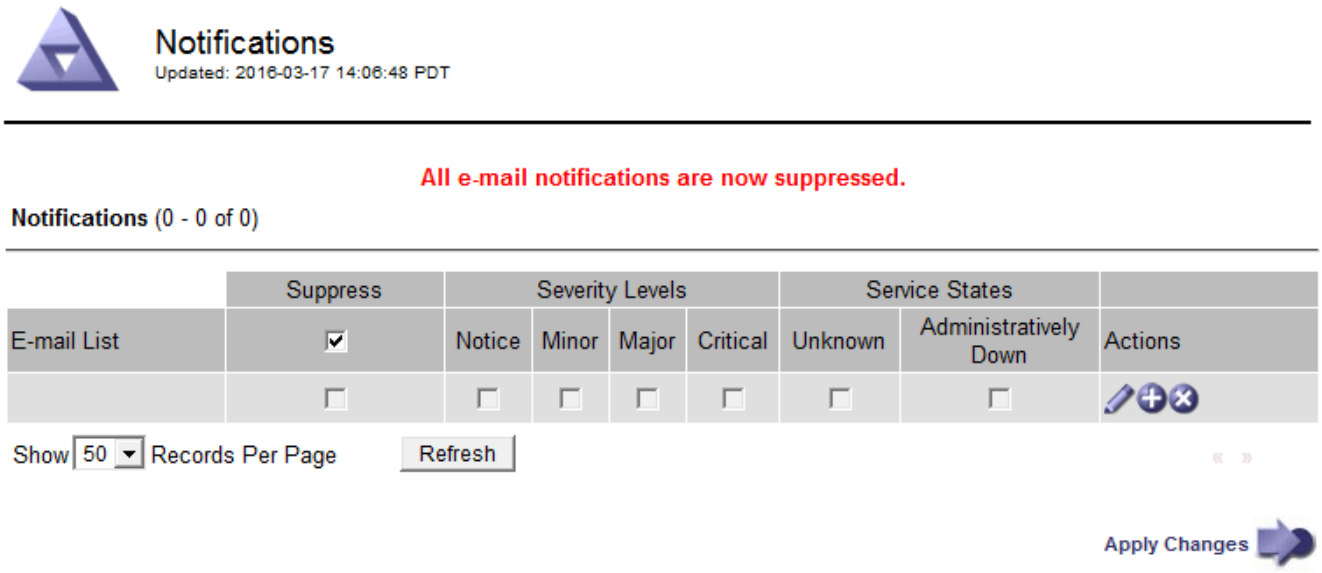
Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**.
2. No menu Opções de exibição, selecione **Opções**.
3. Selecione **notificação suprimir tudo**.



4. Clique em **aplicar alterações**.

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



Informações relacionadas

"Administrar o StorageGRID"

Utilizar 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.

- "Configurando o agente SNMP"
- "Atualizando o agente SNMP"

Recursos

Cada nó do StorageGRID executa um agente SNMP, ou daemon, que fornece uma base de informações de gerenciamento (MIB). O MIB do StorageGRID contém definições de tabela e notificação para alertas e alarmes. O MIB também contém informações de descrição do sistema, como plataforma e número do modelo para cada nó. Cada nó StorageGRID também suporta um subconjunto de objetos MIB-II.

Inicialmente, o SNMP está desativado em todos os nós. Quando você configura o agente SNMP, todos os nós do StorageGRID recebem a mesma configuração.

O agente SNMP do StorageGRID suporta todas as três versões do protocolo SNMP. Ele fornece acesso MIB somente leitura para consultas e pode enviar dois tipos de notificações orientadas a eventos para um sistema de gerenciamento:

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

  Traps são suportados em todas as três versões do SNMP.

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

  As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de 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 configurar um silêncio para o alerta. As notificações de alerta são enviadas por qualquer nó Admin configurado para ser o remetente preferido.
- Certos alarmes (sistema legado) são acionados em níveis de gravidade especificados ou superiores.

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

Suporte à versão SNMP

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

	SNMPv1	SNMPv2c	SNMPv3
Consultas	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	Cadeia de carateres da comunidade	Cadeia de carateres da comunidade	Utilizador do modelo de segurança baseado no utilizador (USM)
Notificações	Apenas armadilhas	Armadilhas e informações	Armadilhas e informações
Autenticação de notificação	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Utilizador USM para cada destino de armadilha

Limitações

- O StorageGRID suporta acesso MIB somente leitura. O acesso de leitura e gravação não é suportado.
- Todos os nós na grade recebem a mesma configuração.
- SNMPv3: O StorageGRID não suporta o modo de suporte de transporte (TSM).
- SNMPv3: O único protocolo de autenticação suportado é SHA (HMAC-SHA-96).
- SNMPv3: O único protocolo de privacidade suportado é AES.

Acessando o MIB

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

/Usr/share/snmp/mibs/NetApp-StorageGRID-MIB.txt

Informações relacionadas

"Referência de alertas"

"Referência de alarmes (sistema legado)"

"Alarmes que geram notificações SNMP (sistema legado)"

"Silenciar notificações de alerta"

Configurando o agente SNMP

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

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

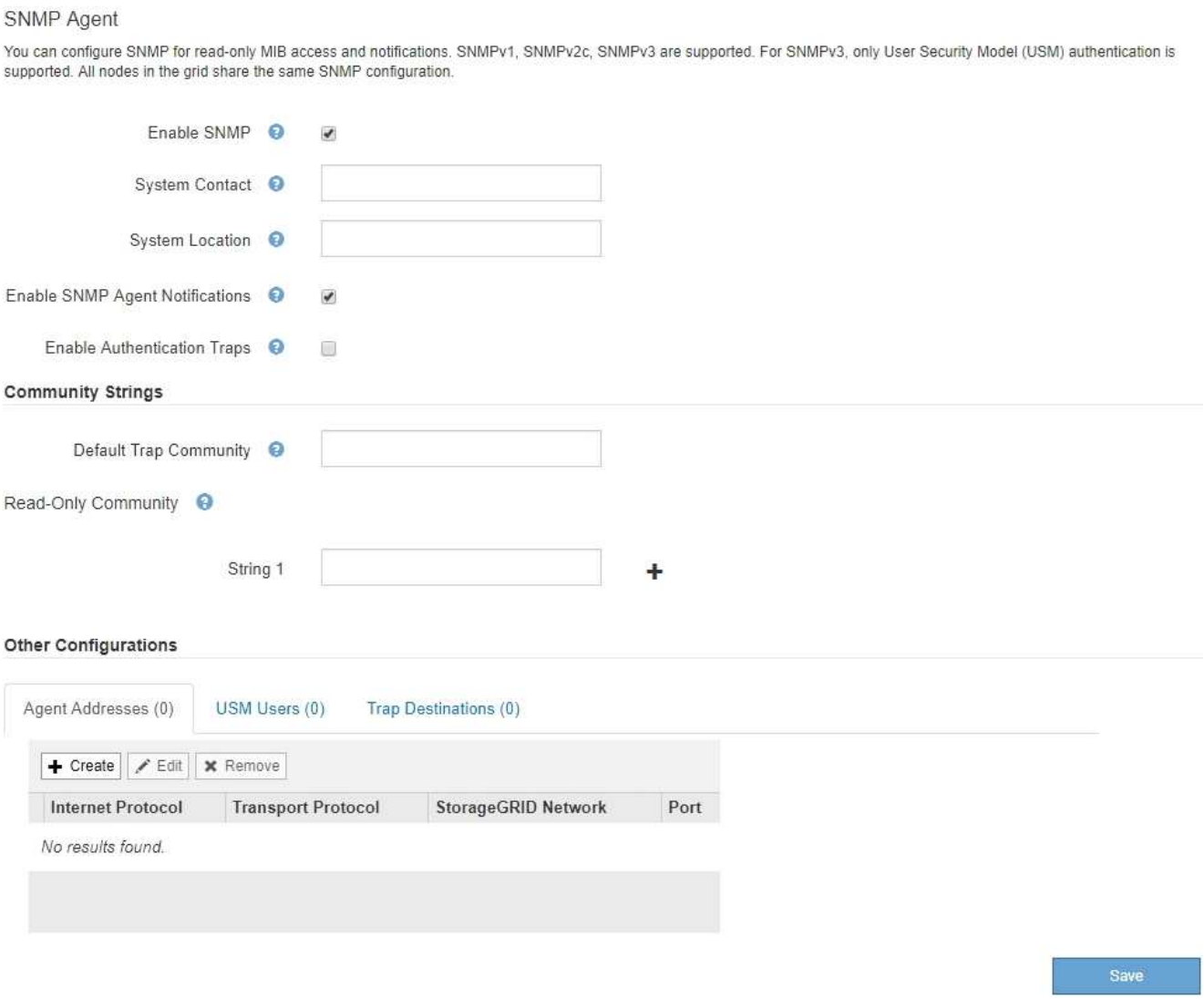
Passos

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

   A página Agente SNMP é exibida.

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

   Os campos para configurar um agente SNMP são exibidos.



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

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

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

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

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

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

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

protocolo autenticada incorretamente.

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

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

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

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

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

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

      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.

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

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

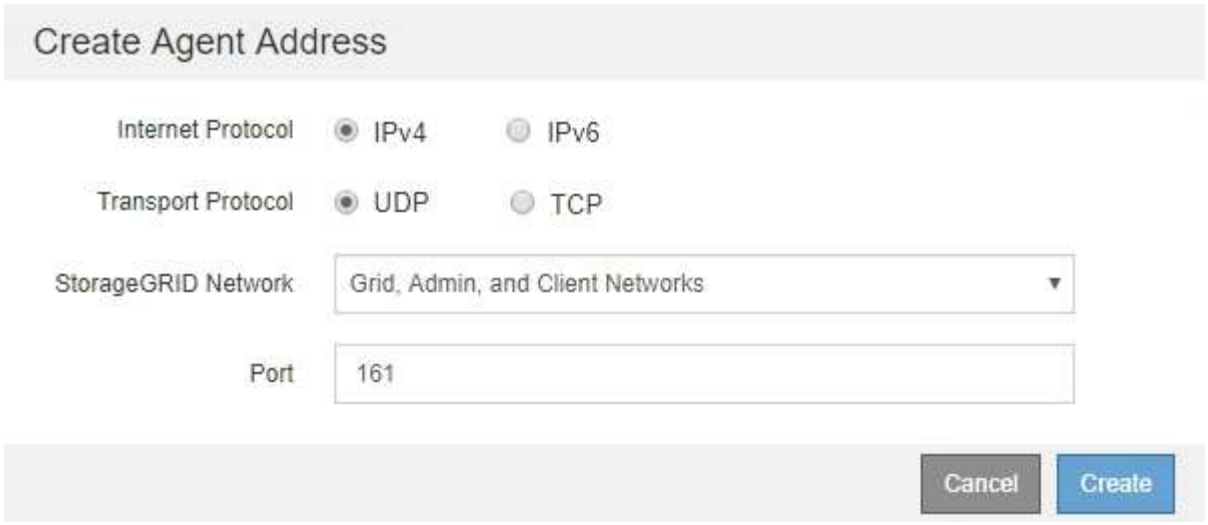
8. Opcionalmente, selecione a guia endereços de agentes na seção outras configurações .

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

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

   a. Clique em **criar**.

      A caixa de diálogo criar endereço do agente é exibida.



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

   Por padrão, o SNMP usa IPv4.

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

   Por padrão, o SNMP usa UDP.

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

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

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

e. No campo **Port**, insira opcionalmente o número da porta que o agente SNMP deve ouvir.

   A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado.

   > Quando você salva o agente SNMP, o StorageGRID abre automaticamente as portas de endereço do agente no firewall interno. Você deve garantir que todos os firewalls externos permitam acesso a essas portas.

f. Clique em **criar**.

   O endereço do agente é criado e adicionado à tabela.

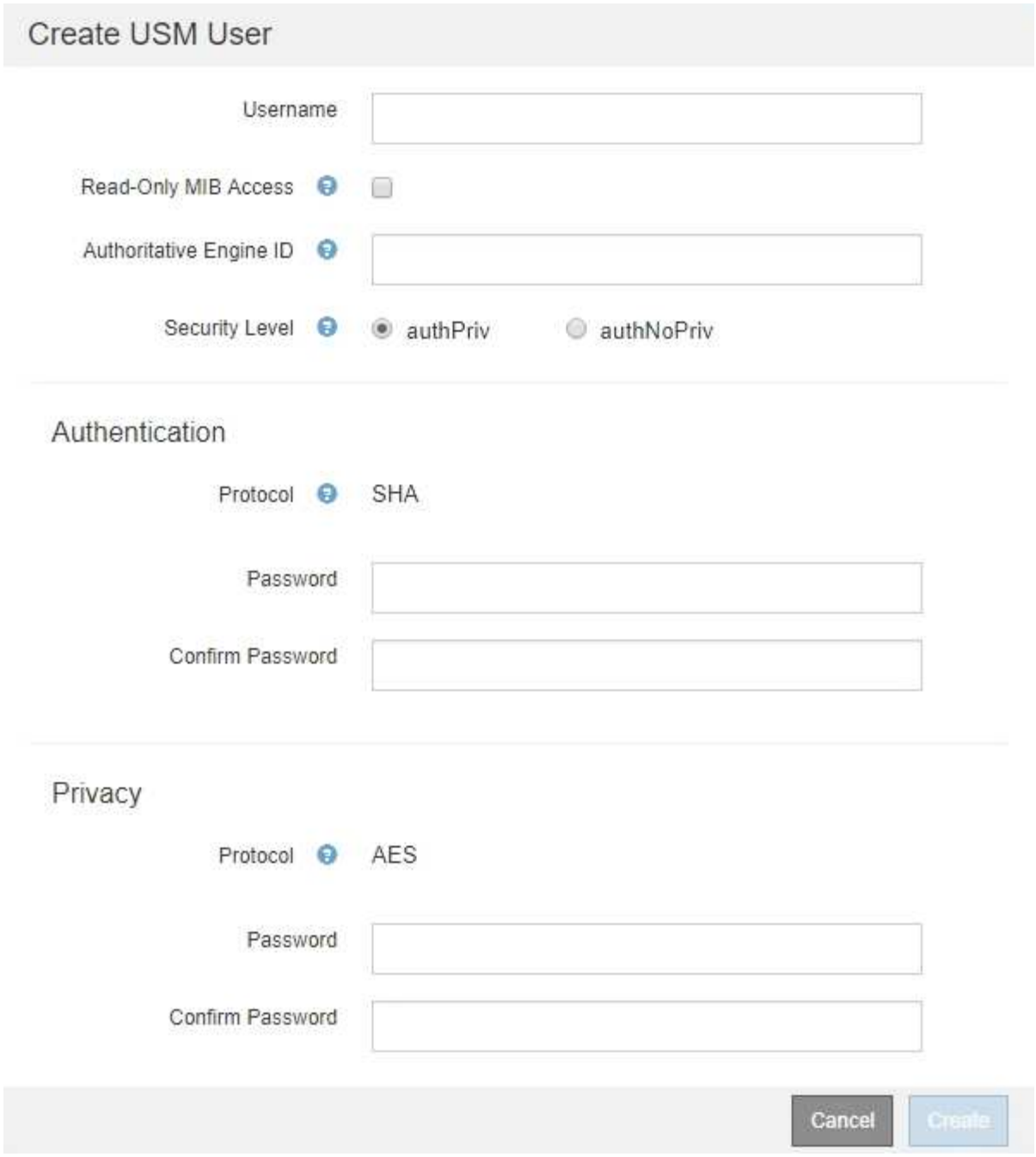
9. Se estiver a utilizar o SNMPv3, selecione o separador utilizadores USM na secção outras configurações.

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

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

   a. Clique em **criar**.

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



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

   Os nomes de usuário têm 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.

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

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

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

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

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

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

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

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

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

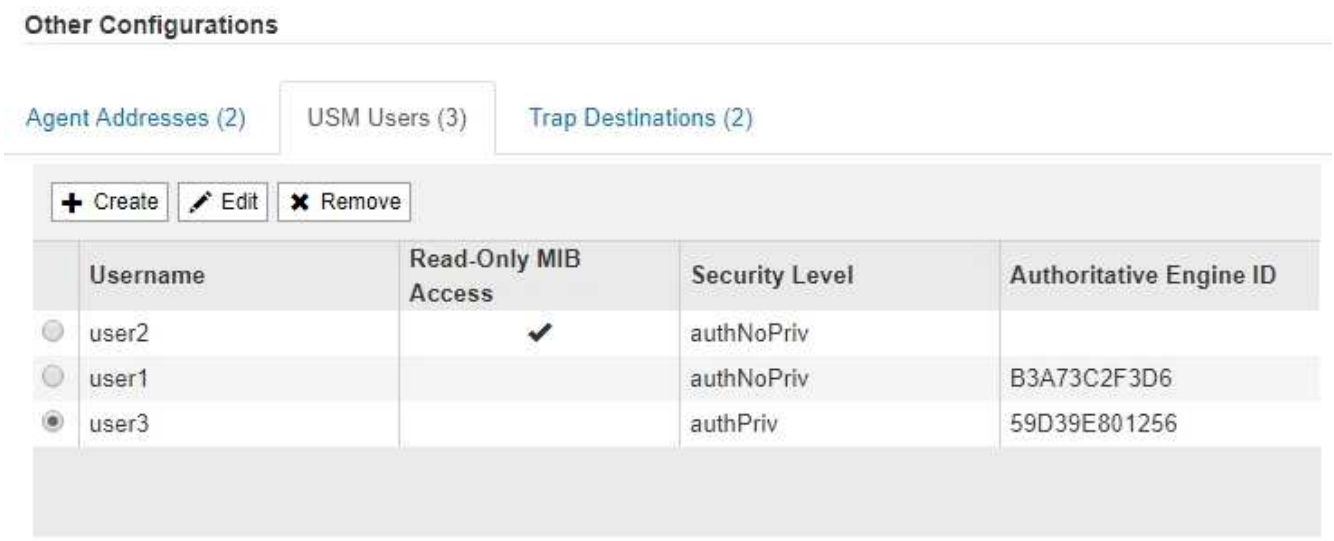
> O único protocolo de autenticação suportado é SHA (HMAC-SHA-96).

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

> O único protocolo de privacidade suportado é AES.

h. Clique em **criar**.

O utilizador USM é criado e adicionado à tabela.

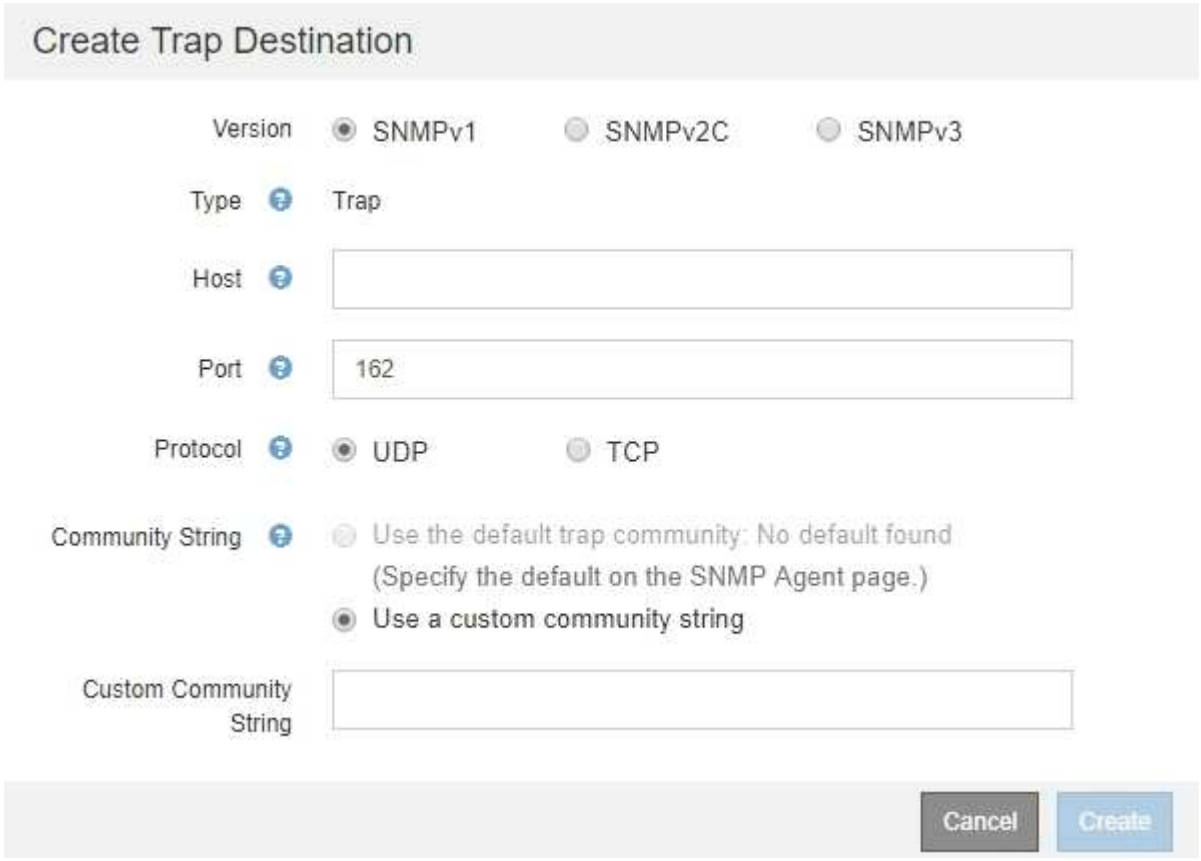


10. na seção outras configurações, selecione a guia Destinos de armadilha.

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

a. Clique em **criar**.

A caixa de diálogo criar destino de armadilha é exibida.



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

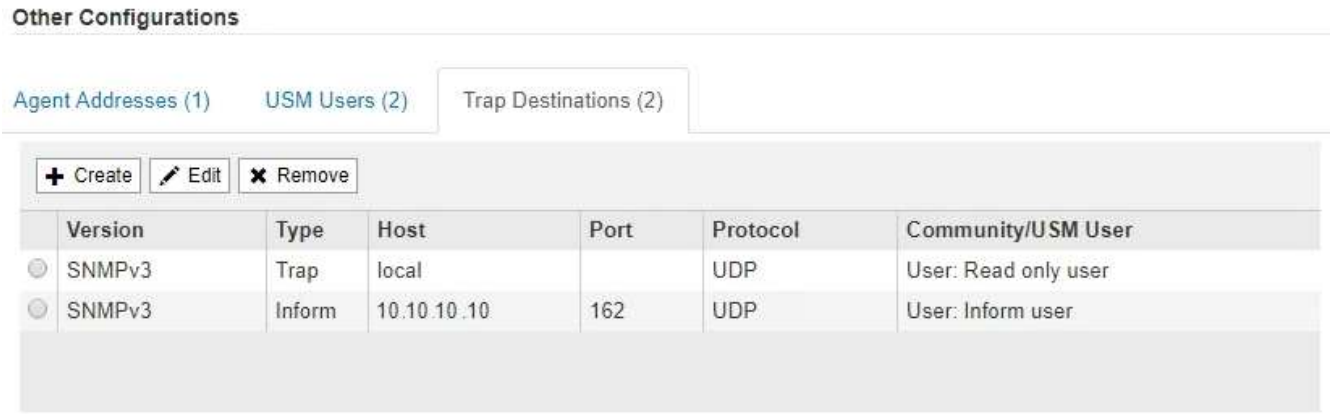
c. Preencha o formulário, com base na versão selecionada

Versão	Especifique esta informação
SNMPv1	**Nota:** para SNMPv1, o agente SNMP só pode enviar traps. As informações não são suportadas. i. No campo **Host**, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. ii. Para **Port**, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iii. Para **Protocolo**, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) iv. Use a comunidade de trap padrão, se uma foi especificada na página Agente SNMP, ou insira uma string de comunidade personalizada para esse destino de trap. A string de comunidade personalizada pode ter no máximo 32 carateres e não pode conter espaço em branco.
SNMPv2c	i. Selecione se o destino será usado para armadilhas ou informações. ii. No campo **Host**, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. iii. Para **Port**, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iv. Para **Protocolo**, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) v. Use a comunidade de trap padrão, se uma foi especificada na página Agente SNMP, ou insira uma string de comunidade personalizada para esse destino de trap. A string de comunidade personalizada pode ter no máximo 32 carateres e não pode conter espaço em branco.

Versão	Especifique esta informação
SNMPv3	i. Selecione se o destino será usado para armadilhas ou informações. ii. No campo **Host**, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. iii. Para **Port**, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iv. Para **Protocolo**, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) v. Selecione o utilizador USM que será utilizado para autenticação. ◦ Se selecionou **Trap**, apenas são apresentados utilizadores USM sem IDs de motor autoritativas. ◦ Se selecionou **inform**, apenas são apresentados utilizadores USM com IDs de motor autoritativas.

d. Clique em **criar**.

O destino da armadilha é criado e adicionado à tabela.



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

A nova configuração do agente SNMP fica ativa.

Informações relacionadas

"Silenciar notificações de alerta"

Atualizando o agente SNMP

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

Sempre que você atualizar a configuração do agente SNMP, esteja ciente de que você deve clicar em **Salvar** na parte inferior da página Agente SNMP para confirmar quaisquer alterações feitas em cada guia.

Passos

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

   A página Agente SNMP é exibida.

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

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

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

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

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

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

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

7. Se quiser 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". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas. Cada endereço de agente inclui um protocolo de Internet, um protocolo de transporte, uma rede StorageGRID e uma porta.

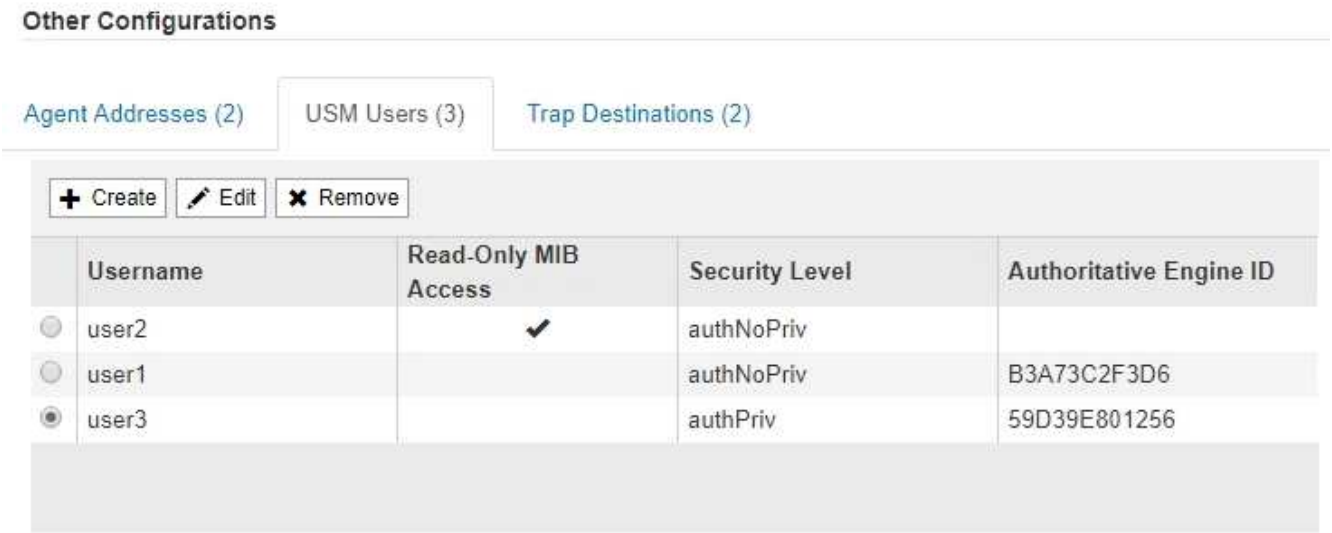
a. Para adicionar um endereço de agente, clique em **criar**. Em seguida, consulte a etapa para obter endereços de agentes nas instruções para configurar o agente SNMP.

b. Para editar um endereço de agente, selecione o botão de opção para o endereço e clique em **Editar**. Em seguida, consulte a etapa para obter endereços de agentes nas instruções para configurar o agente SNMP.

c. Para remover um endereço de agente, selecione o botão de opção para o endereço e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover esse endereço.

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

8. Se pretender atualizar utilizadores USM, selecione o separador utilizadores USM na secção outras configurações.



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

a. Para adicionar um utilizador USM, clique em **criar**. Em seguida, consulte a etapa para usuários USM nas instruções para configurar o agente SNMP.

b. Para editar um utilizador USM, selecione o botão de opção do utilizador e clique em **Edit**. Em seguida,

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

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

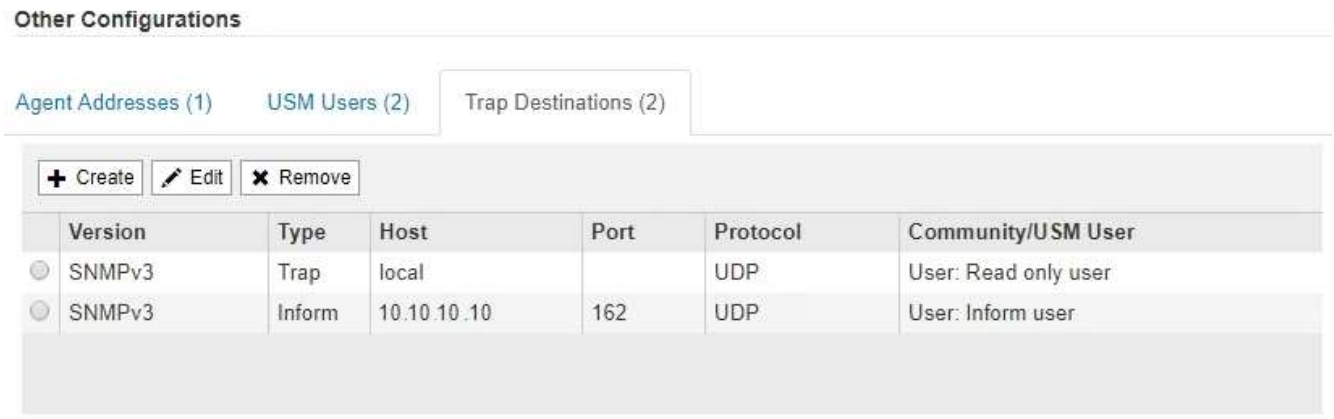
> Se você adicionar ou remover um ID de mecanismo autoritário de um usuário e esse usuário estiver selecionado atualmente para um destino, edite ou remova o destino, conforme descrito na etapa Destino de trap SNMP. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

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

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

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

1. Se quiser atualizar destinos de intercetação, selecione a guia Destinos de intercetação na seção outras configurações.



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

a. Para adicionar um destino de armadilha, clique em **criar**. Em seguida, consulte a etapa para destinos de intercetação nas instruções para configurar o agente SNMP.

b. Para editar um destino de armadilha, selecione o botão de opção do usuário e clique em **Editar**. Em seguida, consulte a etapa para destinos de intercetação nas instruções para configurar o agente SNMP.

c. Para remover um destino de armadilha, selecione o botão de opção para o destino e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover este destino.

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

2. Quando tiver atualizado a configuração do agente SNMP, clique em **Save**.

Informações relacionadas

"Configurando o agente SNMP"

A recolher dados StorageGRID adicionais

Há várias formas adicionais de coletar e analisar dados que podem ser úteis ao investigar o estado do seu sistema StorageGRID ou ao trabalhar com suporte técnico para resolver problemas.

- "Usando gráficos e relatórios"
- "Monitorar O PUT e obter desempenho"
- "Monitoramento de operações de verificação de objetos"
- "Monitoramento de eventos"
- "Rever mensagens de auditoria"
- "Coletando arquivos de log e dados do sistema"
- "Acionando manualmente uma mensagem AutoSupport"
- "Visualizar a árvore de topologia de grelha"
- "Revisão das métricas de suporte"
- "A executar o diagnóstico"
- "Criando aplicativos de monitoramento personalizados"

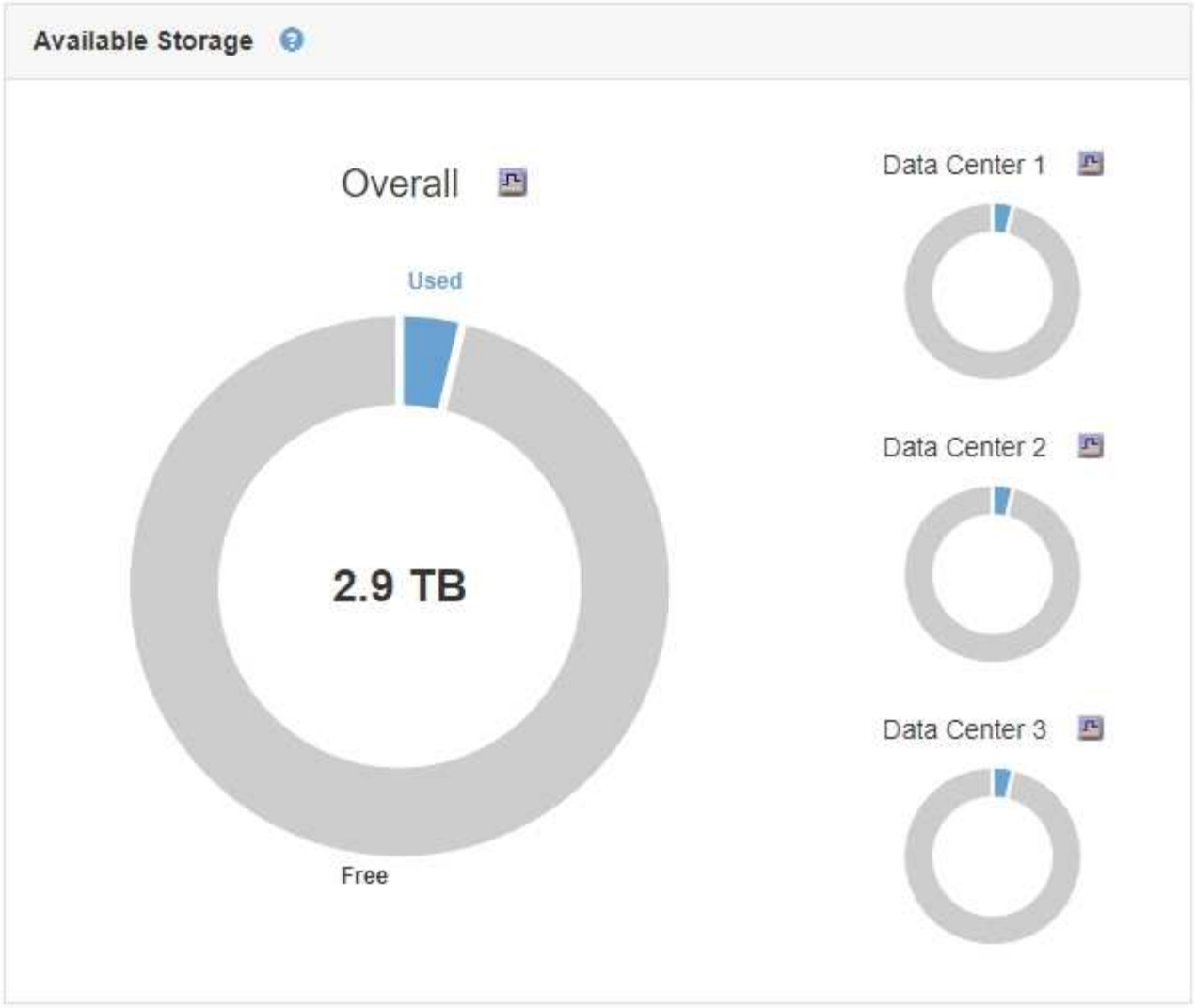
Usando gráficos e relatórios

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

Tipos de gráficos e gráficos

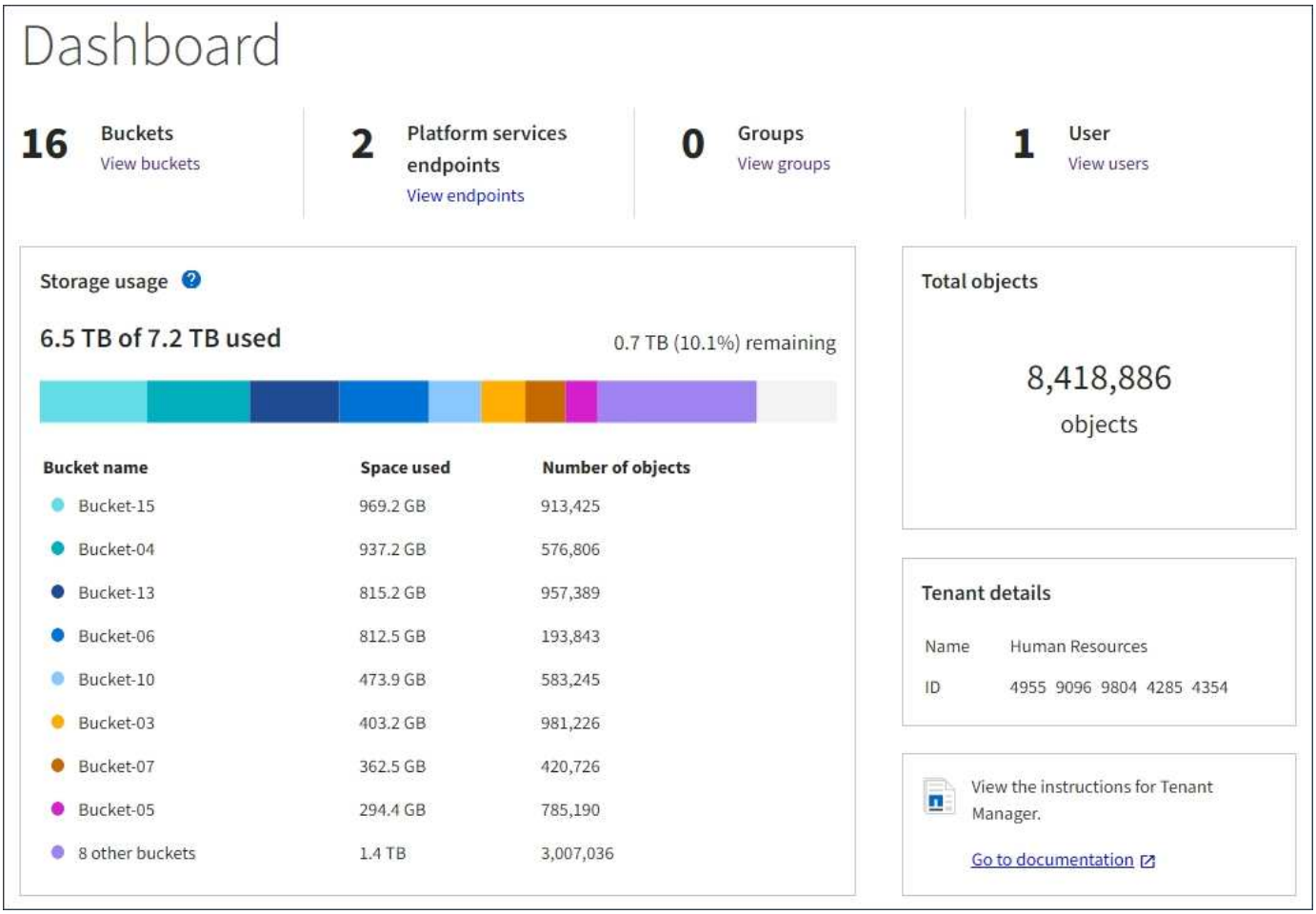
Gráficos e gráficos resumem os valores de métricas e atributos específicos do StorageGRID.

O Painel do Gerenciador de Grade inclui gráficos de pizza (rosca) para resumir o armazenamento disponível para a grade e cada local.



O painel uso do armazenamento no Painel do Gerenciador do locatário exibe o seguinte:

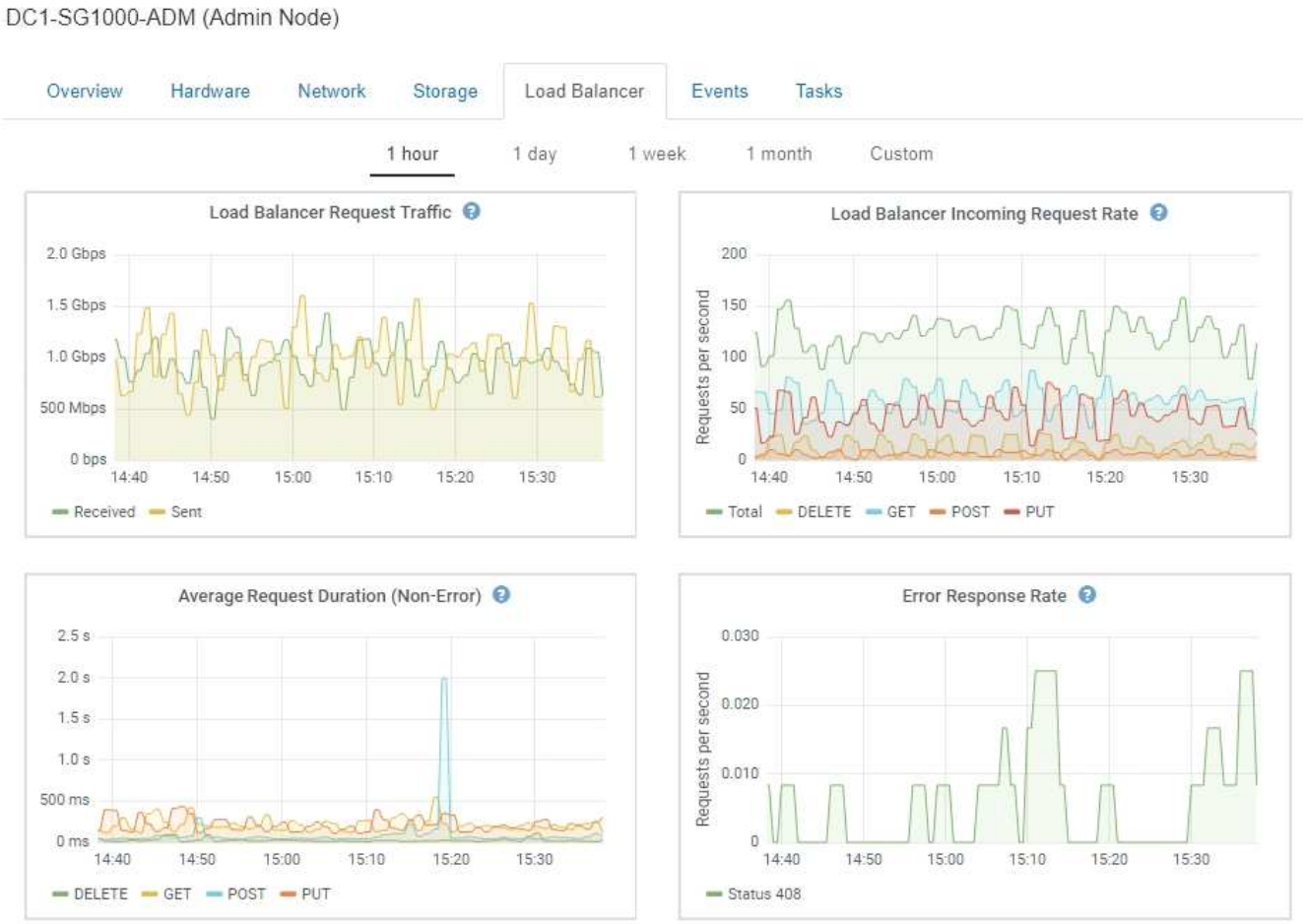
- Uma lista dos maiores baldes (S3) ou contentores (Swift) para o inquilino
- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou contentores
- A quantidade total de espaço utilizado e, se for definida uma quota, a quantidade e a percentagem de espaço restante



Além disso, gráficos que mostram como as métricas e atributos do StorageGRID mudam ao longo do tempo estão disponíveis na página de nós e na página **suporte Ferramentas topologia de grade**.

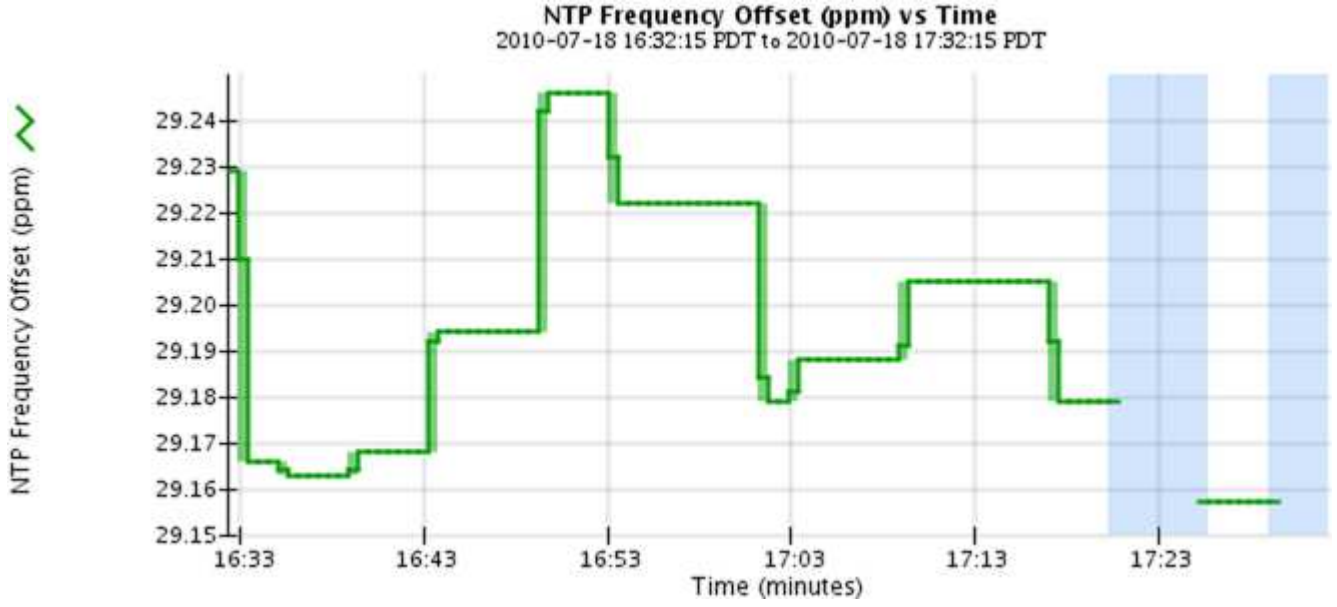
Existem quatro tipos de gráficos:

- **Gráficos Grafana**: Mostrados na página de nós, gráficos Grafana são usados para plotar os valores das métricas Prometheus ao longo do tempo. Por exemplo, a guia **nós Load Balancer** para um nó Admin inclui quatro gráficos Grafana.

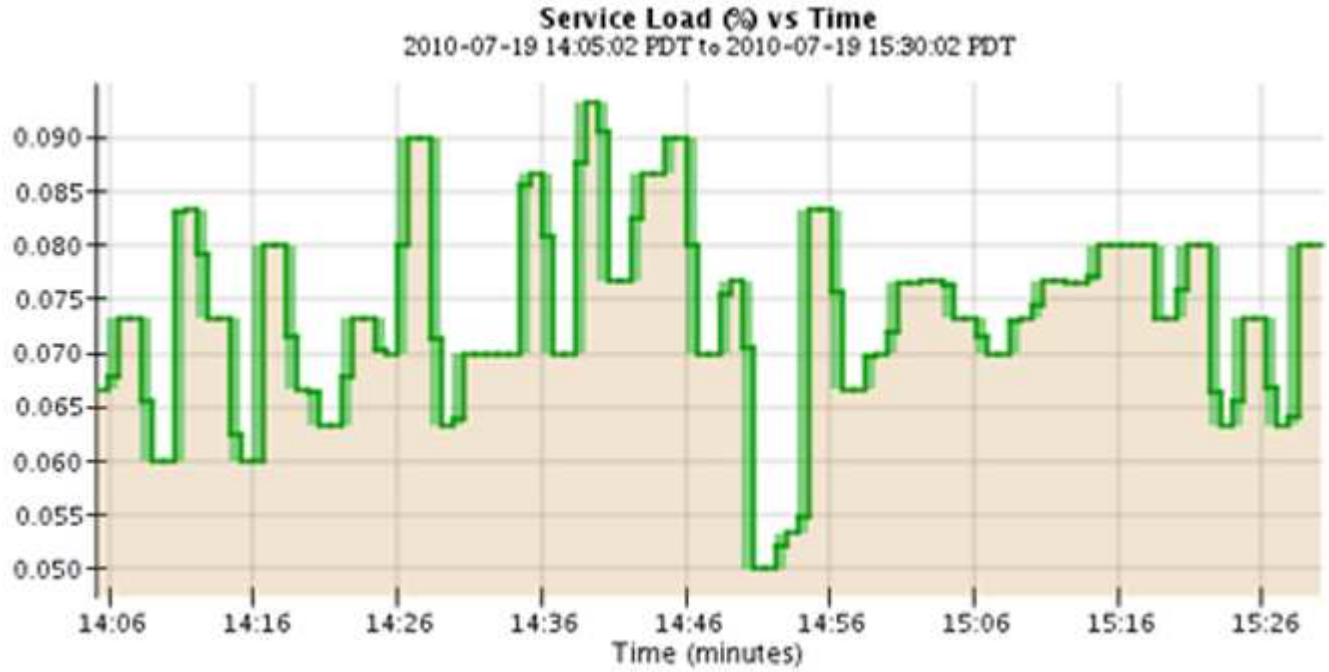


Gráficos Grafana também estão incluídos nos painéis pré-construídos disponíveis na página **suporte Ferramentas métricas**.

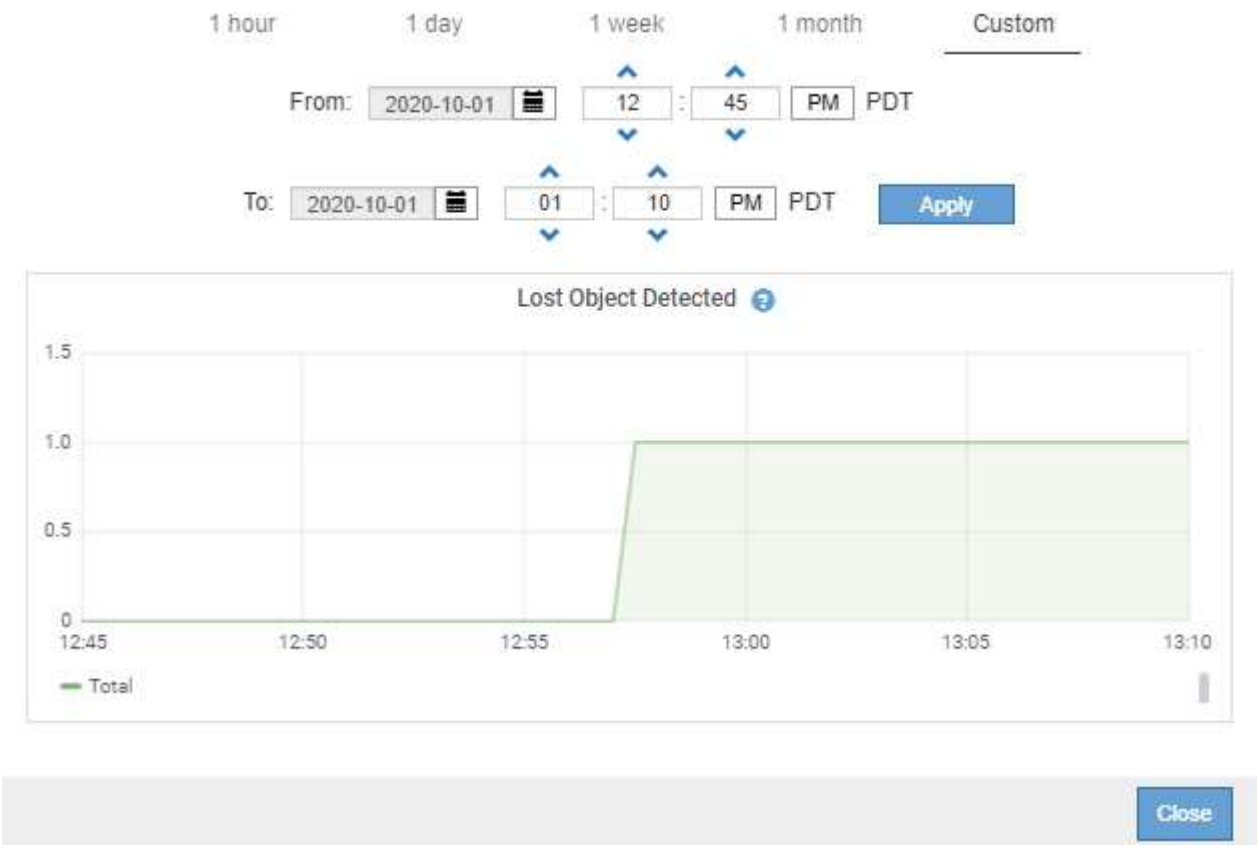
- **Gráficos de linha**: Disponíveis na página de nós e na página **suporte Ferramentas topologia de grade** (clique no ícone do gráfico após um valor de dados), gráficos de linha são usados para plotar os valores de atributos StorageGRID que têm um valor unitário (como desvio de frequência NTP, em ppm). As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



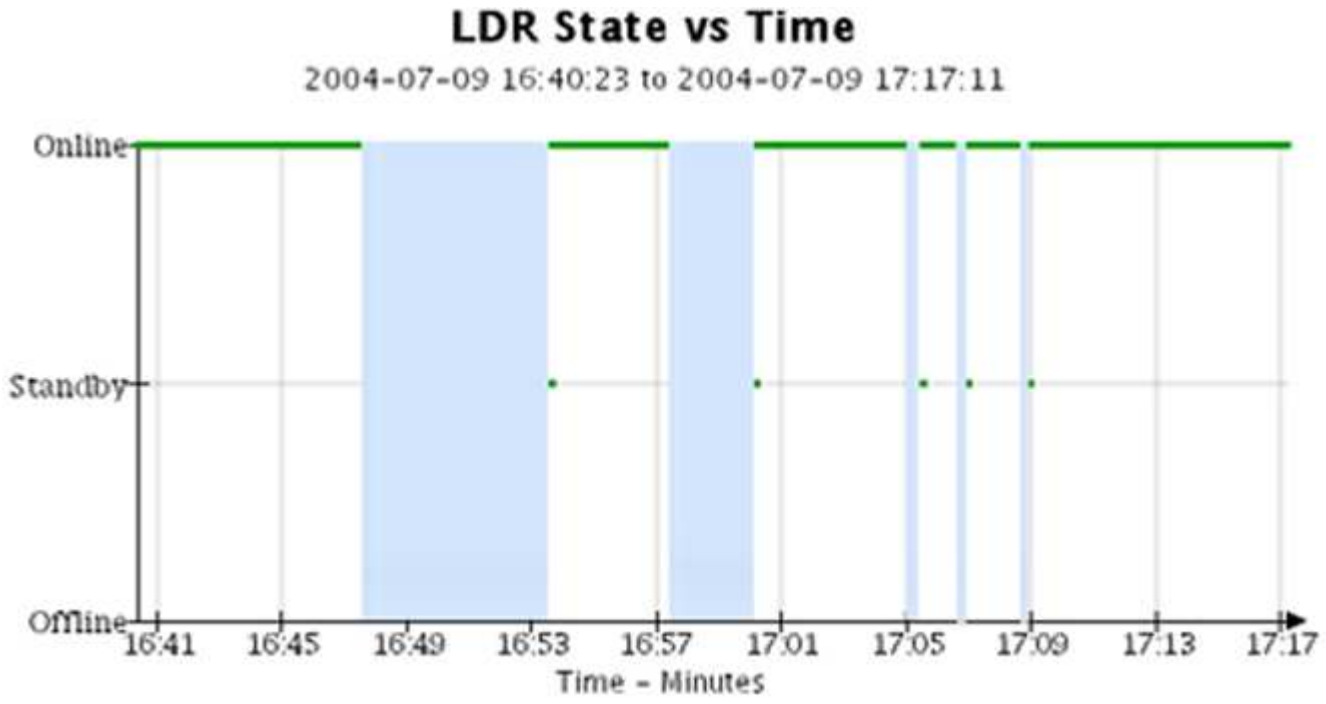
- **Gráficos de área**: Disponíveis na página de nós e na página **suporte Ferramentas topologia de grade** (clique no ícone do gráfico após um valor de dados), os gráficos de área são usados para plotar quantidades de atributos volumétricos, como contagens de objetos ou valores de carga de serviço. 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:



- **Gráfico de estado**: Disponível na página **suporte Ferramentas topologia de grade** (clique no 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, em espera ou off-line. 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

"Exibindo a página de nós"

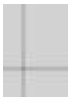
"Visualizar a árvore de topologia de grelha"

"Revisão das métricas de suporte"

Legenda da carta

As linhas e cores usadas para desenhar gráficos têm significado específico.

Amostra	Significado
	Os valores de atributo relatados são plotados usando linhas verdes escuras.
	O sombreamento verde claro em torno de linhas verdes escuras indica que os valores reais nesse intervalo de tempo variam e foram "binned" para plotagem mais rápida. A linha escura representa a média ponderada. O intervalo em verde claro indica os valores máximo e mínimo dentro do compartimento. O sombreamento castanho claro é usado para gráficos de área para indicar dados volumétricos.

Amostra	Significado
	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.

Apresentação de 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 **suporte Ferramentas topologia de grade** para acessar gráficos adicionais.

O que você vai precisar

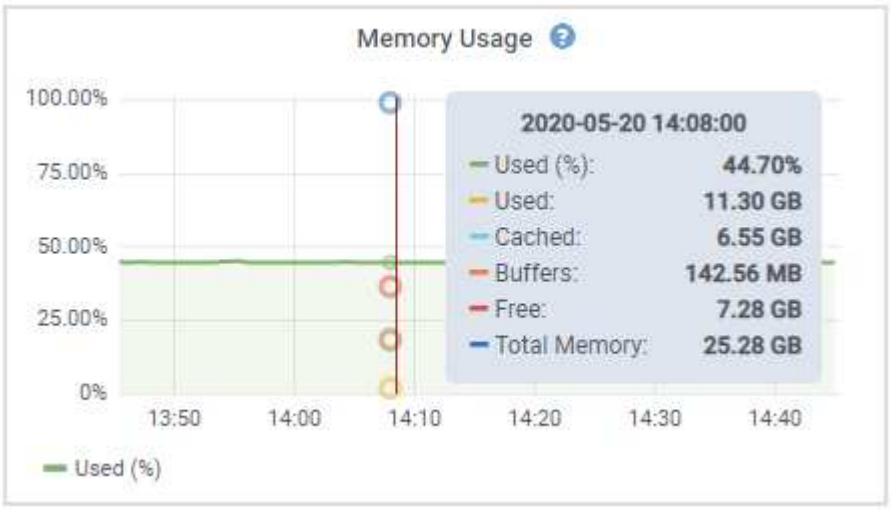
Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Selecione **nós**. Em seguida, selecione um nó, um site ou toda a grade.
2. Selecione o separador para o qual pretende ver as informações.

   Algumas guias incluem um ou mais gráficos Grafana, que são usados para plotar os valores das métricas de Prometheus ao longo do tempo. Por exemplo, a guia **nós hardware** para um nó inclui dois gráficos Grafana.

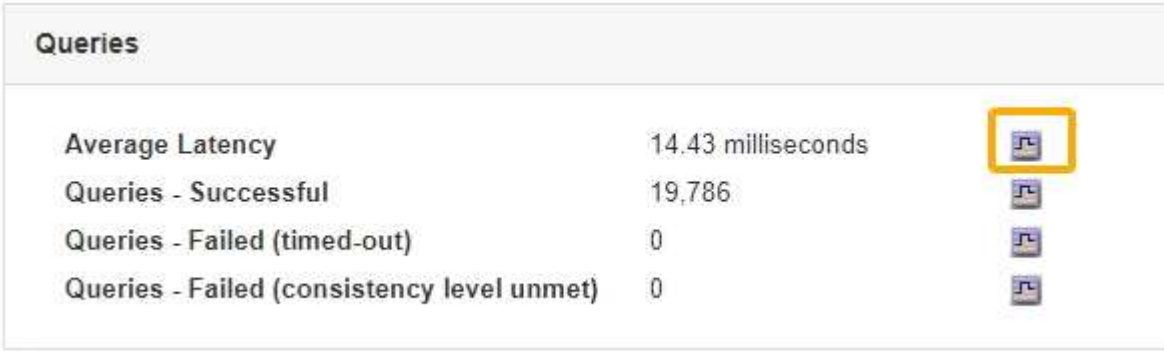
3. Opcionalmente, passe o cursor sobre o gráfico para ver valores mais detalhados para um determinado ponto no tempo.

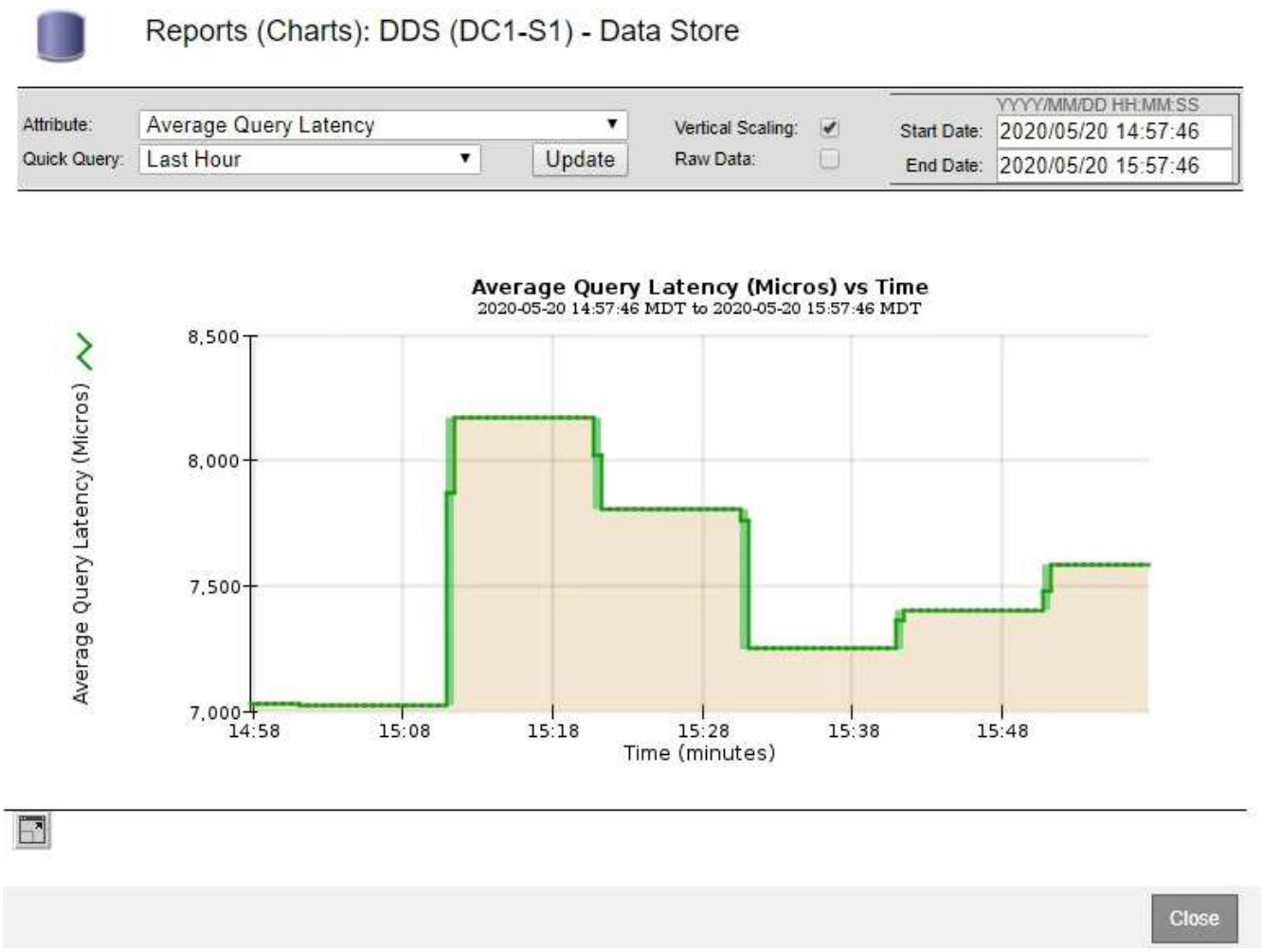


4. Conforme necessário, muitas vezes é possível exibir um gráfico para um atributo ou métrica específico. Na tabela na página nós, clique no ícone do gráfico ou à direita do nome do atributo.

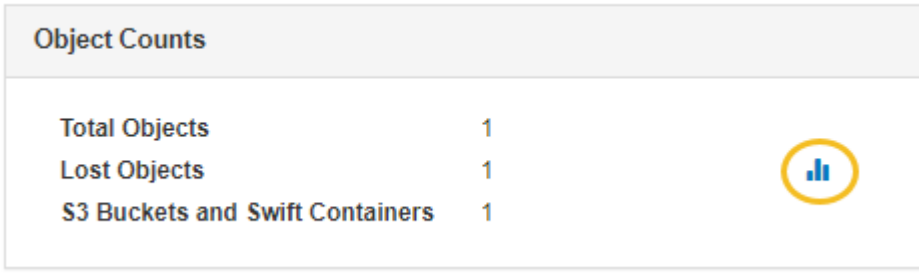
> Os gráficos não estão disponíveis para todas as métricas e atributos.

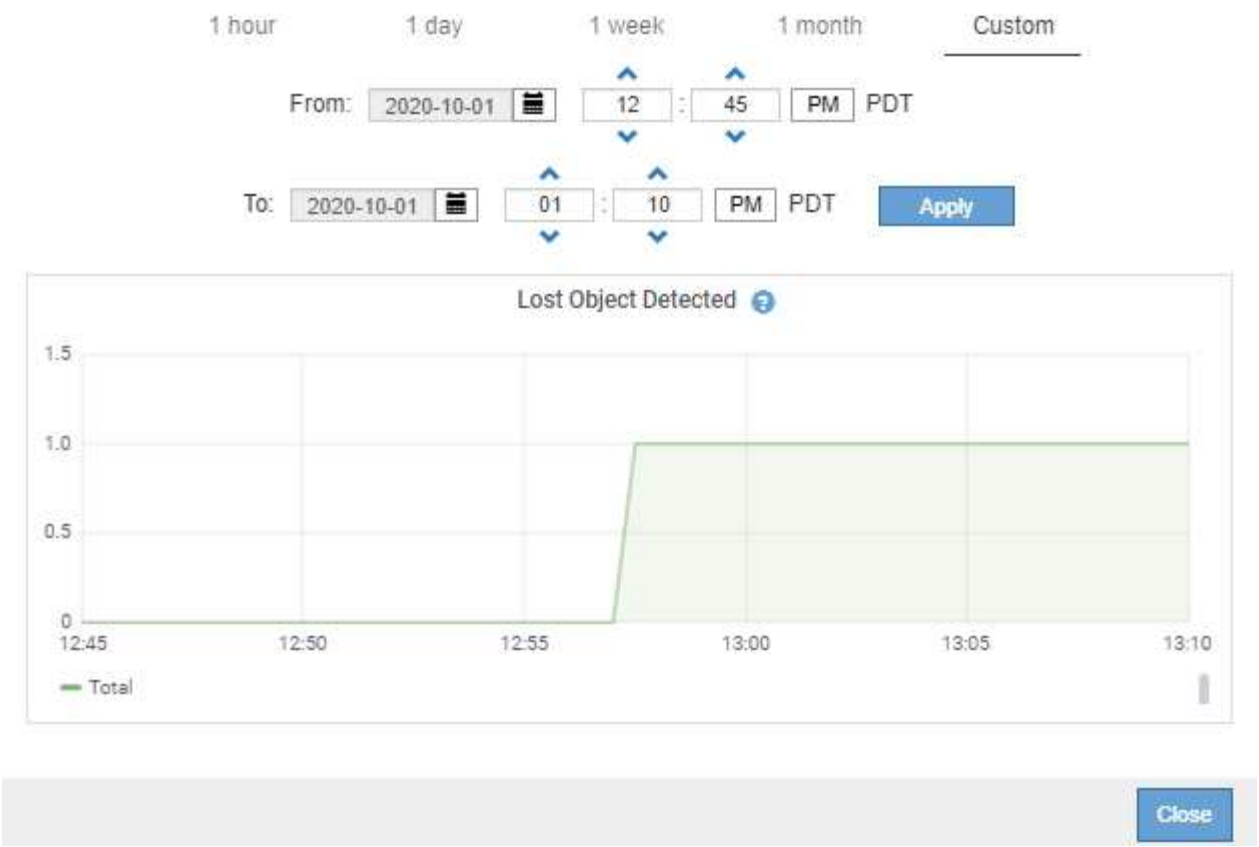
Exemplo 1: Na guia objetos de um nó de armazenamento, você pode clicar no ícone do gráfico para ver a latência média de uma consulta de metadados ao longo do tempo.



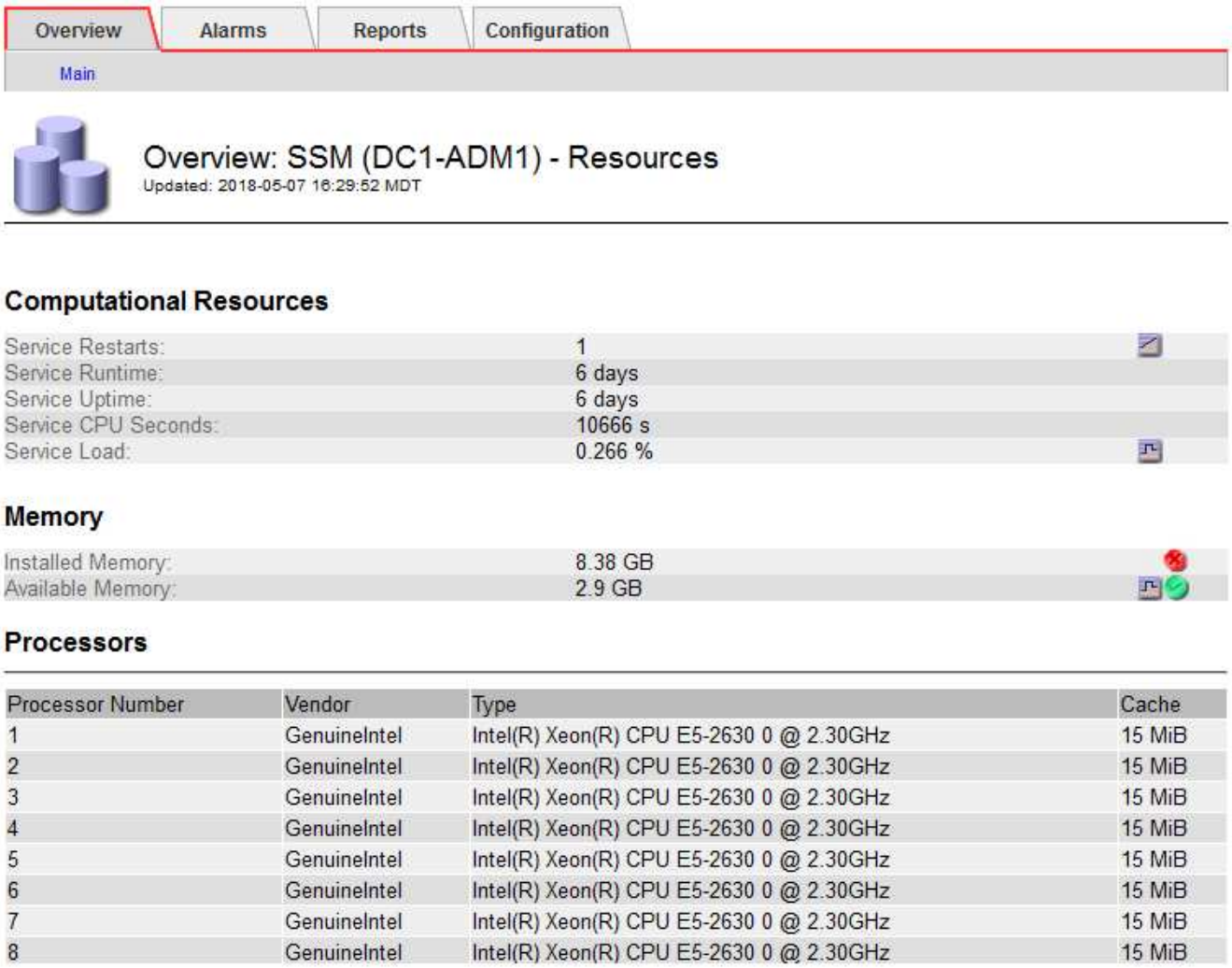


Exemplo 2: Na guia objetos de um nó de armazenamento, você pode clicar no ícone do gráfico para ver o gráfico Grafana da contagem de objetos perdidos detetados ao longo do tempo.





5. Para exibir gráficos para atributos que não são exibidos na página nó, selecione **suporte Ferramentas topologia de grade**.
6. Selecione ***grid node component ou Service*** **Overview Main**.



7. Clique no 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.

Gerando gráficos

Os gráficos exibem uma representação gráfica dos valores de dados de atributos. Você pode gerar relatórios em um local de data center, nó de grade, componente ou serviço.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***grid node component ou Service*** **Reports Charts**.
3. Selecione o atributo para relatar na lista suspensa **Atributo**.
4. Para forçar o eixo Y a iniciar em zero, desmarque a caixa de seleção **vertical Scaling**.
5. Para mostrar valores com precisão total, marque a caixa de seleção **dados brutos** ou arredondar valores

para um máximo de três casas decimais (por exemplo, para atributos relatados como porcentagens), desmarque a caixa de seleção **dados brutos**.

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

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

   O gráfico aparece após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo.

7. Se você selecionou consulta personalizada, personalize o período de tempo para o gráfico inserindo **Data de início** e **Data de término**.

   Utilize o formato *YYYY/MM/DDHH:MM:SS* na hora local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

8. Clique em **Atualizar**.

   Um gráfico 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.

9. Se pretender imprimir o gráfico, clique com o botão direito do rato e selecione **Imprimir**, modifique as definições de impressora necessárias e clique em **Imprimir**.

Tipos de 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

Gerando relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Você pode gerar relatórios em um local de data center, nó de grade, componente ou serviço.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Para dados de atributos que se espera que estejam mudando continuamente, esses dados de atributo são amostrados pelo serviço NMS (na origem) em intervalos regulares. Para dados de atributos que mudam com pouca frequência (por exemplo, dados baseados em eventos como alterações de estado ou status), um valor de atributo é enviado ao serviço NMS quando o valor muda.

O tipo de relatório apresentado depende do período de tempo configurado. Por padrão, relatórios de texto agregados são gerados para períodos de tempo superiores a uma semana.

Texto cinza indica que o serviço foi desativado administrativamente durante o período de amostragem. Texto azul indica que o serviço estava em um estado desconhecido.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***grid node component ou Service*** **Reports Text**.
3. Selecione o atributo para relatar na lista suspensa **Atributo**.
4. Selecione o número de resultados por página na lista suspensa **resultados por página**.
5. Para arredondar valores para um máximo de três casas decimais (por exemplo, para atributos reportados como porcentagens), desmarque a caixa de seleção **dados brutos**.
6. Selecione o período de tempo para relatar na lista suspensa **consulta rápida**.

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

O relatório aparece após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo.

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.

9. Se pretender imprimir o relatório, clique com o botão direito do rato e selecione **Imprimir**, modifique as definições de impressora necessárias e clique em **Imprimir**.

Exportar relatórios de texto

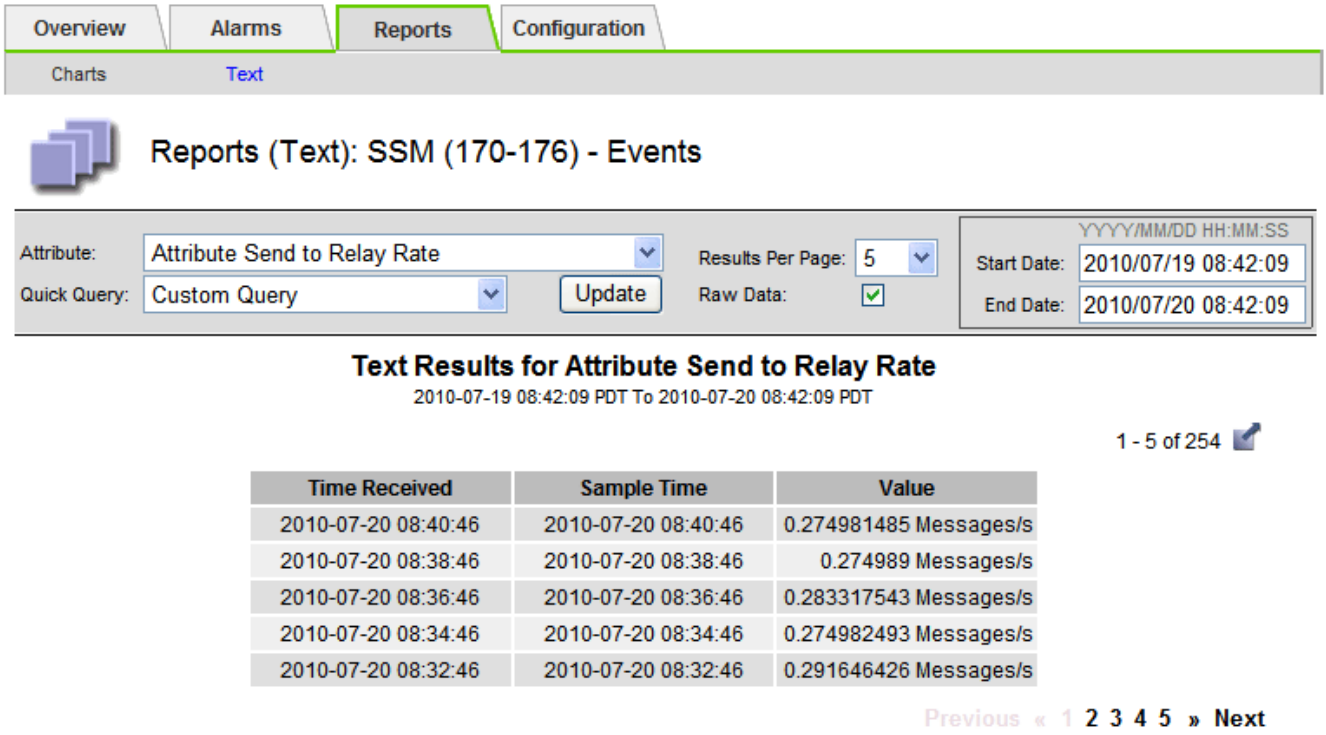
Os relatórios de texto exportados abrem uma nova guia do navegador, que permite selecionar e copiar os dados.

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: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
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.

Monitorar O PUT e obter desempenho

Você pode monitorar o desempenho de certas operações, como armazenamento e recuperação de objetos, para ajudar a identificar alterações que podem exigir mais

investigação.

Sobre esta tarefa

Para monitorar O desempenho, você pode executar comandos S3 e Swift diretamente de uma estação de trabalho ou usando o aplicativo S3tester de código aberto. O uso desses métodos permite avaliar o desempenho independentemente de fatores externos ao StorageGRID, como problemas com um aplicativo cliente ou problemas com uma rede externa.

Ao executar testes de OPERAÇÕES put and GET, use as seguintes diretrizes:

- Use tamanhos de objeto comparáveis aos objetos que você normalmente ingere em sua grade.
- Realize operações em locais locais e remotos.

As mensagens no log de auditoria indicam o tempo total necessário para executar determinadas operações. Por exemplo, para determinar o tempo total de processamento de uma solicitação GET S3, você pode revisar o valor do ATRIBUTO TIME na mensagem de auditoria SGET. Você também pode encontrar o ATRIBUTO TIME nas mensagens de auditoria para as seguintes operações:

- **S3**: EXCLUIR, OBTER, CABEÇA, METADADOS ATUALIZADOS, POSTAR, COLOCAR
- **SWIFT**: EXCLUIR, OBTER, CABEÇA, COLOCAR

Ao analisar os resultados, observe o tempo médio necessário para atender a uma solicitação, bem como o throughput geral que você pode alcançar. Repita os mesmos testes regularmente e registe os resultados, para que possa identificar tendências que possam necessitar de investigação.

- Você pode baixar S3tester de github:https://github.com/s3tester

Informações relacionadas

"Rever registos de auditoria"

Monitoramento de operações de verificação de objetos

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

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Existem dois processos de verificação que funcionam em conjunto para garantir a integridade dos dados:

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

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

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

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

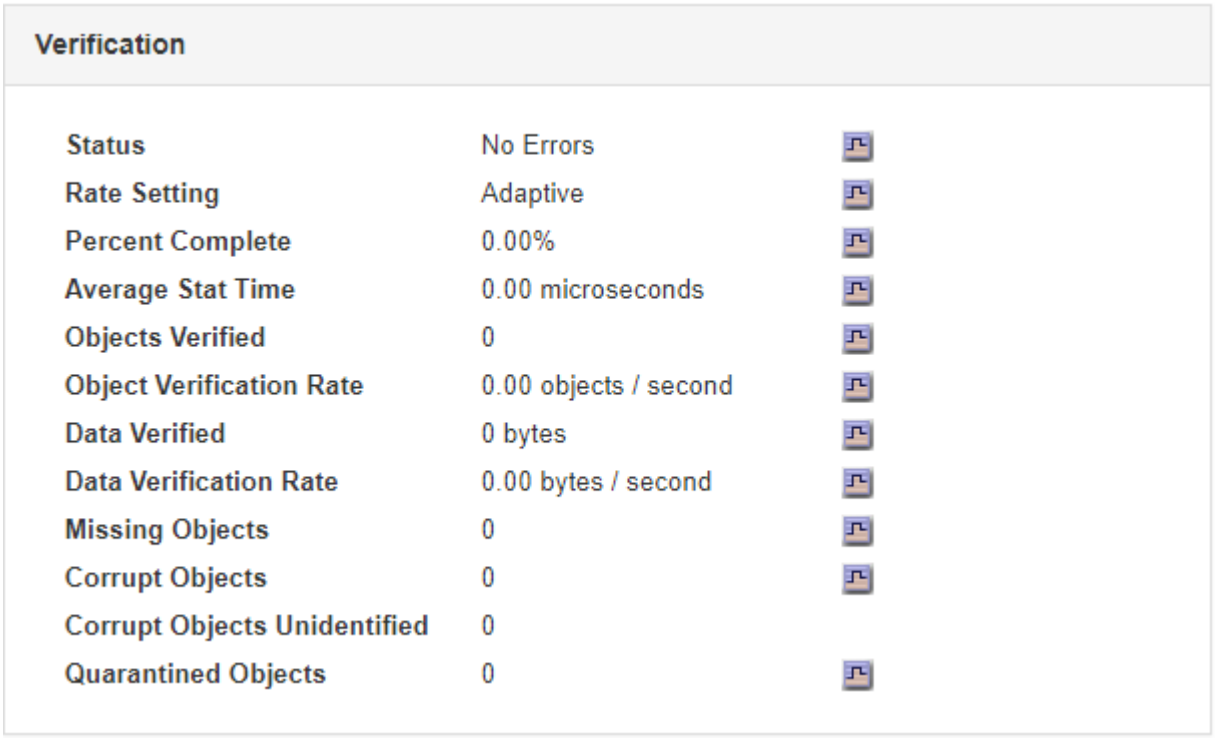
  A verificação em primeiro plano permite verificar a existência de dados de objeto replicados e codificados por apagamento em um nó de armazenamento específico, verificando se cada objeto que se espera estar presente está lá. Você pode executar a verificação em primeiro plano em todos ou alguns armazenamentos de objetos de um nó de armazenamento para ajudar a determinar se há problemas de integridade com um dispositivo de armazenamento. Um grande número de objetos ausentes pode indicar que há um problema com o armazenamento.

Para analisar os resultados de verificações em segundo plano e primeiro plano, como objetos corrompidos ou ausentes, você pode olhar para a página nós para um nó de storage. Você deve investigar quaisquer instâncias de dados de objetos corrompidos ou ausentes imediatamente, para determinar a causa raiz.

Passos

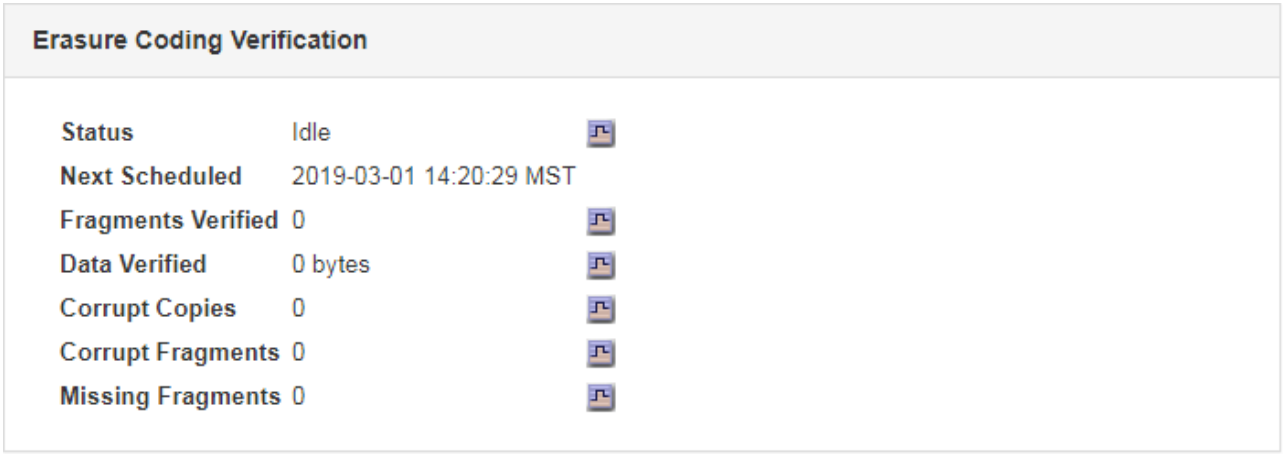
1. Selecione **nós**.
2. Selecione ***Storage Node* Objects**.
3. Para verificar os resultados da verificação:

   - Para verificar a verificação de dados de objetos replicados, observe os atributos na seção Verificação.



     Clique no nome de um atributo na tabela para exibir o texto de ajuda.

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



Clique no nome de um atributo na tabela para exibir o texto de ajuda.

Informações relacionadas

"Verificando a integridade do objeto"

Monitoramento de 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.

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.

Rever eventos a partir da página de nós

A página nós lista os eventos do sistema para cada nó de grade.

1. Selecione **nós**.
2. Selecione ***grid node* Eventos**.
3. Na parte superior da página, determine se um evento é mostrado para **último evento**, que descreve o último evento detetado pelo nó da grade.

   O evento é transmitido verbalmente a partir do nó da grade e inclui quaisquer mensagens de log com um nível de gravidade DE ERRO ou CRÍTICO.

4. Revise a tabela para ver se a contagem de qualquer evento ou erro não é zero.
5. Depois de resolver problemas, clique em **Redefinir contagens de eventos** para retornar as contagens a zero.

Rever eventos a partir da página Grid Topology (topologia de grelha)

A página topologia de Grade também lista os eventos do sistema para cada nó de grade.

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site grid node* SSM Eventos Visão geral Principal**.

Informações relacionadas

"Repor contagens de eventos"

"Referência de ficheiros de registo"

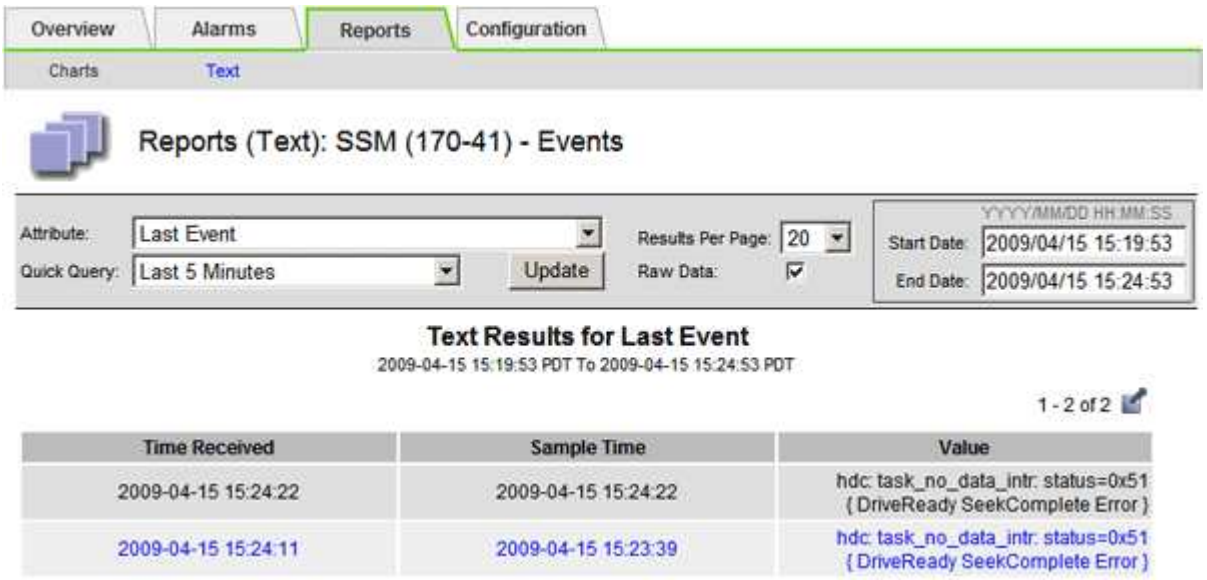
Rever eventos anteriores

Você pode gerar uma lista de mensagens de eventos anteriores para ajudar a isolar problemas que ocorreram no passado.

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site grid node* SSM Eventos relatórios**.
3. Selecione **texto**.

   O atributo **último evento** não é mostrado na visualização gráficos.

4. Altere **Atributo** para **último evento**.
5. Opcionalmente, selecione um período de tempo para **consulta rápida**.
6. Clique em **Atualizar**.



Informações relacionadas

"Usando gráficos e relatórios"

Repor contagens de eventos

Depois de resolver eventos do sistema, você pode redefinir as contagens de eventos para zero.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Configuração da Página de topologia de Grade.

Passos

1. Selecione **nós *Grid Node* Eventos**.
2. Certifique-se de que qualquer evento com uma contagem superior a 0 foi resolvido.
3. Clique em **Redefinir contagens de eventos**.

Events

Last Event No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Heap Out Of Memory Errors	0
Cassandra unhandled exceptions	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Node Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0
Stat Service Events	0
Storage Hardware Events	0
System Time Events	0

Reset event counts

Criando 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

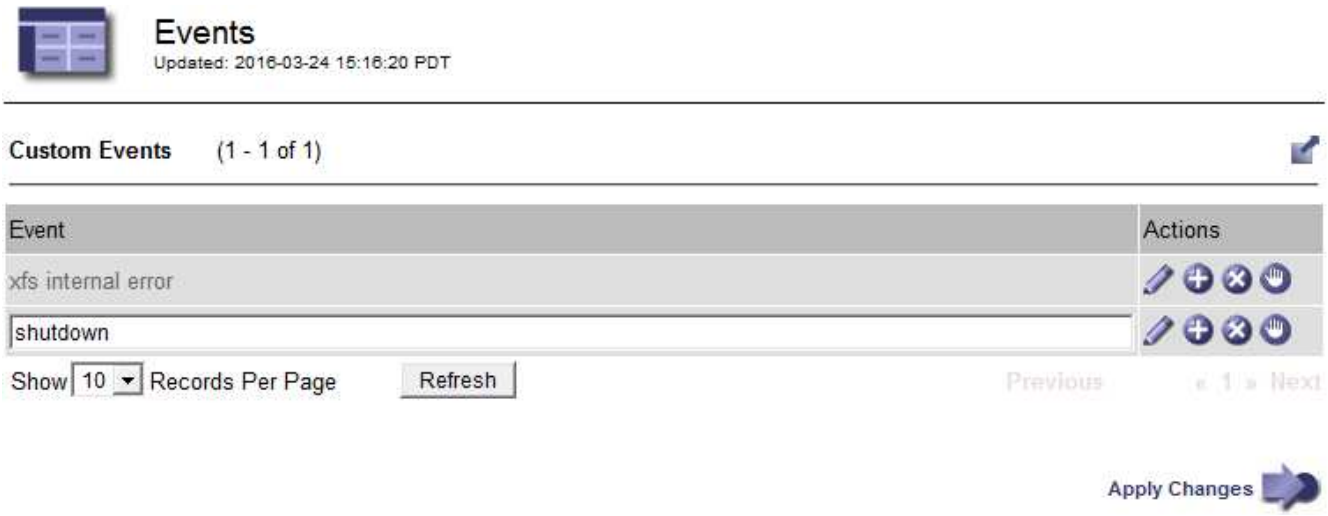
Considere criar eventos personalizados para monitorar problemas recorrentes. As considerações a seguir se aplicam a eventos personalizados.

- Depois que um evento personalizado é criado, cada ocorrência dele é monitorada. Você pode visualizar um valor de contagem cumulativa para todos os eventos personalizados na página **nós *grid node* Eventos**.
- Para criar um evento personalizado com base em palavras-chave `/var/log/messages` nos arquivos ou `/var/log/syslog`, os Registros 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/log/messages` arquivos OR `/var/log/syslog` serão correspondidas, a menos que satisfaçam os requisitos acima indicados.

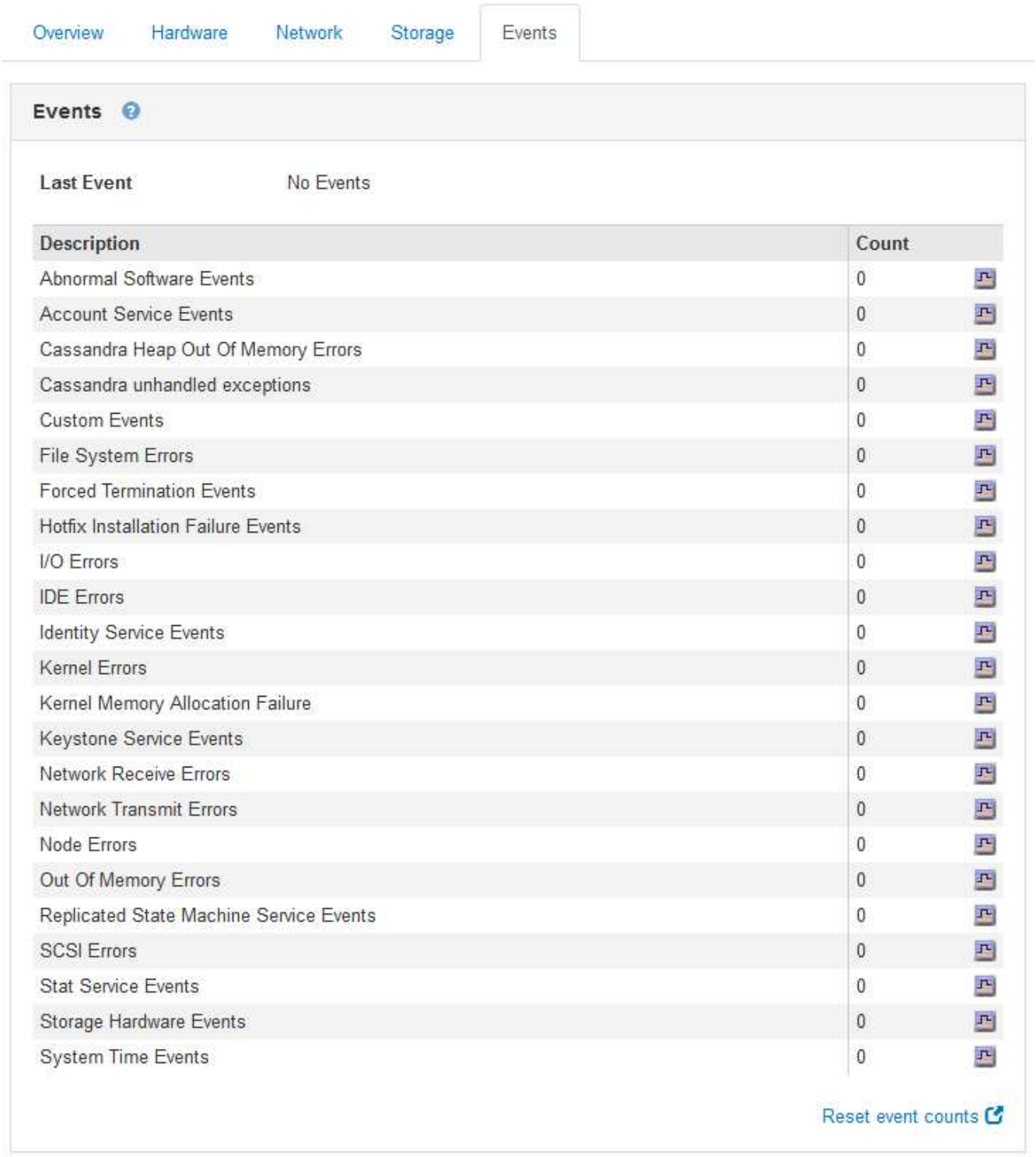
Passos

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



4. Clique em **aplicar alterações**.
5. Selecione **nós**. Em seguida, selecione ***grid node* Events**.
6. 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.



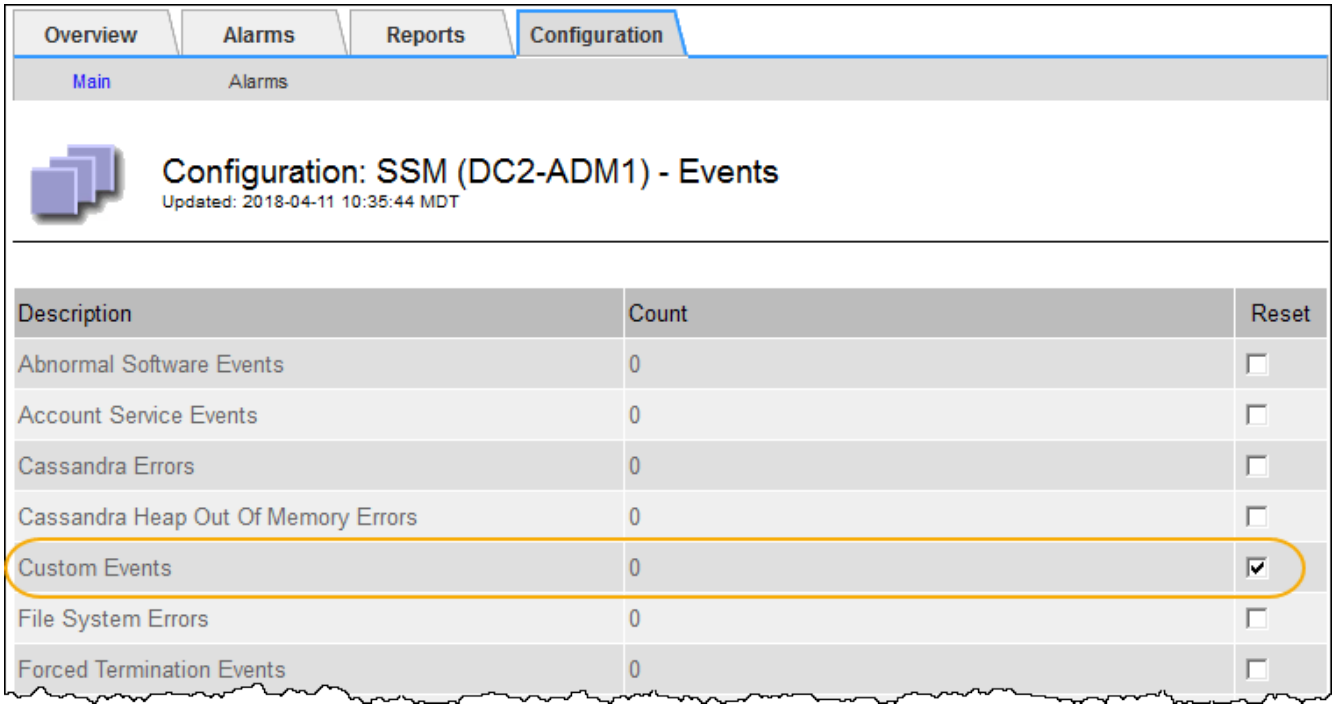
Redefinir a contagem de eventos personalizados para zero

Se você quiser redefinir o contador apenas para eventos personalizados, use a página topologia de grade no menu suporte.

Sobre esta tarefa

A reposição de um contador faz com que o alarme seja acionado pelo próximo evento. Em contraste, quando você reconhece um alarme, esse alarme só é reacionado se o próximo nível de limiar for atingido.

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***grid node* SSM Eventos Configuração Principal**.
3. Marque a caixa de seleção **Reset** para Eventos personalizados.



4. Clique em **aplicar alterações**.

Rever mensagens de auditoria

As mensagens de auditoria podem ajudá-lo a entender melhor as operações detalhadas do seu sistema StorageGRID. Você pode usar logs de auditoria para solucionar problemas e avaliar o desempenho.

Durante a operação normal do sistema, todos os serviços StorageGRID geram mensagens de auditoria, como segue:

- As mensagens de auditoria do sistema estão relacionadas ao próprio sistema de auditoria, aos estados dos nós da grade, à atividade de tarefas em todo o sistema e às operações de backup de serviço.
- As mensagens de auditoria de storage de objetos estão relacionadas ao armazenamento e gerenciamento de objetos no StorageGRID, incluindo armazenamento de objetos e recuperações, transferências de nó de grade para nó de grade e verificações.
- As mensagens de auditoria de leitura e gravação do cliente são registradas quando um aplicativo cliente S3 ou Swift faz uma solicitação para criar, modificar ou recuperar um objeto.
- As mensagens de auditoria de gerenciamento Registram solicitações de usuários para a API de gerenciamento.

Cada nó Admin armazena mensagens de auditoria em arquivos de texto. O compartilhamento de auditoria contém o arquivo ativo (audit.log), bem como logs de auditoria compatados de dias anteriores.

Para facilitar o acesso aos logs de auditoria, você pode configurar o acesso do cliente ao compartilhamento de auditoria para NFS e CIFS (obsoleto). Você também pode acessar arquivos de log de auditoria diretamente da

linha de comando do nó Admin.

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

Informações relacionadas

"Rever registos de auditoria"

"Administrar o StorageGRID"

Coletando arquivos de log e dados do sistema

Você pode usar o Gerenciador de Grade para recuperar arquivos de log e dados do sistema (incluindo dados de configuração) para seu sistema StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter a senha de provisionamento.

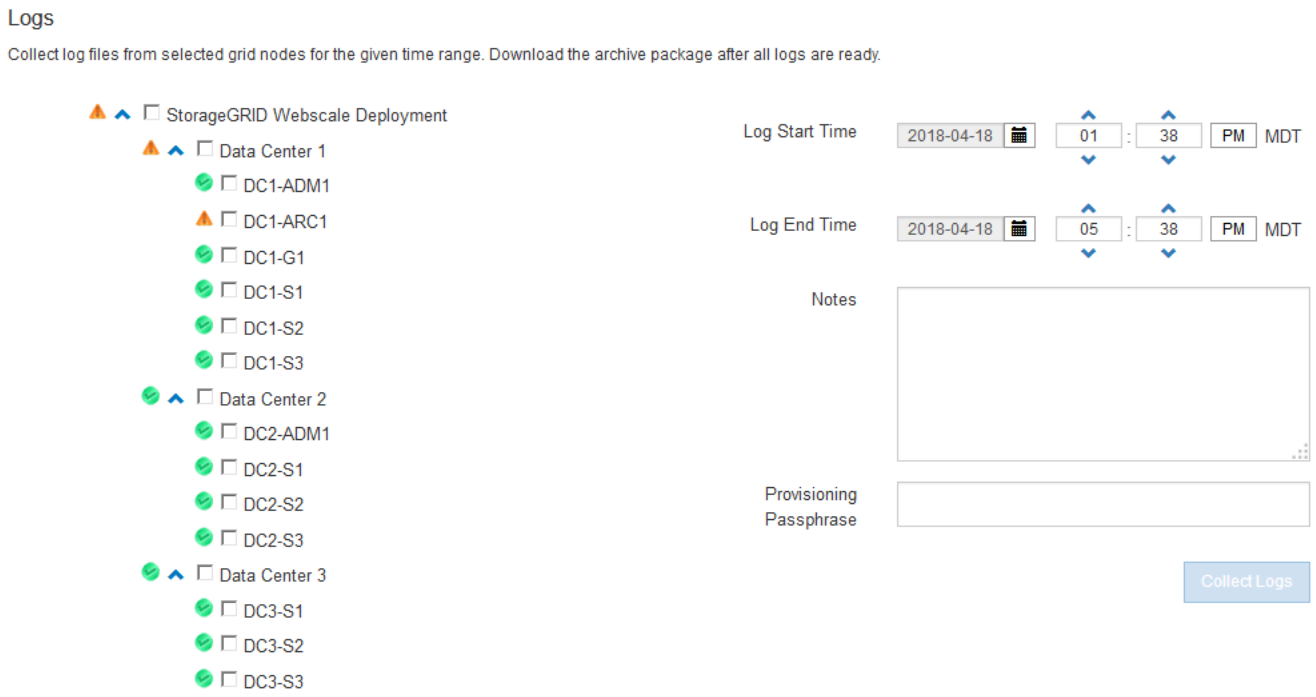
Sobre este taak

Você pode usar o Gerenciador de Grade para coletar arquivos de log, 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.

Como os arquivos de log de aplicativos podem ser muito grandes, o diretório de destino onde você baixa os arquivos de log arquivados deve ter pelo menos 1 GB de espaço livre.

Passos

1. Selecione **suporte Ferramentas 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.

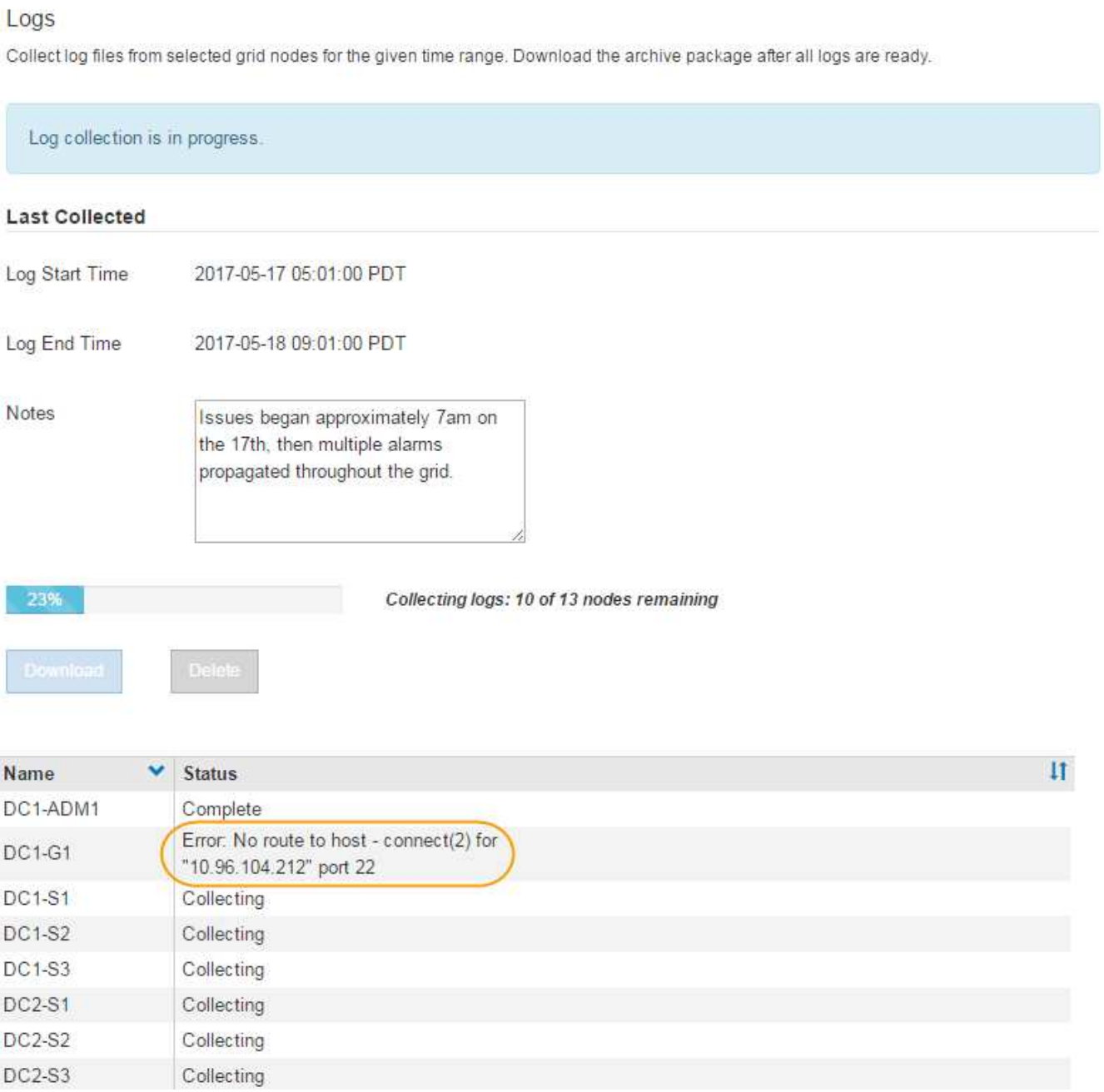
   Se você selecionar um período de tempo muito longo ou coletar logs de todos os nós em uma grade grande, o arquivo de log pode se tornar muito grande para ser armazenado em um nó ou muito grande para ser coletado para o nó de administração principal para download. Se isso ocorrer, você deve reiniciar a coleta de logs com um conjunto menor de dados.

4. Opcionalmente, digite notas sobre os arquivos de log que você está coletando 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.

5. Introduza a frase-passe de aprovisionamento do seu sistema StorageGRID na caixa de texto **frase-passe de aprovisionamento**.
6. Clique em **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.

7. Clique em **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 clicar em **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.

Informações relacionadas

"Referência de ficheiros de registo"

Acionando manualmente uma mensagem AutoSupport

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

Passos

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

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

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

   O StorageGRID tenta enviar uma mensagem do AutoSupport para o suporte técnico. Se a tentativa for bem-sucedida, os valores **resultado mais recente** e **último tempo bem-sucedido** na guia **resultados** serão atualizados. Se houver um problema, o valor **resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar a mensagem AutoSupport novamente.

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

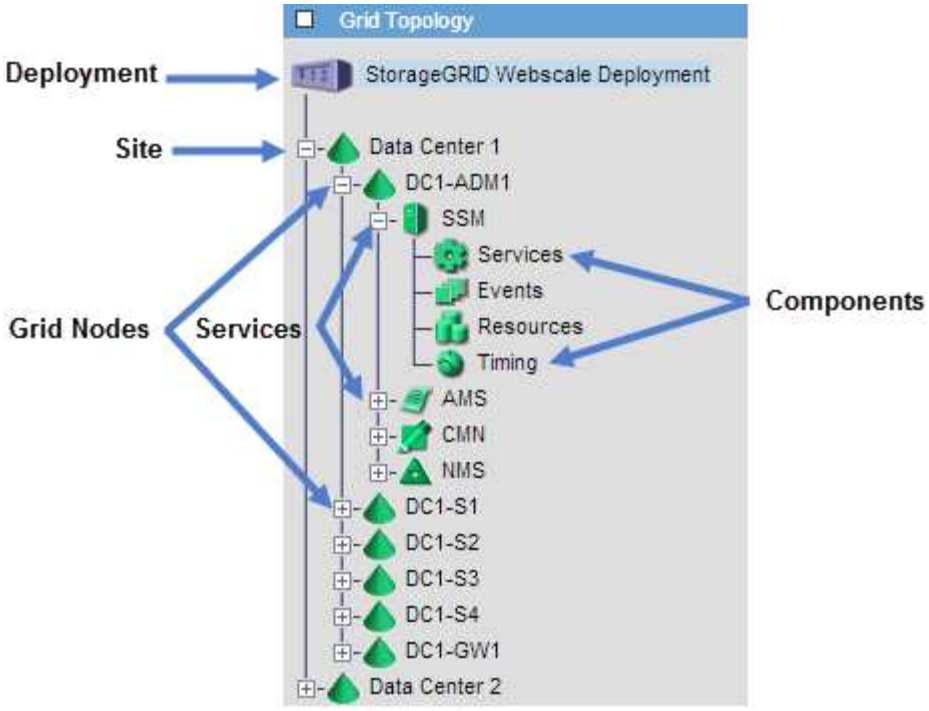
Informações relacionadas

"Configuração das configurações do servidor de e-mail para alarmes (sistema legado)"

Visualizar a árvore de topologia de grelha

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 **suporte Ferramentas topologia de grade**.



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.

Revisão das métricas de suporte

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

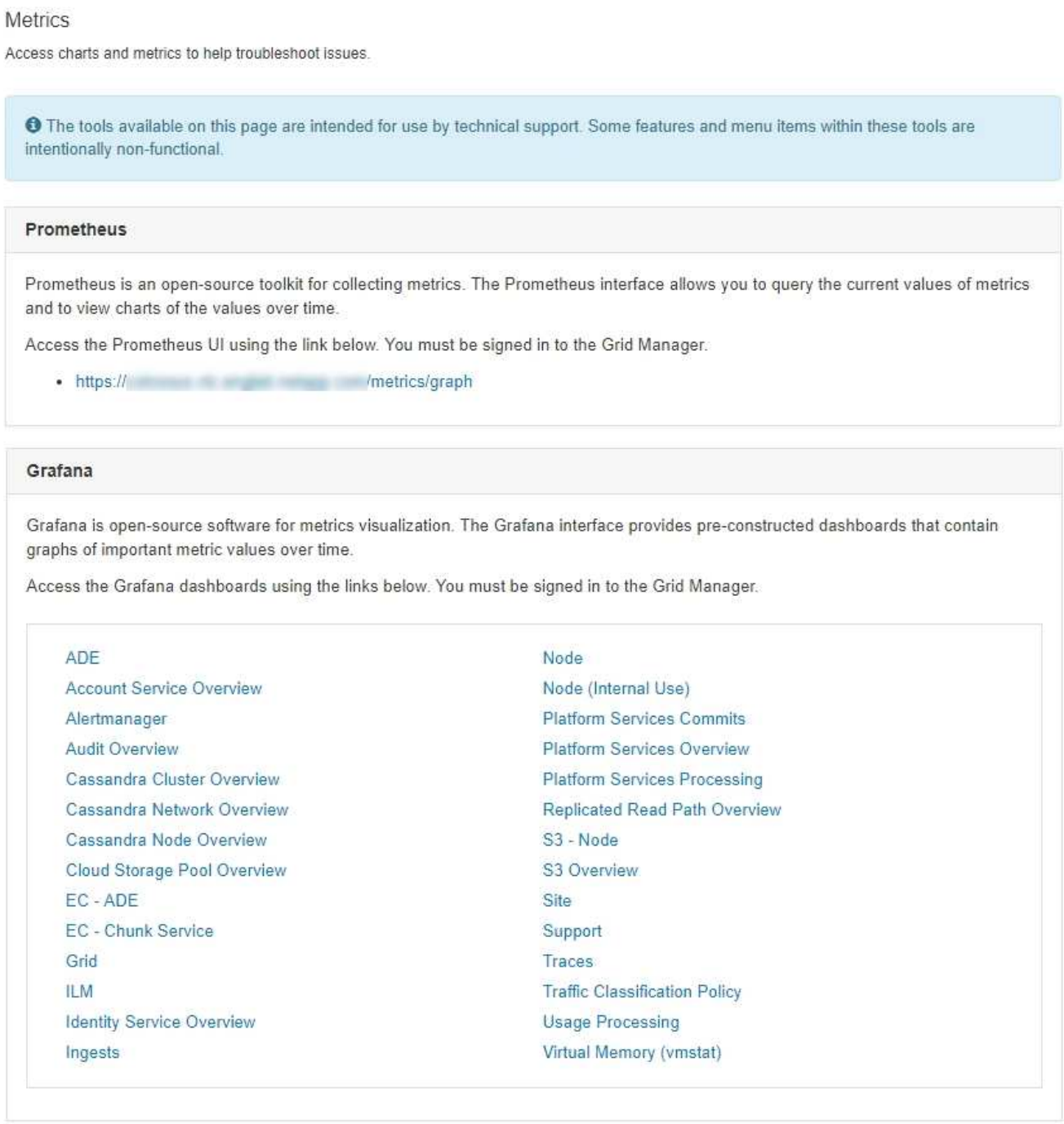
A página Metrics permite que você acesse as interfaces de usuário Prometheus e Grafana. Prometheus é um software de código aberto para coletar métricas. Grafana é um software de código aberto para visualização de métricas.

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

Passos

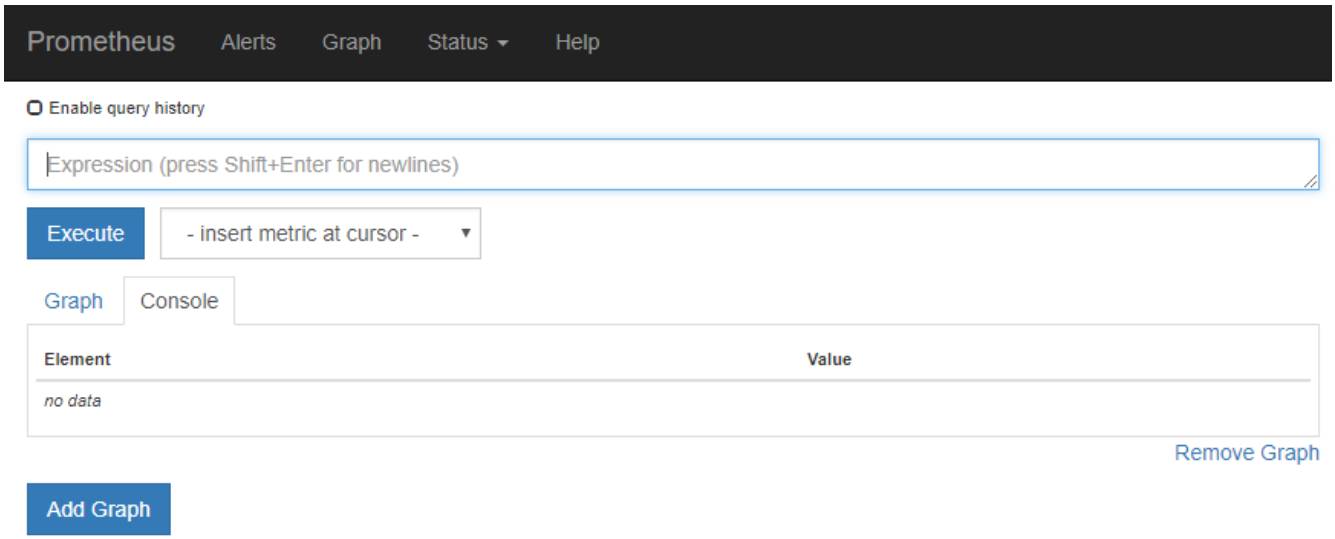
1. Conforme indicado pelo suporte técnico, selecione **suporte Ferramentas métricas**.

   É apresentada a página Metrics (métricas).



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.

Informações relacionadas

"Métricas de Prometheus comumente usadas"

A executar o diagnóstico

Ao solucionar um problema, você pode trabalhar com o suporte técnico para executar diagnósticos no sistema StorageGRID e analisar os resultados.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

A página Diagnósticos executa um conjunto de verificações de diagnóstico no estado atual da grade. Cada verificação de diagnóstico pode ter um de três Estados:

- **Normal**: Todos os valores estão dentro do intervalo normal.

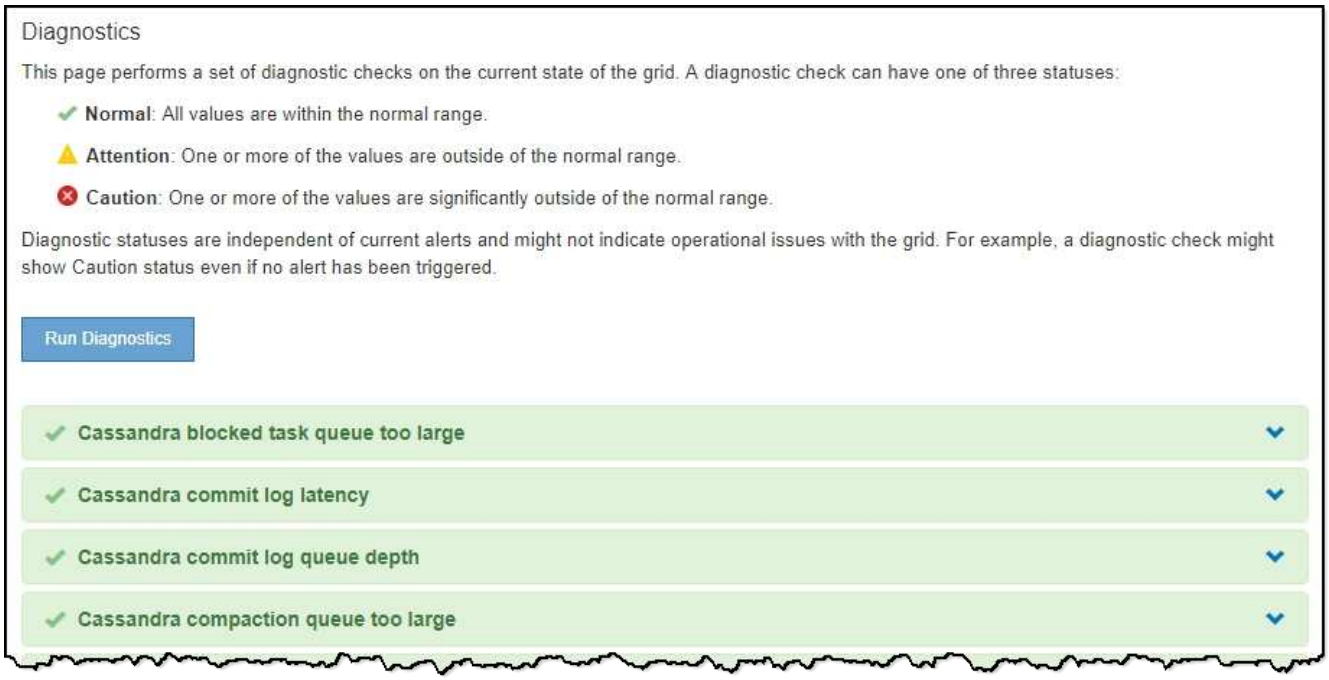
- ⚠ **Atenção**: Um ou mais valores estão fora do intervalo normal.
- ⊗ **Atenção**: Um ou mais dos valores estão significativamente fora do intervalo normal.

Os Estados de diagnóstico são independentes dos alertas atuais e podem não indicar problemas operacionais com a grade. Por exemplo, uma verificação de diagnóstico pode mostrar o estado de precaução mesmo que nenhum alerta tenha sido acionado.

Passos

1. Selecione **suporte Ferramentas Diagnóstico**.

   A página Diagnósticos é exibida e lista os resultados de cada verificação de diagnóstico. No exemplo, todos os diagnósticos têm um status normal.



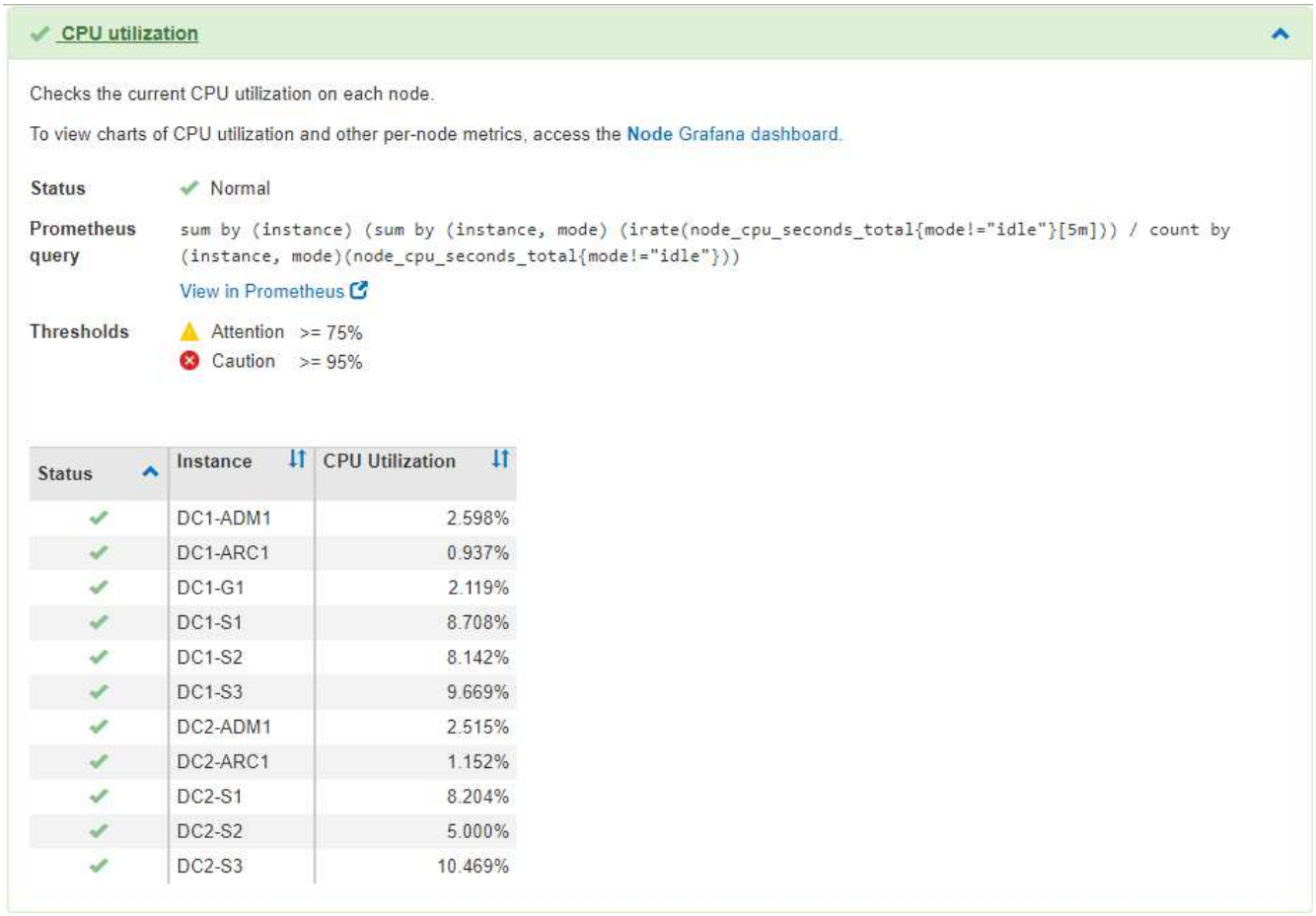
2. Para saber mais sobre um diagnóstico específico, clique em qualquer lugar da linha.

   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 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**.

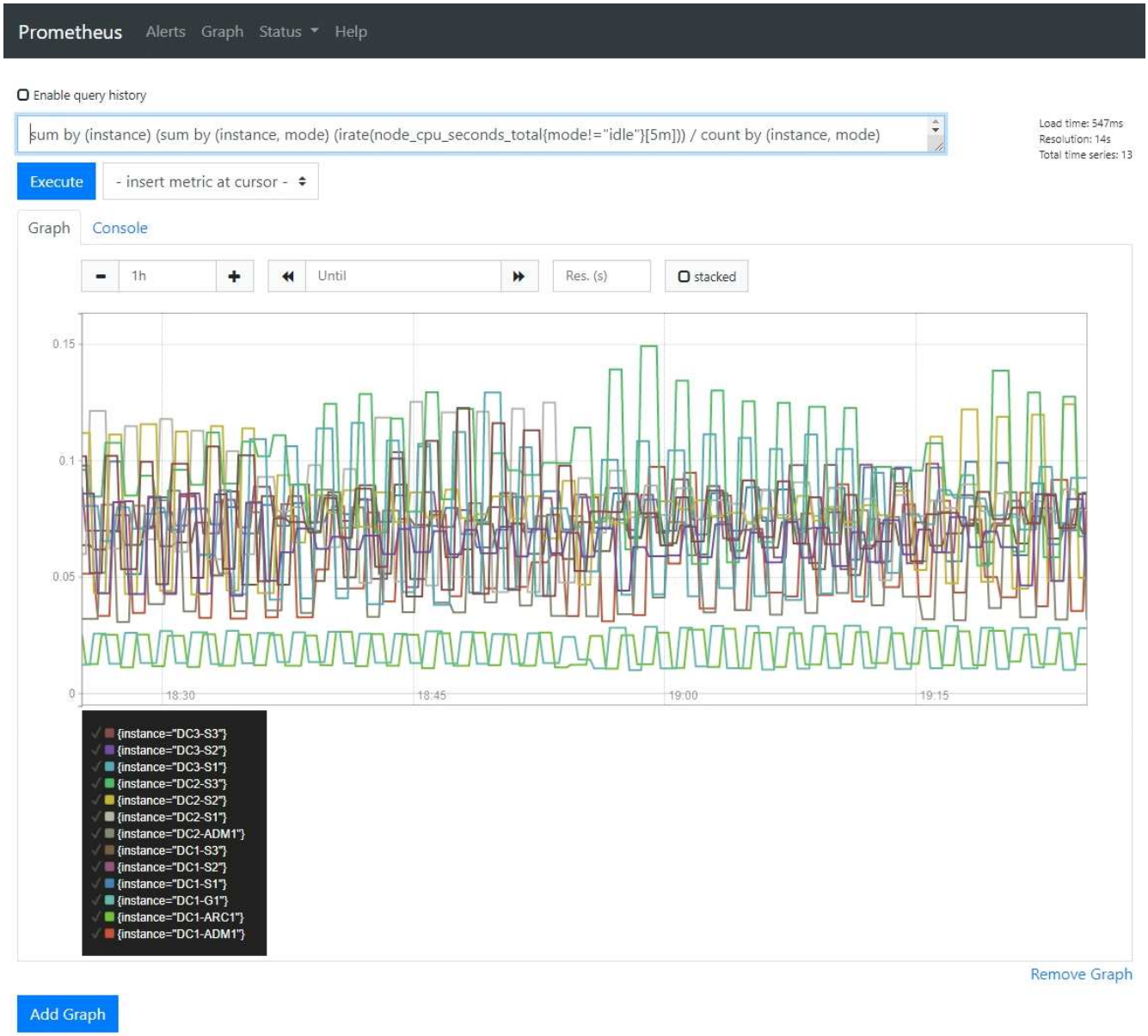
   Este link não é exibido para todos os diagnósticos.

   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 **suporte Ferramentas métricas**.

4. **Opcional**: Para ver um gráfico da expressão Prometheus ao longo do tempo, clique em **Exibir em Prometheus**.

   Aparece um gráfico Prometheus da expressão usada no diagnóstico.



Informações relacionadas

"Revisão das métricas de suporte"

"Métricas de Prometheus comumente usadas"

Criando aplicativos de monitoramento personalizados

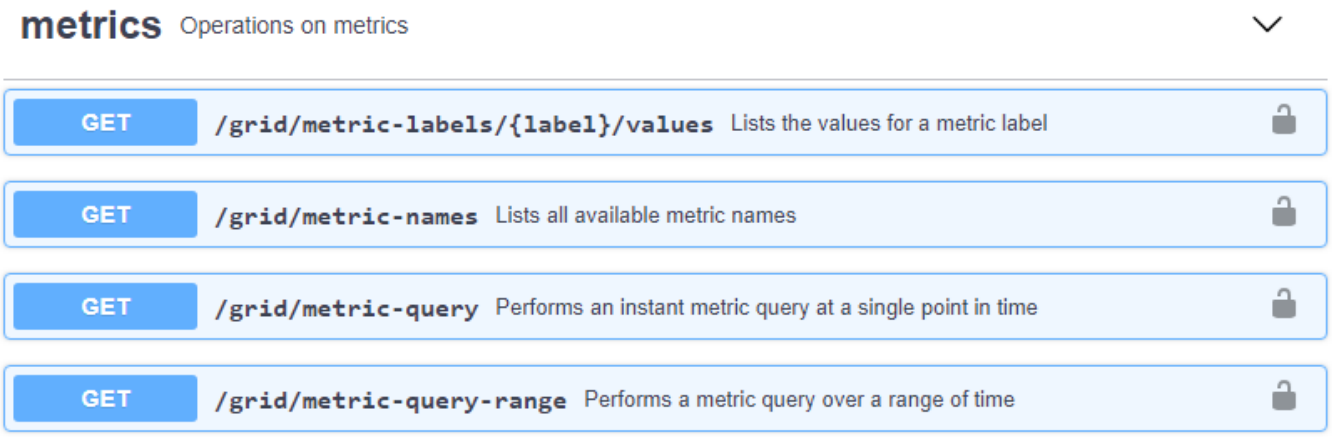
Você pode criar aplicativos e painéis de monitoramento personalizados usando as métricas do StorageGRID disponíveis na API de gerenciamento de grade.

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 as

instruções para administrar o StorageGRID.

Para visualizar as operações da API de métricas, incluindo a lista completa das métricas disponíveis, acesse o Gerenciador de Grade e selecione **Ajuda Documentação da API métricas**.



Os detalhes de como implementar um aplicativo de monitoramento personalizado estão além do escopo deste guia.

Informações relacionadas

"Administrar o StorageGRID"

Referência de alertas

A tabela a seguir lista todos os alertas padrão do StorageGRID. Conforme necessário, você pode criar regras de alerta personalizadas para se adequar à sua abordagem de gerenciamento de sistema.

Veja informações sobre as métricas do Prometheus comumente usadas para saber mais sobre as métricas usadas em alguns desses alertas.

Nome do alerta	Descrição e ações recomendadas
A bateria do aparelho expirou	A bateria do controlador de armazenamento do aparelho expirou. 1. Substitua a bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento nas instruções de instalação e manutenção do aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" 2. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
A bateria do aparelho falhou	A bateria do controlador de armazenamento do aparelho falhou. 1. Substitua a bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento nas instruções de instalação e manutenção do aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" 2. Se este alerta persistir, contacte a assistência técnica.
A bateria do aparelho não tem capacidade programada suficiente	A bateria do controlador de armazenamento do aparelho não tem capacidade de aprendizagem suficiente. 1. Substitua a bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento nas instruções de instalação e manutenção do aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" 2. Se este alerta persistir, contacte a assistência técnica.
A bateria do aparelho está quase a expirar	A bateria do controlador de armazenamento do aparelho está prestes a expirar. 1. Substitua a bateria em breve. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento nas instruções de instalação e manutenção do aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" 2. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
Bateria do aparelho removida	A bateria do controlador de armazenamento do aparelho está em falta. 1. Instale uma bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento nas instruções de instalação e manutenção do aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" 2. Se este alerta persistir, contacte a assistência técnica.
Bateria do aparelho demasiado quente	A bateria do controlador de armazenamento do aparelho está sobreaquecida. 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Investigue possíveis razões para o aumento de temperatura, como uma falha da ventoinha ou do sistema de ar condicionado, ventilação e aquecimento (HVAC). 3. Se este alerta persistir, contacte a assistência técnica.
Erro de comunicação do Appliance BMC	A comunicação com o controlador de gestão do rodapé (BMC) foi perdida. 1. Confirme se o BMC está a funcionar normalmente. Selecione **nós** e, em seguida, selecione a guia **hardware** para o nó do dispositivo. Localize o campo IP do controlador de computação BMC e navegue até esse IP. 2. Tente restaurar as comunicações BMC colocando o nó no modo de manutenção e, em seguida, desligando e voltando a ligar o aparelho. Consulte as instruções de instalação e manutenção do seu aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "Aparelhos de serviços SG100 SG1000" 3. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
Falha no dispositivo de backup do cache do dispositivo	Um dispositivo de backup de cache persistente falhou. 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Entre em Contato com o suporte técnico.
Dispositivo de backup de cache de dispositivo capacidade insuficiente	Não há capacidade insuficiente do dispositivo de backup em cache.Contate o suporte técnico.
Dispositivo de backup protegido contra gravação em cache do dispositivo	Um dispositivo de backup em cache está protegido contra gravação.Contate o suporte técnico.
Incompatibilidade do tamanho da memória cache do dispositivo	Os dois controladores do dispositivo têm tamanhos de cache diferentes.Contacte o suporte técnico.
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. 1. Verifique os componentes do hardware quanto a condições de sobreaquecimento e siga as ações recomendadas: ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Aparelhos de serviços SG100 SG1000"

Nome do alerta	Descrição e ações recomendadas
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. 1. Verifique os componentes do hardware quanto a condições de sobreaquecimento e siga as ações recomendadas: ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Aparelhos de serviços SG100 SG1000"
O controlador de computação do dispositivo precisa de atenção	Uma falha de hardware foi detetada no controlador de computação de um dispositivo StorageGRID. 1. Verifique se há erros nos componentes de hardware e siga as ações recomendadas: ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Aparelhos de serviços SG100 SG1000"

Nome do alerta	Descrição e ações recomendadas
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.este alerta pode indicar que a fonte de alimentação falhou ou que tem um problema de fornecimento de energia. 1. Verifique se há erros nos componentes de hardware e siga as ações recomendadas: ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Aparelhos de serviços SG100 SG1000"
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.este alerta pode indicar que a fonte de alimentação falhou ou que tem um problema de fornecimento de energia. 1. Verifique se há erros nos componentes de hardware e siga as ações recomendadas: ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Aparelhos de serviços SG100 SG1000"

Nome do alerta	Descrição e ações recomendadas
O serviço de monitor de hardware de computação do dispositivo parou	O serviço que monitora o status do hardware de storage parou de relatar dados. 1. Verifique o estado do serviço de estado do sistema eos na base-os. 2. Se o serviço estiver parado ou em estado de erro, reinicie o serviço. 3. Se este alerta persistir, contacte a assistência técnica.
Detectada avaria no canal de fibra do dispositivo	Há um problema com a conexão Fibre Channel entre as controladoras de storage e computação no dispositivo. 1. Verifique se há erros nos componentes de hardware (**nós *Appliance node* hardware**). Se o estatuto de qualquer um dos componentes não for "nominal", tomar as seguintes medidas: a. Verifique se os cabos Fibre Channel entre os controladores estão completamente conetados. b. Certifique-se de que os cabos Fibre Channel não apresentam dobras excessivas. c. Confirme se os módulos SFP estão devidamente encaixados. **Nota:** se este problema persistir, o sistema StorageGRID poderá tornar a ligação problemática offline automaticamente. 1. Se necessário, substitua os componentes. Consulte as instruções de instalação e manutenção do seu aparelho.
Falha na porta HBA Fibre Channel do dispositivo	Uma porta HBA Fibre Channel está falhando ou falhou.Contate o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
O cache flash do dispositivo não é ideal	As unidades usadas para o cache SSD não são ideais. 1. Substitua as unidades de cache SSD. Consulte as instruções de instalação e manutenção do aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" 2. Se este alerta persistir, contacte a assistência técnica.
Recipiente da bateria/interligação do aparelho removido	O depósito da bateria/interligação está em falta. 1. Substitua a bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento nas instruções de instalação e manutenção do aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" 2. Se este alerta persistir, contacte a assistência técnica.
Porta LACP do aparelho em falta	Uma porta em um dispositivo StorageGRID não está participando da ligação LACP. 1. Verifique a configuração do interrutor. Certifique-se de que a interface está configurada no grupo de agregação de links correto. 2. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
A fonte de alimentação geral do aparelho está degradada	A alimentação de um aparelho StorageGRID desviou-se da tensão de funcionamento recomendada. 1. Verifique o estado das fontes de alimentação A e B para determinar qual fonte de alimentação está a funcionar de forma anormal e siga as ações recomendadas: ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Aparelhos de serviços SG100 SG1000"
Falha do controlador de storage do dispositivo A	O controlador de storage A em um dispositivo StorageGRID falhou. 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento"
Falha no controlador B de storage do dispositivo	O controlador de storage B em um dispositivo StorageGRID falhou. 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento"

Nome do alerta	Descrição e ações recomendadas
Falha na unidade do controlador de armazenamento do dispositivo	Uma ou mais unidades em um dispositivo StorageGRID falhou ou não é ideal. 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento"
Problema de hardware do controlador de storage do dispositivo	O software SANtricity está relatando "precisa de atenção" para um componente em um dispositivo StorageGRID. 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento"
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. 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento"

Nome do alerta	Descrição e ações recomendadas
Falha na fonte de alimentação B do controlador de armazenamento do dispositivo	A fonte de alimentação B num aparelho StorageGRID desviou-se da tensão de funcionamento recomendada. 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento"
O serviço de monitor de hardware de armazenamento do dispositivo parou	O serviço que monitora o status do hardware de storage parou de relatar dados. 1. Verifique o estado do serviço de estado do sistema eos na base-os. 2. Se o serviço estiver parado ou em estado de erro, reinicie o serviço. 3. Se este alerta persistir, contacte a assistência técnica.
Prateleiras de storage do dispositivo degradadas	O status de um dos componentes na prateleira de armazenamento de um dispositivo de armazenamento é degradado. 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho: ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento"

Nome do alerta	Descrição e ações recomendadas
Temperatura do aparelho excedida	A temperatura nominal ou máxima para o controlador de armazenamento do aparelho foi excedida. 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Investigue possíveis razões para o aumento de temperatura, como uma falha da ventoinha ou do sistema de ar condicionado, ventilação e aquecimento (HVAC). 3. Se este alerta persistir, contacte a assistência técnica.
Sensor de temperatura do aparelho removido	Um sensor de temperatura foi removido. Entre em Contato com o suporte técnico.
Erro de auto-compactador Cassandra	O compactador automático Cassandra apresentou um erro. O compactador automático Cassandra existe em todos os nós de armazenamento e gerencia o tamanho do banco de dados Cassandra para substituir e excluir cargas de trabalho pesadas. Embora essa condição persista, certas cargas de trabalho sofrerão um consumo inesperadamente alto de metadados. 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Entre em Contato com o suporte técnico.
Métricas do compactador automático Cassandra desatualizadas	As métricas que descrevem o compactador automático Cassandra estão desatualizadas. O compactador automático Cassandra existe em todos os nós de storage e gerencia o tamanho do banco de dados Cassandra para substituir e excluir cargas de trabalho pesadas. Embora esse alerta persista, certas cargas de trabalho sofrerão um consumo inesperadamente alto de metadados. 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Entre em Contato com o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Erro de comunicação Cassandra	Os nós que executam o serviço Cassandra estão tendo problemas para se comunicar uns com os outros. Este alerta indica que algo está interferindo nas comunicações nó-a-nó. Pode haver um problema de rede ou o serviço Cassandra pode estar inativo em um ou mais nós de storage. 1. Determine se há outro alerta afetando um ou mais nós de storage. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Verifique se há um problema de rede que possa estar afetando um ou mais nós de storage. 3. Selecione **Support** > **Tools** > **Grid Topology**. 4. Para cada nó de armazenamento no seu sistema, selecione **SSM Serviços**. Assegurar-se de que o estatuto do serviço Cassandra é ""em execução".". 5. Se o Cassandra não estiver em execução, siga as etapas para iniciar ou reiniciar um serviço nas instruções de recuperação e manutenção. 6. Se todas as instâncias do serviço Cassandra estiverem em execução e o alerta não for resolvido, entre em Contato com o suporte técnico. "Manter recuperar"
Cassandra compactions sobrecarregado	O processo de compactação Cassandra está sobrecarregado. Se o processo de compactação estiver sobrecarregado, o desempenho de leitura pode ser degradado e a RAM pode ser usada. O serviço Cassandra também pode ficar sem resposta ou falhar. 1. Reinicie o serviço Cassandra seguindo as etapas para reiniciar um serviço nas instruções de recuperação e manutenção. 2. Se este alerta persistir, contacte a assistência técnica. "Manter recuperar"

Nome do alerta	Descrição e ações recomendadas
Métricas de reparo do Cassandra desatualizadas	As métricas que descrevem os trabalhos de reparo do Cassandra estão desatualizadas. Se essa condição persistir por mais de 48 horas, as consultas de clientes, como listas de intervalos, podem mostrar dados excluídos. 1. Reinicie o nó. No Gerenciador de Grade, vá para **nós**, selecione o nó e selecione a guia tarefas. 2. Se este alerta persistir, contacte a assistência técnica.
O progresso do reparo do Cassandra lento	O progresso dos reparos do banco de dados Cassandra é lento. Quando os reparos do banco de dados são lentos, as operações de consistência de dados Cassandra são impedidas. Se essa condição persistir por mais de 48 horas, as consultas de clientes, como listas de intervalos, podem mostrar dados excluídos. 1. Confirme se todos os nós de storage estão online e não há alertas relacionados à rede. 2. Monitore esse alerta por até 2 dias para ver se o problema resolve por conta própria. 3. Se as reparações da base de dados continuarem a prosseguir lentamente, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
O serviço de reparação Cassandra não está disponível	O serviço de reparo Cassandra não está disponível. O serviço de reparo Cassandra existe em todos os nós de armazenamento e fornece funções de reparo críticas para o banco de dados Cassandra. Se essa condição persistir por mais de 48 horas, as consultas de clientes, como listas de intervalos, podem mostrar dados excluídos. 1. Selecione **Support** > **Tools** > **Grid Topology**. 2. Para cada nó de armazenamento no seu sistema, selecione **SSM Serviços**. Certifique-se de que o status do serviço Cassandra Reaper é "em execução". 3. Se o Cassandra Reaper não estiver em execução, siga as etapas para iniciar ou reiniciar um serviço nas instruções de recuperação e manutenção. 4. Se todas as instâncias do serviço Cassandra Reaper estiverem em execução e o alerta não for resolvido, entre em Contato com o suporte técnico. "Manter recuperar"
Erro de conetividade do Cloud Storage Pool	A verificação de integridade dos pools de armazenamento em nuvem detetou um ou mais erros novos. 1. Vá para a seção Cloud Storage Pools da página Storage Pools. 2. Observe a coluna último erro para determinar qual pool de armazenamento em nuvem tem um erro. 3. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações. "Gerenciar objetos com ILM"

Nome do alerta	Descrição e ações recomendadas
A concessão DHCP expirou	A concessão DHCP numa interface de rede expirou.se a concessão DHCP expirou, siga as ações recomendadas: 1. Certifique-se de que existe conetividade entre este nó e o servidor DHCP na interface afetada. 2. Certifique-se de que existem endereços IP disponíveis para atribuir na sub-rede afetada no servidor DHCP. 3. Certifique-se de que existe uma reserva permanente para o endereço IP configurado no servidor DHCP. Ou use a ferramenta StorageGRID Change IP para atribuir um endereço IP estático fora do pool de endereços DHCP. Consulte as instruções de recuperação e manutenção. "Manter recuperar"
A concessão DHCP expira em breve	A concessão DHCP em uma interface de rede está expirando em breve. Para evitar que a concessão DHCP expire, siga as ações recomendadas: 1. Certifique-se de que existe conetividade entre este nó e o servidor DHCP na interface afetada. 2. Certifique-se de que existem endereços IP disponíveis para atribuir na sub-rede afetada no servidor DHCP. 3. Certifique-se de que existe uma reserva permanente para o endereço IP configurado no servidor DHCP. Ou use a ferramenta StorageGRID Change IP para atribuir um endereço IP estático fora do pool de endereços DHCP. Consulte as instruções de recuperação e manutenção. "Manter recuperar"

Nome do alerta	Descrição e ações recomendadas
Servidor DHCP indisponível	O servidor DHCP não está disponível.o nó StorageGRID não consegue contactar o servidor DHCP. A concessão DHCP para o endereço IP do nó não pode ser validada. 1. Certifique-se de que existe conetividade entre este nó e o servidor DHCP na interface afetada. 2. Certifique-se de que existem endereços IP disponíveis para atribuir na sub-rede afetada no servidor DHCP. 3. Certifique-se de que existe uma reserva permanente para o endereço IP configurado no servidor DHCP. Ou use a ferramenta StorageGRID Change IP para atribuir um endereço IP estático fora do pool de endereços DHCP. Consulte as instruções de recuperação e manutenção. "Manter recuperar"
A e/S do disco é muito lenta	E/S de disco muito lento pode estar impactando o desempenho do StorageGRID. 1. Se o problema estiver relacionado a um nó de dispositivo de armazenamento, use o Gerenciador de sistema SANtricity para verificar se há unidades com defeito, unidades com falhas previstas ou reparos em andamento. Verifique também o status dos links Fibre Channel ou SAS entre a computação do dispositivo e os controladores de storage para ver se há algum link inativo ou mostrando taxas de erro excessivas. 2. Examine o sistema de armazenamento que hospeda os volumes deste nó para determinar e corrigir a causa raiz da e/S lenta 3. Se este alerta persistir, contacte a assistência técnica. Os nós afetados podem desativar os serviços e reinicializar-se para evitar afetar o desempenho geral da grade. Quando a condição subjacente for limpa e esses nós detetarem o desempenho normal de e/S, eles retornarão ao serviço completo automaticamente.

Nome do alerta	Descrição e ações recomendadas
Falha na notificação por e-mail	Não foi possível enviar a notificação por e-mail de um alerta.este alerta é acionado quando uma notificação por e-mail de alerta falhar ou um e-mail de teste (enviado da página **Alertas Configuração de e-mail**) não pode ser entregue. 1. Inicie sessão no Grid Manager a partir do Admin Node listado na coluna **Site/nó** do alerta. 2. Vá para a página **Alertas Configuração de e-mail**, verifique as configurações e altere-as, se necessário. 3. Clique em **Enviar e-mail de teste** e verifique a caixa de entrada de um destinatário de teste para o e-mail. Uma nova instância desse alerta pode ser acionada se o e-mail de teste não puder ser enviado. 4. Se o e-mail de teste não puder ser enviado, confirme se o servidor de e-mail está online. 5. Se o servidor estiver funcionando, selecione **suporte Ferramentas Logs** e colete o log para o nó Admin. Especifique um período de tempo que seja de 15 minutos antes e depois da hora do alerta. 6. Extraia o arquivo baixado e revise o conteúdo do `prometheus.log` (`_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log`). 7. Se não conseguir resolver o problema, contacte o suporte técnico.
Expiração de certificados configurados na página certificados de cliente	Um ou mais certificados configurados na página certificados de cliente estão prestes a expirar. 1. Selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**. 2. Selecione um certificado que expirará em breve. 3. Selecione **Editar** para carregar ou gerar um novo certificado. 4. Repita estas etapas para cada certificado que expirará em breve. "Administrar o StorageGRID"

Nome do alerta	Descrição e ações recomendadas
Expiração do certificado de ponto final do balanceador de carga	Um ou mais certificados de endpoint do balanceador de carga estão prestes a expirar. 1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**. 2. Selecione um endpoint que tenha um certificado que expirará em breve. 3. Selecione **Editar endpoint** para carregar ou gerar um novo certificado. 4. Repita essas etapas para cada ponto final que tenha um certificado expirado ou que expirará em breve. Para obter mais informações sobre como gerenciar pontos de extremidade do balanceador de carga, consulte as instruções de administração do StorageGRID. "Administrar o StorageGRID"
Expiração do certificado do servidor para a interface de gerenciamento	O certificado do servidor usado para a interface de gerenciamento está prestes a expirar. 1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**. 2. Na seção certificado do servidor de interface de gerenciamento, carregue um novo certificado. "Administrar o StorageGRID"
Expiração do certificado do servidor para os Endpoints da API Storage	O certificado do servidor usado para acessar endpoints da API de armazenamento está prestes a expirar. 1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**. 2. Na seção Object Storage API Service Endpoints Server Certificate (certificado do servidor de Endpoints), faça o upload de um novo certificado. "Administrar o StorageGRID"

Nome do alerta	Descrição e ações recomendadas
Incompatibilidade da MTU da rede da grelha	A configuração da unidade de transmissão máxima (MTU) para a interface de rede de Grade (eth0) difere significativamente entre nós na grade. 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. "Solução de problemas do alerta de incompatibilidade da MTU da rede de Grade"
Alto uso de heap Java	Uma alta porcentagem de espaço de heap Java está sendo usada. Se o heap Java ficar cheio, os serviços de metadados podem ficar indisponíveis e as solicitações do cliente podem falhar. 1. Reveja a atividade do ILM no Dashboard. Esse alerta pode ser resolvido por conta própria quando a carga de trabalho do ILM diminui. 2. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 3. Se este alerta persistir, contacte a assistência técnica.
Alta latência para consultas de metadados	O tempo médio para consultas de metadados do Cassandra é muito longo. Um aumento na latência de consulta pode ser causado por uma alteração de hardware, como a substituição de um disco ou uma alteração de carga de trabalho, como um aumento súbito de ingerências. 1. Determine se houve alterações de hardware ou carga de trabalho em torno do tempo em que a latência da consulta aumentou. 2. Se não conseguir resolver o problema, contacte o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Falha na sincronização da federação de identidade	Não é possível sincronizar grupos federados e usuários da origem da identidade. 1. Confirme se o servidor LDAP configurado está online e disponível. 2. Revise as configurações na página Federação de identidade. Confirme se todos os valores são atuais. Consulte ""Configurando uma fonte de identidade federada"" nas instruções de administração do StorageGRID. 3. Clique em **Test Connection** para validar as configurações do servidor LDAP. 4. Se não conseguir resolver o problema, contacte o suporte técnico. "Administrar o StorageGRID"

Nome do alerta	Descrição e ações recomendadas
Colocação de ILM inalcançável	Uma instrução de colocação em uma regra ILM não pode ser alcançada para determinados objetos. Este alerta indica que um nó exigido por uma instrução de colocação não está disponível ou que uma regra ILM está mal configurada. Por exemplo, uma regra pode especificar mais cópias replicadas do que há nós de storage. 1. Certifique-se de que todos os nós estejam online. 2. Se todos os nós estiverem on-line, revise as instruções de posicionamento em todas as regras ILM usadas na política ILM ativa. Confirme se existem instruções válidas para todos os objetos. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações. 3. Conforme necessário, atualize as configurações das regras e ative uma nova política. Pode demorar até 1 dia para que o alerta seja apagado. 4. Se o problema persistir, entre em Contato com o suporte técnico. Esse alerta pode aparecer durante uma atualização e pode persistir por 1 dia após a atualização ser concluída com êxito. Quando esse alerta é acionado por uma atualização, ele será apagado por conta própria. "Gerenciar objetos com ILM"

Nome do alerta	Descrição e ações recomendadas
Período de digitalização ILM demasiado longo	O tempo necessário para digitalizar, avaliar objetos e aplicar ILM é muito longo.se o tempo estimado para concluir uma varredura ILM completa de todos os objetos for muito longo (consulte **período de digitalização - estimado** no Dashboard), a política ILM ativa pode não ser aplicada a objetos recém-ingeridos. As alterações à política ILM podem não ser aplicadas a objetos existentes. 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Confirme se todos os nós de storage estão online. 3. Reduza temporariamente a quantidade de tráfego do cliente. Por exemplo, no Gerenciador de Grade, selecione **Configuração Configurações de rede classificação de tráfego** e crie uma política que limite a largura de banda ou o número de solicitações. 4. Se a e/S de disco ou a CPU estiverem sobrecarregadas, tente reduzir a carga ou aumentar o recurso. 5. Se necessário, atualize as regras do ILM para usar o posicionamento síncrono (padrão para regras criadas após o StorageGRID 11,3). 6. Se este alerta persistir, contacte a assistência técnica. "Administrar o StorageGRID"
Taxa de digitalização ILM baixa	A taxa de digitalização ILM está definida para menos de 100 objetos/segundo. Este alerta indica que alguém alterou a taxa de digitalização ILM para o seu sistema para menos de 100 objetos/segundo (predefinição: 400 objetos/segundo). A política ILM ativa pode não ser aplicada a objetos recém-ingeridos. As alterações subsequentes à política ILM não serão aplicadas a objetos existentes. 1. Determine se foi efetuada uma alteração temporária à taxa de digitalização ILM como parte de uma investigação de suporte em curso. 2. Entre em Contato com o suporte técnico. Nunca altere a taxa de digitalização ILM sem contactar o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
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. 1. Usando o software KMS, atualize o certificado da CA para o servidor de gerenciamento de chaves. 2. No Gerenciador de Grade, selecione **Configuração Configurações do sistema servidor de gerenciamento de chaves**. 3. Selecione o KMS que tem um aviso de status de certificado. 4. Selecione **Editar**. 5. Selecione **Next** para ir para a Etapa 2 (carregar certificado do servidor). 6. Selecione **Procurar** para carregar o novo certificado. 7. Selecione **Guardar**. "Administrar o StorageGRID"
Expiração do certificado do cliente KMS	O certificado de cliente para um servidor de gerenciamento de chaves está prestes a expirar. 1. No Gerenciador de Grade, selecione **Configuração Configurações do sistema servidor de gerenciamento de chaves**. 2. Selecione o KMS que tem um aviso de status de certificado. 3. Selecione **Editar**. 4. Selecione **Next** para ir para a Etapa 3 (carregar certificados de cliente). 5. Selecione **Procurar** para carregar o novo certificado. 6. Selecione **Procurar** para carregar a nova chave privada. 7. Selecione **Guardar**. "Administrar o StorageGRID"

Nome do alerta	Descrição e ações recomendadas
Falha ao carregar a configuração DE KMS	A configuração para o servidor de gerenciamento de chaves existe, mas não foi possível carregar. 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Se este alerta persistir, contacte a assistência técnica.
Erro de conetividade DE KMS	Um nó de dispositivo não pôde se conetar ao servidor de gerenciamento de chaves para seu site. 1. No Gerenciador de Grade, selecione **Configuração Configurações do sistema servidor de gerenciamento de chaves**. 2. Confirme se as entradas da porta e do nome do host estão corretas. 3. Confirme se o certificado do servidor, o certificado do cliente e a chave privada do certificado do cliente estão corretos e não expiraram. 4. Certifique-se de que as definições da firewall permitem que o nó do dispositivo comunique com o KMS especificado. 5. Corrija quaisquer problemas de rede ou DNS. 6. Se precisar de assistência ou este alerta persistir, contacte o suporte técnico.
Nome da chave de encriptação KMS não encontrado	O servidor de gerenciamento de chaves configurado não possui uma chave de criptografia que corresponda ao nome fornecido. 1. Confirme se o KMS atribuído ao site está usando o nome correto para a chave de criptografia e quaisquer versões anteriores. 2. Se precisar de assistência ou este alerta persistir, contacte o suporte técnico.
Falha na rotação da chave de CRIPTOGRAFIA KMS	Todos os volumes de appliance foram descriptografados, mas um ou mais volumes não puderam girar para a chave mais recente.Contate o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
KMS não está configurado	Não existe nenhum servidor de gerenciamento de chaves para este site. 1. No Gerenciador de Grade, selecione **Configuração Configurações do sistema servidor de gerenciamento de chaves**. 2. Adicione um KMS para este site ou adicione um KMS padrão. "Administrar o StorageGRID"
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. 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Certifique-se de que o servidor de gerenciamento de chaves (KMS) tenha a chave de criptografia configurada e quaisquer versões anteriores de chaves. 3. Se precisar de assistência ou este alerta persistir, contacte o suporte técnico.
Expiração do certificado do servidor DE KMS	O certificado do servidor usado pelo KMS (Key Management Server) está prestes a expirar. 1. Usando o software KMS, atualize o certificado do servidor para o servidor de gerenciamento de chaves. 2. Se precisar de assistência ou este alerta persistir, contacte o suporte técnico. "Administrar o StorageGRID"

Nome do alerta	Descrição e ações recomendadas
Fila de auditoria grande	A fila de discos para mensagens de auditoria está cheia. 1. Verifique a carga no sistema - se houve um número significativo de transações, o alerta deve resolver-se ao longo do tempo, e você pode ignorar o alerta. 2. Se o alerta persistir e aumentar a gravidade, veja um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. 3. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para gravações do cliente e leituras do cliente para erro ou Desativado (**Configuração Monitoramento Auditoria**). "Rever registos de auditoria"
Baixa capacidade de disco de log de auditoria	O espaço disponível para logs de auditoria é baixo. 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.
Baixa memória disponível do nó	A quantidade de RAM disponível em um nó é baixa. A RAM baixa disponível pode indicar uma alteração na carga de trabalho ou um vazamento de memória com um ou mais nós. 1. Monitore esse alerta para ver se o problema resolve por conta própria. 2. Se a memória disponível descer abaixo do limite de alerta principal, contacte o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Baixo espaço livre para piscina de armazenamento	A quantidade de espaço disponível para armazenar dados de objetos em um pool de armazenamento é baixa. 1. Selecione **ILM** > **Storage Pools**. 2. Selecione o pool de armazenamento listado no alerta e selecione **Exibir detalhes**. 3. Determine onde a capacidade de armazenamento adicional é necessária. Você pode adicionar nós de storage a cada local no pool de storage ou adicionar volumes de storage (LUNs) a um ou mais nós de storage existentes. 4. Execute um procedimento de expansão para aumentar a capacidade de armazenamento. "Expanda sua grade"
Baixa memória do nó instalada	A quantidade de memória instalada em um nó é baixa. Aumente a quantidade de RAM disponível para a máquina virtual ou host Linux. Verifique o valor de limite do alerta principal para determinar o requisito mínimo padrão para um nó StorageGRID. Consulte as instruções de instalação da sua plataforma: • "Instale o Red Hat Enterprise Linux ou CentOS" • "Instale Ubuntu ou Debian" • "Instale o VMware"

Nome do alerta	Descrição e ações recomendadas
Baixo armazenamento de metadados	O espaço disponível para armazenar metadados de objetos é baixo.**Alerta crítico** 1. Pare de ingerir objetos. 2. Adicione imediatamente nós de storage em um procedimento de expansão. **Alerta principal** Adicione imediatamente nós de storage em um procedimento de expansão. **Menor alerta** 1. Monitore a taxa na qual o espaço de metadados de objetos está sendo usado. Selecione **nós *Storage Node* Storage** e veja o gráfico Storage Used - Object Metadata. 2. Adicione nós de storage em um procedimento de expansão o mais rápido possível. Depois que novos nós de storage são adicionados, o sistema reequilibra automaticamente os metadados de objetos em todos os nós de storage e o alarme é apagado. "Solução de problemas do alerta de armazenamento de metadados baixos" "Expanda sua grade"
Baixa capacidade de disco de métricas	O espaço disponível para o banco de dados de métricas é baixo. 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.
Baixo armazenamento de dados de objetos	O espaço disponível para armazenar dados de objetos é baixo.execute um procedimento de expansão. Você pode adicionar volumes de storage (LUNs) aos nós de storage existentes ou adicionar novos nós de storage. "Solução de problemas do alerta de armazenamento de dados de objetos baixos" "Expanda sua grade"

Nome do alerta	Descrição e ações recomendadas
Baixa capacidade de disco raiz	O espaço disponível para o disco raiz é baixo. 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.
Baixa capacidade de dados do sistema	O espaço disponível para os dados do sistema StorageGRID no sistema de arquivos /var/local é baixo. 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.
Erro de conetividade de rede do nó	Ocorreram erros durante a transferência de dados entre nodes.Network erros de conetividade podem ser apagados sem intervenção manual. Entre em Contato com o suporte técnico se os erros não forem claros. "Resolução de problemas do alarme Network Receive Error (NRER)"
Erro de quadro de receção de rede do nó	Uma alta porcentagem dos quadros de rede recebidos por um nó teve erros. Esse alerta pode indicar um problema de hardware, como um cabo com defeito ou um transcetor com falha em qualquer extremidade da conexão Ethernet. 1. Se você estiver usando um dispositivo, tente substituir cada transcetor SFP ou SFP28 e cabo, um de cada vez, para ver se o alerta é apagado. 2. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
Nó não sincronizado com o servidor NTP	A hora do nó não está sincronizada com o servidor NTP (Network Time Protocol). 1. Verifique se você especificou pelo menos quatro servidores NTP externos, cada um fornecendo uma referência estrato 3 ou melhor. 2. Verifique se todos os servidores NTP estão operando normalmente. 3. Verifique as conexões com os servidores NTP. Certifique-se de que eles não estão bloqueados por um firewall.
Nó não bloqueado com servidor NTP	O nó não está bloqueado para um servidor NTP (Network Time Protocol). 1. Verifique se você especificou pelo menos quatro servidores NTP externos, cada um fornecendo uma referência estrato 3 ou melhor. 2. Verifique se todos os servidores NTP estão operando normalmente. 3. Verifique as conexões com os servidores NTP. Certifique-se de que eles não estão bloqueados por um firewall.
Rede do nó que não é do dispositivo inativa	Um ou mais dispositivos de rede estão inativos ou desconetados. Este alerta indica que uma interface de rede (eth) para um nó instalado em uma máquina virtual ou host Linux não está acessível. Entre em Contato com o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Objetos perdidos	Um ou mais objetos foram perdidos da grade.este alerta pode indicar que os dados foram perdidos permanentemente e não podem ser recuperados. 1. Investigue este alerta imediatamente. Talvez seja necessário tomar medidas para evitar mais perda de dados. Você também pode restaurar um objeto perdido se você executar uma ação de prompt. "Solução de problemas de dados de objetos perdidos e ausentes" 2. Quando o problema subjacente for resolvido, reinicie o contador: a. Selecione **Support** > **Tools** > **Grid Topology**. b. Para o nó de armazenamento que levantou o alerta, selecione ***site grid node*** **LDR Data Store Configuration Main**. c. Selecione **Redefinir contagem de objetos perdidos** e clique em **aplicar alterações**.
Serviços de plataforma indisponíveis	Poucos nós de storage com o serviço RSM estão em execução ou disponíveis em um local.Certifique-se de que a maioria dos nós de storage que têm o serviço RSM no local afetado esteja em execução e em um estado não-erro. Consulte ""solução de problemas de serviços de plataforma" nas instruções para administrar o StorageGRID. "Administrar o StorageGRID"
Link do utilitário de serviços para baixo na porta de rede Admin 1	A porta Admin Network 1 do aparelho está inativa ou desconetada. 1. Verifique o cabo e a conexão física à porta Admin Network 1. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione **Alertas regras de alerta**, selecione a regra e clique em **Editar regra**. Em seguida, desmarque a caixa de seleção **Enabled**. ◦ "Aparelhos de serviços SG100 SG1000" ◦ "Desativar uma regra de alerta"

Nome do alerta	Descrição e ações recomendadas
Link do utilitário de serviços para baixo na rede de administração (ou rede de cliente)	A interface do dispositivo para a rede de administração (eth1) ou a rede de cliente (eth2) está inativa ou desligada. 1. Verifique os cabos, SFPs e conexões físicas à rede StorageGRID. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione **Alertas regras de alerta**, selecione a regra e clique em **Editar regra**. Em seguida, desmarque a caixa de seleção **Enabled**. ◦ "Aparelhos de serviços SG100 SG1000" ◦ "Desativar uma regra de alerta"
O utilitário de serviços está conetado na porta de rede 1, 2, 3 ou 4	A porta de rede 1, 2, 3 ou 4 do aparelho está inativa ou desligada. 1. Verifique os cabos, SFPs e conexões físicas à rede StorageGRID. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione **Alertas regras de alerta**, selecione a regra e clique em **Editar regra**. Em seguida, desmarque a caixa de seleção **Enabled**. ◦ "Aparelhos de serviços SG100 SG1000" ◦ "Desativar uma regra de alerta"

Nome do alerta	Descrição e ações recomendadas
Conectividade de storage do dispositivo de serviços degradada	Um dos dois SSDs em um dispositivo de serviços falhou ou está fora de sincronização com o outro. A funcionalidade do outro. Não é afetada, mas você deve resolver o problema imediatamente. Se ambas as unidades falharem, o aparelho deixará de funcionar. 1. No Gerenciador de Grade, selecione **nós *Services Appliance* e, em seguida, selecione a guia hardware**. 2. Reveja a mensagem no campo **Storage RAID Mode** (modo RAID de armazenamento*). 3. Se a mensagem mostrar o andamento de uma operação de ressincronização, aguarde a conclusão da operação e confirme se o alerta foi resolvido. Uma mensagem de ressincronização significa que o SSD foi substituído recentemente ou que está sendo ressincronizado por outro motivo. 4. Se a mensagem indicar que um dos SSDs falhou, substitua a unidade com falha o mais rápido possível. Para obter instruções sobre como substituir uma unidade em um dispositivo de serviços, consulte o guia de instalação e manutenção dos aparelhos SG100 e SG1000. "Aparelhos de serviços SG100 SG1000"
Link do dispositivo de armazenamento na porta Admin Network 1	A porta Admin Network 1 do aparelho está inativa ou desconetada. 1. Verifique o cabo e a conexão física à porta Admin Network 1. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione **Alertas regras de alerta**, selecione a regra e clique em **Editar regra**. Em seguida, desmarque a caixa de seleção **Enabled**. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Desativar uma regra de alerta"

Nome do alerta	Descrição e ações recomendadas
Link do dispositivo de armazenamento na rede Admin (ou rede do cliente)	A interface do dispositivo para a rede de administração (eth1) ou a rede de cliente (eth2) está inativa ou desligada. 1. Verifique os cabos, SFPs e conexões físicas à rede StorageGRID. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione **Alertas regras de alerta**, selecione a regra e clique em **Editar regra**. Em seguida, desmarque a caixa de seleção **Enabled**. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Desativar uma regra de alerta"
Ligação do dispositivo de armazenamento na porta de rede 1, 2, 3 ou 4	A porta de rede 1, 2, 3 ou 4 do aparelho está inativa ou desligada. 1. Verifique os cabos, SFPs e conexões físicas à rede StorageGRID. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione **Alertas regras de alerta**, selecione a regra e clique em **Editar regra**. Em seguida, desmarque a caixa de seleção **Enabled**. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento" ◦ "Desativar uma regra de alerta"

Nome do alerta	Descrição e ações recomendadas
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. 1. Vá ao aparelho para verificar as luzes indicadoras da porta. 2. Se as luzes de uma porta estiverem apagadas, confirme se o cabo está conetado corretamente. Conforme necessário, substitua o cabo. 3. Aguarde até cinco minutos. Se for necessário substituir um segundo cabo, não o desligue durante, pelo menos, 5 minutos. Caso contrário, o volume raiz pode se tornar somente leitura, o que requer uma reinicialização de hardware. 4. No Gerenciador de Grade, selecione **nós**. Em seguida, selecione a guia hardware do nó que teve o problema. Verifique se a condição de alerta foi resolvida.

Nome do alerta	Descrição e ações recomendadas
Dispositivo de armazenamento inacessível	Não é possível aceder a um dispositivo de armazenamento. Este alerta indica que não é possível montar ou aceder a um volume devido a um problema com um dispositivo de armazenamento subjacente. 1. Verifique o status de todos os dispositivos de armazenamento usados para o nó: ◦ Se o nó estiver instalado em uma máquina virtual ou em um host Linux, siga as instruções para que seu sistema operacional execute diagnósticos de hardware ou execute uma verificação do sistema de arquivos. ▪ "Instale o Red Hat Enterprise Linux ou CentOS" ▪ "Instale Ubuntu ou Debian" ▪ "Instale o VMware" ◦ Se o nó estiver instalado em um dispositivo SG100, SG1000 ou SG6000, use o BMC. ◦ Se o nó estiver instalado em um dispositivo SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. ◦ "SG6000 dispositivos de armazenamento" ◦ "SG5700 dispositivos de armazenamento" ◦ "SG5600 dispositivos de armazenamento"

Nome do alerta	Descrição e ações recomendadas
Uso de cota de locatário alto	Uma alta porcentagem de espaço de cota de locatário está sendo usada. Se um inquilino exceder sua cota, novos ingerências são rejeitados. Esta regra de alerta é desativada por padrão porque pode gerar muitas notificações. 1. No Gerenciador de Grade, selecione **tenants**. 2. Classifique a tabela por **quota de utilização**. 3. Selecione um locatário cuja utilização da cota seja próxima de 100%. 4. Faça um ou ambos os procedimentos a seguir: ◦ Selecione **Editar** para aumentar a cota de armazenamento do locatário. ◦ Notificar o locatário de que a utilização da cota é alta.

Nome do alerta	Descrição e ações recomendadas
Não é possível comunicar com o nó	Um ou mais serviços não respondem, ou o nó não pode ser alcançado. Este alerta indica que um nó está desconetado por um motivo desconhecido. Por exemplo, um serviço no nó pode ser interrompido ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada. Monitore esse alerta para ver se o problema resolve por conta própria. Se o problema persistir: 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Confirme se todos os serviços neste nó estão em execução. Se um serviço for interrompido, tente iniciá-lo. Consulte as instruções de recuperação e manutenção. 3. Certifique-se de que o host do nó esteja ligado. Se não estiver, inicie o host. Se mais de um host for desligado, consulte as instruções de recuperação e manutenção. 4. Determine se há um problema de conetividade de rede entre este nó e o nó Admin. 5. Se não conseguir resolver o alerta, contacte o suporte técnico. "Manter recuperar"
Reinicialização inesperada do nó	Um nó reinicializou inesperadamente nas últimas 24 horas. 1. Monitorize este alerta. O alerta será apagado após 24 horas. No entanto, se o nó reiniciar inesperadamente novamente, este alerta será acionado novamente. 2. Se você não conseguir resolver o alerta, pode haver uma falha de hardware. Entre em Contato com o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Objeto corrompido não identificado detetado	Um arquivo foi encontrado no storage de objetos replicado que não pôde ser identificado como um objeto replicado. 1. Determine se há algum problema com o storage subjacente em um nó de storage. Por exemplo, execute diagnósticos de hardware ou execute uma verificação do sistema de arquivos. 2. Depois de resolver quaisquer problemas de armazenamento, execute a verificação de primeiro plano para determinar se os objetos estão em falta e substituí-los, se possível. 3. Monitorize este alerta. O alerta será apagado após 24 horas, mas será acionado novamente se o problema não tiver sido corrigido. 4. Se não conseguir resolver o alerta, contacte o suporte técnico. "A executar a verificação de primeiro plano"

Informações relacionadas

"Métricas de Prometheus comumente usadas"

Métricas de Prometheus comumente usadas

O serviço Prometheus nos Admin Nodes coleta métricas de séries temporais dos serviços em todos os nós. Enquanto Prometheus coleta mais de mil métricas, um número relativamente pequeno é necessário para monitorar as operações mais críticas do StorageGRID.

A tabela a seguir lista as métricas de Prometheus mais usadas e fornece um mapeamento de cada métrica para o atributo equivalente (usado no sistema de alarme).

Você pode consultar esta lista para entender melhor as condições nas regras de alerta padrão ou para construir as condições para regras de alerta personalizadas. Para obter uma lista completa de métricas, selecione **Ajuda Documentação da API**.

> 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.

> As métricas do Prometheus são mantidas por 31 dias.

Métrica Prometheus	Descrição
alertmanager_notifications_failed_total	O número total de notificações de alerta com falha.

Métrica Prometheus	Descrição
node_filesystem_avail_bytes	A quantidade de espaço de sistema de arquivos disponível para usuários não-root em bytes.
Node_Memory_MemAvailable_bytes	Campo de informações de memória MemAvailable_bytes.
node_network_carrier	Valor do transportador de /sys/class/net/iface.
node_network_receive_errs_total	Estatísticas do dispositivo de rede Receive_errs.
node_network_transmit_errs_total	Estatísticas do dispositivo de rede transmit_errs.
StorageGRID_administrativamente_down	O nó não está conetado à grade por um motivo esperado. Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado.
StorageGRID_appliance_compute_controller_hardware_status	O status do hardware do controlador de computação em um dispositivo.
StorageGRID_appliance_failed_disks	Para o controlador de armazenamento em um dispositivo, o número de unidades que não são ideais.
StorageGRID_appliance_storage_controller_hardware_status	O status geral do hardware do controlador de storage em um dispositivo.
StorageGRID_content_buckets_and_containers	O número total de buckets S3 e contentores Swift conhecidos por este nó de armazenamento.
StorageGRID_content_objects	O número total de objetos de dados S3 e Swift conhecido por este nó de storage. A contagem é válida apenas para objetos de dados criados por aplicativos clientes que fazem interface com o sistema através de S3 ou Swift.
StorageGRID_content_objects_lost	O número total de objetos que este serviço deteta como ausentes no sistema StorageGRID. Devem ser tomadas medidas para determinar a causa da perda e se a recuperação é possível. "Solução de 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.

Métrica Prometheus	Descrição
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.

Métrica Prometheus	Descrição
StorageGRID_ntp_chosen_time_source_offset_milliseconds	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_load	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_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.

Métrica Prometheus	Descrição
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_metadata_bytes	Uma estimativa do tamanho total dos dados de objetos codificados de apagamento e replicados 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.

Métrica Prometheus	Descrição
StorageGRID_storage_utilization_metadata_bytes	A quantidade de metadados de objetos no volume de armazenamento 0, em bytes.
StorageGRID_storage_utilization_metadata_reserved_bytes	O espaço total no volume 0 de cada nó de storage que é realmente reservado para metadados de objetos. Para qualquer nó de armazenamento, o espaço reservado real para metadados depende do tamanho do volume 0 para o nó e da configuração espaço reservado para metadados em todo o sistema.
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.

Referência de alarmes (sistema legado)

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

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

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

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

Código	Nome	Serviço	Ação recomendada
ADCE	Estado ADC	ADC	Se o valor do Estado ADC for Standby, continue monitorando o serviço e, se o problema persistir, entre em Contato com o suporte técnico. Se o valor de ADC State for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
AITE	Recuperar Estado	BARC	Disponível apenas para nós de arquivo com um tipo de destino do Tivoli Storage Manager (TSM). Se o valor de Retrieve State estiver aguardando o Target, verifique o servidor de middleware TSM e certifique-se de que ele está funcionando corretamente. Se o nó de arquivo tiver sido adicionado ao sistema StorageGRID, certifique-se de que a ligação do nó de arquivo ao sistema de armazenamento de arquivos externo visado está configurada corretamente. Se o valor do Estado de recuperação de Arquivo for Offline, tente atualizar o estado para Online. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **ARC Retrieve Configuration Main**, selecione **Archive Retrieve State Online** e clique em **Apply Changes**. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
AITU	Recuperar Estado	BARC	Se o valor de Retrieve Status for Target Error, verifique se há erros no sistema de armazenamento de arquivos externo de destino. Se o valor de Archive Retrieve Status (Estado de recuperação de arquivo) for Session Lost (perda de sessão), verifique o sistema de armazenamento de arquivo externo alvo para garantir que está online e a funcionar corretamente. Verifique a conexão de rede com o destino. Se o valor do Estado de recuperação de Arquivo for erro desconhecido, contacte o suporte técnico.
ALIS	Sessões Atributo inbound	ADC	Se o número de sessões de atributo de entrada em um relay de atributo crescer muito grande, pode ser uma indicação de que o sistema StorageGRID ficou desequilibrado. Em condições normais, as sessões de atributos devem ser distribuídas uniformemente entre os serviços ADC. Um desequilíbrio pode levar a problemas de desempenho. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
ALOS	Sessões de Atributo de saída	ADC	O serviço ADC tem um alto número de sessões de atributos e está se tornando sobrecarregado. Se este alarme for acionado, contacte a assistência técnica.
ALUR	Repositórios Atributo inalcançáveis	ADC	Verifique a conetividade de rede com o serviço NMS para garantir que o serviço possa entrar em Contato com o repositório de atributos. Se este alarme for acionado e a conetividade de rede estiver boa, contacte o suporte técnico.

Código	Nome	Serviço	Ação recomendada
AMQS	Mensagens de auditoria enfileiradas	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Se as mensagens de auditoria não puderem ser encaminhadas imediatamente para um reencaminhamento ou repositório de auditoria, as mensagens serão armazenadas em uma fila de discos. Se a fila de discos ficar cheia, podem ocorrer interrupções. Para permitir que você responda a tempo para evitar uma interrupção, os alarmes AMQS são acionados quando o número de mensagens na fila de discos atinge os seguintes limites: • Aviso: Mais de 100.000 mensagens • Menor: Pelo menos 500.000 mensagens • Maior: Pelo menos 2.000.000 mensagens • Crítico: Pelo menos 5.000.000 mensagens Se um alarme AMQS for acionado, verifique a carga no sistema - se houver um número significativo de transações, o alarme deve resolver-se ao longo do tempo. Neste caso, pode ignorar o alarme. Se o alarme persistir e aumentar a gravidade, visualize um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de

Código	Nome	Serviço	Ação recomendada
AOTE	Estado da loja	BARC	Disponível apenas para nós de arquivo com um tipo de destino do Tivoli Storage Manager (TSM). Se o valor do Estado de armazenamento estiver a aguardar o destino, verifique o sistema de armazenamento de arquivos externo e certifique-se de que está a funcionar corretamente. Se o nó de arquivo tiver sido adicionado ao sistema StorageGRID, certifique-se de que a ligação do nó de arquivo ao sistema de armazenamento de arquivos externo visado está configurada corretamente. Se o valor de Estado da loja estiver offline, verifique o valor de Estado da loja. Corrija quaisquer problemas antes de mover o estado da loja de volta para Online.
AOTU	Estado da loja	BARC	Se o valor de Status da Loja for sessão perdida, verifique se o sistema de armazenamento de arquivos externo está conetado e on-line. Se o valor de Target Error (erro de destino), verifique se há erros no sistema de armazenamento de arquivos externo. Se o valor do Status da Loja for erro desconhecido, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
APMS	Conetividade Multipath de armazenamento	SSM	Se o alarme de estado multipath aparecer como ""degradado""" (selecione **suporte Ferramentas topologia de grade**, selecione ***site grid node*** **SSM Eventos**), faça o seguinte: 1. Conete ou substitua o cabo que não exibe nenhuma luz indicadora. 2. Aguarde de um a cinco minutos. Não desligue o outro cabo até, pelo menos, cinco minutos depois de ligar o primeiro. Desconetar muito cedo pode fazer com que o volume raiz se torne somente leitura, o que requer que o hardware seja reiniciado. 3. Retorne à página **SSM Resources** e verifique se o status do Multipath ""degradado"" mudou para ""nominal"" na seção hardware de armazenamento.

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

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

Código	Nome	Serviço	Ação recomendada
ARRV	Falhas de verificação	ARCO	Para diagnosticar e corrigir esse problema, entre em Contato com o suporte técnico. Assim que o problema que acionou este alarme for resolvido, reponha a contagem de avarias. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **ARC Retrieve Configuration Main**, selecione **Reset Verification Failure Count** e clique em **Apply Changes**.
ARVF	Falhas de armazenamento	ARCO	Este alarme pode ocorrer como resultado de erros com o sistema de armazenamento de arquivos externo visado. Verifique se há erros no sistema de armazenamento de arquivos externo e verifique se ele está funcionando corretamente. Assim que o problema que acionou este alarme for resolvido, reponha a contagem de avarias. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **ARC Retrieve Configuration Main**, selecione **Reset Store Failure Count** e clique em **Apply Changes**.

Código	Nome	Serviço	Ação recomendada
ASXP	Compartilhamentos de auditoria	AMS	Um alarme é acionado se o valor de compartilhamentos de auditoria for desconhecido. Este alarme pode indicar um problema com a instalação ou configuração do nó Admin. Se o problema persistir, entre em Contato com o suporte técnico.
AUMA	Estado AMS	AMS	Se o valor do Status AMS for DB Connectivity Error (erro de conetividade de banco de dados), reinicie o nó da grade. Se o problema persistir, entre em Contato com o suporte técnico.
AUME	Estado AMS	AMS	Se o valor do estado AMS for em espera, continue a monitorizar o sistema StorageGRID. Se o problema persistir, entre em Contato com o suporte técnico. Se o valor do Estado AMS for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
AUXS	Estado exportação Auditoria	AMS	Se um alarme for acionado, corrija o problema subjacente e reinicie o serviço AMS. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
BADD	Falha na contagem de unidades do controlador de armazenamento	SSM	Este alarme é acionado quando uma ou mais unidades de um dispositivo StorageGRID falharam ou não são ideais. Substitua as unidades conforme necessário.
BASF	Identificadores de Objeto disponíveis	CMN	Quando um sistema StorageGRID é provisionado, o serviço CMN recebe um número fixo de identificadores de objeto. Este alarme é acionado quando o sistema StorageGRID começa a esgotar o seu fornecimento de identificadores de objetos. Para alocar mais identificadores, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
GRAVES	Estado Alocação bloco Identificador	CMN	Por padrão, um alarme é acionado quando os identificadores de objeto não podem ser alocados porque o quórum de ADC não pode ser alcançado. A alocação de bloco de identificador no serviço CMN requer um quorum (50% mais 1) dos serviços ADC para estar on-line e conetado. Se o quórum não estiver disponível, o serviço CMN não poderá alocar novos blocos de identificador até que o quórum de ADC seja restabelecido. Se o quórum de ADC for perdido, geralmente não há impactos imediato no sistema StorageGRID (os clientes ainda podem ingerir e recuperar conteúdo), já que aproximadamente um mês de fornecimento de identificadores são armazenados em cache em outro lugar na grade; no entanto, se a condição continuar, o sistema StorageGRID perderá a capacidade de ingerir novo conteúdo. Se um alarme for acionado, investigue o motivo da perda do quórum de ADC (por exemplo, pode ser uma falha de rede ou nó de armazenamento) e tome medidas corretivas. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
BRDT	Temperatura do chassi do controlador de computação	SSM	Um alarme é acionado se a temperatura do controlador de computação em um dispositivo StorageGRID exceder um limite nominal. Verifique os componentes do hardware e problemas ambientais quanto a condições de sobreaquecimento. Se necessário, substituir o órgão.
BTOF	Desvio	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Um alarme é acionado se o tempo de serviço (segundos) diferir significativamente do tempo do sistema operacional. Em condições normais, o serviço deve ressincronizar-se. Se o tempo de serviço se afastar demasiado do tempo do sistema operativo, as operações do sistema podem ser afetadas. Confirme se a fonte de hora do sistema StorageGRID está correta. Se o problema persistir, entre em Contato com o suporte técnico.

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

Código	Nome	Serviço	Ação recomendada
CAQH	Número de destinos disponíveis	CLB	Este alarme é apagado quando os problemas subjacentes dos serviços LDR disponíveis são corrigidos. Certifique-se de que o componente HTTP dos serviços LDR esteja online e funcionando normalmente. Se o problema persistir, entre em Contato com o suporte técnico.

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

Código	Nome	Serviço	Ação recomendada
CCES	Sessões recebidas - estabelecidas	CLB	Este alarme é acionado se houver 20.000 ou mais sessões HTTP atualmente ativas (abertas) no Gateway Node. Se um cliente tiver muitas conexões, você poderá ver falhas de conexão. Você deve reduzir o workload.
CCNA	Hardware de computação	SSM	Esse alarme é acionado se o status do hardware do controlador de computação em um dispositivo StorageGRID precisar de atenção.

Código	Nome	Serviço	Ação recomendada
CDLP	Espaço usado (porcentagem)	DDS	Este alarme é acionado quando o espaço efetivo de metadados (CEMS) atinge 70% cheio (alarme menor), 90% cheio (alarme principal) e 100% cheio (alarme crítico). Se esse alarme atingir o limite de 90%, um aviso será exibido no Painel no Gerenciador de Grade. Você deve executar um procedimento de expansão para adicionar novos nós de storage o mais rápido possível. Consulte as instruções para expandir uma grade StorageGRID. Se esse alarme atingir o limite de 100%, você deve parar de ingerir objetos e adicionar nós de storage imediatamente. O Cassandra requer uma certa quantidade de espaço para realizar operações essenciais, como compactação e reparo. Essas operações serão impactadas se os metadados de objetos usarem mais de 100% do espaço permitido. Resultados indesejáveis podem ocorrer. **Nota**: Entre em Contato com o suporte técnico se você não conseguir adicionar nós de storage. Depois que novos nós de storage são adicionados, o sistema reequilibra automaticamente os metadados de objetos em todos os nós de storage e o alarme é apagado. "Solução de problemas do alerta de armazenamento de metadados baixos" "Expanda sua grade"

Código	Nome	Serviço	Ação recomendada
CLBA	Estado CLB	CLB	Se um alarme for acionado, selecione **Support Tools Grid Topology**, em seguida selecione ***site grid node*** **CLB Overview Main** e **CLB Alarmes Main** para determinar a causa do alarme e solucionar o problema. Se o problema persistir, entre em Contato com o suporte técnico.
CLBE	Estado CLB	CLB	Se o valor do Estado CLB for Standby (em espera), continue a monitorizar a situação e, se o problema persistir, contacte o suporte técnico. Se o estado estiver Offline e não houver problemas conhecidos de hardware do servidor (por exemplo, o servidor está desconetado) ou tempo de inatividade programado, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
CMNA	Estado CMN	CMN	Se o valor do Status do CMN for erro, selecione **suporte Ferramentas topologia de grade** e, em seguida, selecione ***site grid node* CMN Visão geral Principal** e **CMN Alarmes Main** para determinar a causa do erro e solucionar o problema. Um alarme é acionado e o valor de Status do CMN é no Online CMN durante uma atualização de hardware do nó Admin primário quando as CMNs são comutadas (o valor do estado antigo do CMN é Standby e o novo é Online). Se o problema persistir, entre em Contato com o suporte técnico.
CPRC	Capacidade restante	NMS	Um alarme é acionado se a capacidade restante (número de conexões disponíveis que podem ser abertas para o banco de dados NMS) ficar abaixo da gravidade do alarme configurada. Se um alarme for acionado, contacte a assistência técnica.
CPSA	Fonte de Alimentação A do controlador de computação	SSM	Um alarme é acionado se houver um problema com a fonte de Alimentação A no controlador de computação para um dispositivo StorageGRID. Se necessário, substituir o órgão.

Código	Nome	Serviço	Ação recomendada
CPSB	Fonte de alimentação B do controlador de computação	SSM	Um alarme é acionado se houver um problema com a fonte de alimentação B no controlador de computação para um dispositivo StorageGRID. Se necessário, substituir o órgão.
CPUT	Temperatura da CPU do controlador de computação	SSM	Um alarme é acionado se a temperatura da CPU no controlador de computação em um dispositivo StorageGRID exceder um limite nominal. Se o nó de armazenamento for um dispositivo StorageGRID, o sistema StorageGRID indica que o controlador precisa de atenção. Verifique os componentes de hardware e problemas de ambiente quanto a condições de sobreaquecimento. Se necessário, substituir o órgão.
DNST	Estado DNS	SSM	Após a conclusão da instalação, um alarme DNST é acionado no serviço SSM. Depois que o DNS é configurado e as novas informações do servidor atingem todos os nós da grade, o alarme é cancelado.

Código	Nome	Serviço	Ação recomendada
ECCD	Fragmentos corrompidos detetados	LDR	Um alarme é acionado quando o processo de verificação em segundo plano deteta um fragmento codificado de apagamento corrompido. Se um fragmento corrompido for detetado, uma tentativa é feita para reconstruir o fragmento. Redefina os fragmentos corrompidos detetados e copie os atributos perdidos para zero e monitorize-os para ver se as contagens aumentam novamente. Se as contagens aumentarem, pode haver um problema com o armazenamento subjacente do nó de armazenamento. Uma cópia de dados de objeto codificado de apagamento não é considerada ausente até que o número de fragmentos perdidos ou corrompidos viole a tolerância de falhas do código de apagamento; portanto, é possível ter fragmento corrompido e ainda ser capaz de recuperar o objeto. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
ECST	Estado de verificação	LDR	Este alarme indica o estado atual do processo de verificação em segundo plano para apagar dados de objetos codificados neste nó de armazenamento. Um alarme principal é acionado se houver um erro no processo de verificação em segundo plano.
FOPN	Abra descritores de arquivo	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	FOPN pode tornar-se grande durante a atividade de pico. Se não diminuir durante períodos de atividade lenta, entre em Contato com o suporte técnico.
HSTE	Estado HTTP	ERRO	Consulte ações recomendadas para HSTU.

Código	Nome	Serviço	Ação recomendada
HSTU	Estado HTTP	ERRO	HSTE e HSTU estão relacionados ao protocolo HTTP para todo o tráfego LDR, incluindo S3, Swift e outro tráfego interno de StorageGRID. Um alarme indica que ocorreu uma das seguintes situações: • O protocolo HTTP foi colocado offline manualmente. • O atributo Auto-Start HTTP foi desativado. • O serviço LDR está a encerrar. O atributo Auto-Start HTTP é ativado por padrão. Se essa configuração for alterada, o HTTP poderá permanecer offline após uma reinicialização. Se necessário, aguarde que o serviço LDR seja reiniciado. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***Storage Node* LDR Configuration**. Se o protocolo HTTP estiver offline, coloque-o online. Verifique se o atributo Auto-Start HTTP está ativado. Se o protocolo HTTP permanecer off-line, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
HTAS	Auto-Iniciar HTTP	LDR	Especifica se os serviços HTTP devem ser iniciados automaticamente na inicialização. Esta é uma opção de configuração especificada pelo usuário.
IRSU	Estado de replicação de entrada	BLDR, BARC	Um alarme indica que a replicação de entrada foi desativada. Confirmar configurações: Selecione **suporte Ferramentas topologia de grade**. Em seguida, selecione ***site grid node*** **LDR Replication Configuration Main**.
LATA	Latência média	NMS	Verifique se há problemas de conetividade. Verifique a atividade do sistema para confirmar que existe um aumento na atividade do sistema. Um aumento na atividade do sistema resultará em um aumento para atribuir a atividade de dados. Essa atividade aumentada resultará em um atraso no processamento de dados de atributos. Esta pode ser uma atividade normal do sistema e irá diminuir. Verifique se existem vários alarmes. Um aumento nos tempos médios de latência pode ser indicado por um número excessivo de alarmes acionados. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
LDRE	Estado LDR	LDR	Se o valor do Estado LDR for Standby (em espera), continue a monitorizar a situação e, se o problema persistir, contacte o suporte técnico. Se o valor de LDR State for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
PERDIDO	Objetos perdidos	DDS, LDR	Acionado quando o sistema StorageGRID não consegue recuperar uma cópia do objeto solicitado de qualquer lugar do sistema. Antes de um alarme PERDIDO (objetos perdidos) ser acionado, o sistema tenta recuperar e substituir um objeto em falta de outro local do sistema. Objetos perdidos representam uma perda de dados. O atributo objetos perdidos é incrementado sempre que o número de locais para um objeto cai para zero sem o serviço DDS propositadamente purgando o conteúdo para satisfazer a política ILM. Investigue imediatamente os alarmes PERDIDOS (LOST Object). Se o problema persistir, entre em Contato com o suporte técnico. "Solução de problemas de dados de objetos perdidos e ausentes"

Código	Nome	Serviço	Ação recomendada
MCEP	Validade do certificado de Interface de Gestão	CMN	Acionado quando o certificado usado para acessar a interface de gerenciamento está prestes a expirar. 1. Vá para **Configuração certificados de servidor**. 2. Na seção certificado do servidor de interface de gerenciamento, carregue um novo certificado. "Administrar o StorageGRID"
MINQ	Notificações de e-mail na fila	NMS	Verifique as conexões de rede dos servidores que hospedam o serviço NMS e o servidor de e-mail externo. Confirme também se a configuração do servidor de e-mail está correta. "Configuração das configurações do servidor de e-mail para alarmes (sistema legado)"

Código	Nome	Serviço	Ação recomendada
MIN	Estado das notificações por e-mail	BNMS	Um alarme menor é acionado se o serviço NMS não conseguir se conetar ao servidor de e-mail. Verifique as conexões de rede dos servidores que hospedam o serviço NMS e o servidor de e-mail externo. Confirme também se a configuração do servidor de e-mail está correta. "Configuração das configurações do servidor de e-mail para alarmes (sistema legado)"
SAUDADES	Estado do motor da interface NMS	BNMS	Um alarme é acionado se o mecanismo de interface NMS no Admin Node que reúne e gera conteúdo da interface for desconetado do sistema. Verifique o Gerenciador do servidor para determinar se o aplicativo individual do servidor está inativo.
NANG	Configuração de negociação automática de rede	SSM	Verifique a configuração do adaptador de rede. A configuração deve corresponder às preferências dos roteadores e switches de rede. Uma definição incorreta pode ter um impactos grave no desempenho do sistema.

Código	Nome	Serviço	Ação recomendada
NDUP	Configuração Duplex de rede	SSM	Verifique a configuração do adaptador de rede. A configuração deve corresponder às preferências dos roteadores e switches de rede. Uma definição incorreta pode ter um impactos grave no desempenho do sistema.
NLNK	Detecção de ligação de rede	SSM	Verifique as conexões do cabo de rede na porta e no switch. Verifique as configurações do roteador, do switch e do adaptador de rede. Reinicie o servidor. Se o problema persistir, entre em Contato com o suporte técnico.
NRER	Receber erros	SSM	As seguintes causas podem ser os alarmes NRER: • Correção de erro de avanço (FEC) não corresponde • Incompatibilidade da MTU da porta do switch e da NIC • Altas taxas de erro de link • Buffer de anel NIC excedido "Resolução de problemas do alarme Network Receive Error (NRER)"

Código	Nome	Serviço	Ação recomendada
NRLY	Relés de auditoria disponíveis	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Se os relés de auditoria não estiverem conetados aos serviços ADC, os eventos de auditoria não poderão ser relatados. Eles estão em fila de espera e indisponíveis para os usuários até que a conexão seja restaurada. Restaure a conetividade a um serviço ADC o mais rápido possível. Se o problema persistir, entre em Contato com o suporte técnico.
NSCA	Estado NMS	NMS	Se o valor de Status do NMS for DB Connectivity Error (erro de conetividade de banco de dados), reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
NSCE	Estado NMS	NMS	Se o valor do estado NMS for Standby (espera), continue a monitorização e, se o problema persistir, contacte o suporte técnico. Se o valor de Estado NMS for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
VELOCIDADE MÁXIMA	Velocidade	SSM	Isso pode ser causado por problemas de conetividade de rede ou compatibilidade de driver. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
NTBR	Livre Tablespace	NMS	Se um alarme for acionado, verifique a rapidez com que a utilização da base de dados foi alterada. Uma queda súbita (ao contrário de uma mudança gradual ao longo do tempo) indica uma condição de erro. Se o problema persistir, entre em Contato com o suporte técnico. Ajustar o limite de alarme permite que você gerencie proativamente quando o armazenamento adicional precisa ser alocado. Se o espaço disponível atingir um limite baixo (consulte o limiar de alarme), contacte o suporte técnico para alterar a alocação da base de dados.

Código	Nome	Serviço	Ação recomendada
NTER	Transmitir erros	SSM	Esses erros podem ser apagados sem serem reiniciados manualmente. Se eles não limparem, verifique o hardware de rede. Verifique se o hardware e o driver do adaptador estão corretamente instalados e configurados para funcionar com seus roteadores e switches de rede. Quando o problema subjacente for resolvido, reinicie o contador. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **SSM Resources Configuration Main**, selecione **Reset Transmit Error Count** e clique em **Apply Changes**.
NTFQ	Desvio de frequência NTP	SSM	Se o desvio de frequência exceder o limite configurado, é provável que haja um problema de hardware com o relógio local. Se o problema persistir, contacte o suporte técnico para agendar uma substituição.
NTLK	Bloqueio NTP	SSM	Se o daemon NTP não estiver bloqueado para uma fonte de tempo externa, verifique a conetividade de rede com as fontes de tempo externas designadas, sua disponibilidade e sua estabilidade.

Código	Nome	Serviço	Ação recomendada
NTOF	Desvio horário NTP	SSM	Se o desvio de tempo exceder o limite configurado, é provável que haja um problema de hardware com o oscilador do relógio local. Se o problema persistir, contacte o suporte técnico para agendar uma substituição.
NTSJ	Jitter de fonte de tempo escolhido	SSM	Este valor indica a confiabilidade e estabilidade da fonte de tempo que o NTP no servidor local está usando como referência. Se um alarme for acionado, pode ser uma indicação de que o oscilador da fonte de tempo está com defeito ou que há um problema com o link WAN para a fonte de tempo.
NTSU	Estado NTP	SSM	Se o valor do Status NTP não estiver em execução, entre em Contato com o suporte técnico.
OPST	Estado geral da alimentação	SSM	Um alarme é acionado se a alimentação de um aparelho StorageGRID se desviar da tensão de funcionamento recomendada. Verifique o estado da fonte de Alimentação A ou B para determinar qual fonte de alimentação está a funcionar de forma anormal. Se necessário, substitua a fonte de alimentação.

Código	Nome	Serviço	Ação recomendada
OQRT	Objetos em quarentena	LDR	Depois que os objetos são restaurados automaticamente pelo sistema StorageGRID, os objetos em quarentena podem ser removidos do diretório de quarentena. 1. Selecione **Support** > **Tools** > **Grid Topology**. 2. Selecione **site nó de armazenamento LDR Verificação Configuração Principal**. 3. Selecione **Excluir objetos em quarentena**. 4. Clique em **aplicar alterações**. Os objetos em quarentena são removidos e a contagem é redefinida para zero.

Código	Nome	Serviço	Ação recomendada
ORSU	Estado replicação saída	BLDR, BARC	Um alarme indica que a replicação de saída não é possível: O armazenamento está em um estado em que os objetos não podem ser recuperados. Um alarme é acionado se a replicação de saída for desativada manualmente. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **LDR Replication Configuration**. Um alarme é acionado se o serviço LDR não estiver disponível para replicação. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **LDR Storage**.
OSLF	Status do compartimento	SSM	Um alarme é acionado se o status de um dos componentes na prateleira de armazenamento de um dispositivo de armazenamento for degradado. Os componentes da prateleira de armazenamento incluem IOMs, ventiladores, fontes de alimentação e gavetas de unidade.se este alarme for acionado, consulte as instruções de manutenção do seu aparelho.

Código	Nome	Serviço	Ação recomendada
PMEM	Utilização da memória de serviço (percentagem)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Pode ter um valor de mais de Y% de RAM, onde Y representa a porcentagem de memória que está sendo usada pelo servidor. Valores abaixo de 80% são normais. Mais de 90% é considerado um problema. Se o uso de memória for alto para um único serviço, monitore a situação e investigue. Se o problema persistir, entre em Contato com o suporte técnico.
PSAS	Estado da fonte de alimentação A.	SSM	Um alarme é acionado se a fonte de Alimentação A num aparelho StorageGRID se desviar da tensão de funcionamento recomendada. Se necessário, substitua a fonte de alimentação A.
PSB	Estado da fonte de alimentação B.	SSM	Um alarme é acionado se a fonte de alimentação B num aparelho StorageGRID se desviar da tensão de funcionamento recomendada. Se necessário, substitua a fonte de alimentação B..

Código	Nome	Serviço	Ação recomendada
RDTE	Estado do Tivoli Storage Manager	BARC	Disponível apenas para nós de arquivamento com um tipo de destino do Tivoli Storage Manager (TSM). Se o valor do estado do Tivoli Storage Manager estiver offline, verifique o status do Tivoli Storage Manager e resolva quaisquer problemas. Coloque o componente novamente online. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node* ARC Target Configuration Main**, selecione **Tivoli Storage Manager State Online** e clique em **Apply Changes**.

Código	Nome	Serviço	Ação recomendada
RDTU	Status do Tivoli Storage Manager	BARC	Disponível apenas para nós de arquivamento com um tipo de destino do Tivoli Storage Manager (TSM). Se o valor do status do Gerenciador de armazenamento Tivoli for erro de configuração e o nó de arquivo tiver sido adicionado ao sistema StorageGRID, verifique se o servidor de middleware TSM está configurado corretamente. Se o valor do status do Gerenciador de armazenamento Tivoli for falha de conexão ou falha de conexão, tente novamente, verifique a configuração de rede no servidor middleware TSM e a conexão de rede entre o servidor de middleware TSM e o sistema StorageGRID. Se o valor do status do Gerenciador de armazenamento Tivoli for Falha de autenticação ou Falha de autenticação, reconetando, o sistema StorageGRID poderá se conetar ao servidor middleware TSM, mas não poderá autenticar a conexão. Verifique se o servidor de middleware TSM está configurado com o usuário, senha e permissões corretos e reinicie o serviço. Se o valor do status do Tivoli Storage Manager for Falha da sessão, uma sessão estabelecida foi perdida inesperadamente. Verifique a conexão de rede entre o servidor middleware TSM e o sistema StorageGRID. Verifique se há erros no

Código	Nome	Serviço	Ação recomendada
RIRF	Replicações de entrada — falhou	BLDR, BARC	Um alarme Inbound replicações — Falha pode ocorrer durante períodos de alta carga ou interrupções temporárias da rede. Após a redução da atividade do sistema, este alarme deve ser apagado. Se a contagem de replicações falhadas continuar a aumentar, procure problemas de rede e verifique se os serviços LDR e ARC de origem e destino estão online e disponíveis. Para redefinir a contagem, selecione **Support Tools Grid Topology** e, em seguida, selecione ***site grid node*** **LDR Replication Configuration Main**. Selecione **Redefinir contagem de falhas de replicação de entrada** e clique em **aplicar alterações**.
RIRQ	Replicações de entrada — na fila	BLDR, BARC	Os alarmes podem ocorrer durante períodos de alta carga ou interrupção temporária da rede. Após a redução da atividade do sistema, este alarme deve ser apagado. Se a contagem de repetições em fila continuar a aumentar, procure problemas de rede e verifique se os serviços LDR e ARC de origem e destino estão online e disponíveis.

Código	Nome	Serviço	Ação recomendada
RORQ	Repetições de saída — em fila	BLDR, BARC	A fila de replicação de saída contém dados de objeto que estão sendo copiados para satisfazer as regras e objetos ILM solicitados pelos clientes. Um alarme pode ocorrer como resultado de uma sobrecarga do sistema. Aguarde para ver se o alarme é apagado quando a atividade do sistema diminui. Se o alarme voltar a ocorrer, adicione capacidade adicionando nós de storage.
SAVP	Espaço utilizável total (percentagem)	LDR	Se o espaço utilizável atingir um limite baixo, as opções incluem a expansão do sistema StorageGRID ou a movimentação de dados de objetos para arquivamento por meio de um nó de arquivamento.

Código	Nome	Serviço	Ação recomendada
SCAS	Estado	CMN	Se o valor de Status para a tarefa de grade ativa for erro, procure a mensagem de tarefa de grade. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **CMN Grid Tasks Overview Main**. A mensagem de tarefa de grade exibe informações sobre o erro (por exemplo, "'verificação falhou no nó 12130011'"). Depois de investigar e corrigir o problema, reinicie a tarefa de grade. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **CMN Grid Tasks Configuration Main** e selecione **Actions Run**. Se o valor de Status para uma tarefa de grade que está sendo cancelada for erro, tente abortar novamente a tarefa de grade. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
SCEP	Validade do certificado de Endpoints do Serviço de API de armazenamento	CMN	Acionado quando o certificado usado para acessar endpoints de API de armazenamento está prestes a expirar. 1. Vá para **Configuração certificados de servidor**. 2. Na seção Object Storage API Service Endpoints Server Certificate (certificado do servidor de Endpoints), faça o upload de um novo certificado. "Administrar o StorageGRID"
SCHR	Estado	CMN	Se o valor de Status para a tarefa de grade histórica for abortado, investigue o motivo e execute a tarefa novamente, se necessário. Se o problema persistir, entre em Contato com o suporte técnico.
SCSA	Controlador de armazenamento A	SSM	Um alarme é acionado se houver um problema com o controlador de armazenamento A em um dispositivo StorageGRID. Se necessário, substituir o órgão.

Código	Nome	Serviço	Ação recomendada
SCSB	Controlador de armazenamento B	SSM	Um alarme é acionado se houver um problema com o controlador de armazenamento B em um dispositivo StorageGRID. Se necessário, substituir o órgão. Alguns modelos de aparelhos não têm um controlador de armazenamento B..
SHLH	Saúde	LDR	Se o valor de integridade para um armazenamento de objetos for erro, verifique e corrija: • problemas com o volume a ser montado • erros do sistema de arquivos
SLSA	Média de carga da CPU	SSM	Quanto maior for o valor, mais ocupado o sistema. Se a média de carga da CPU persistir em um valor alto, o número de transações no sistema deve ser investigado para determinar se isso se deve a uma carga pesada no momento. Veja um gráfico da média de carga da CPU: Selecione **suporte Ferramentas topologia de grade**. Em seguida, selecione ***site grid node*** **SSM Resources Reports Charts**. Se a carga no sistema não for pesada e o problema persistir, contacte a assistência técnica.

Código	Nome	Serviço	Ação recomendada
SMST	Estado do monitor de registo	SSM	Se o valor do Estado do Monitor de Registos não estiver ligado durante um período de tempo persistente, contacte o suporte técnico.
SMTT	Total de eventos	SSM	Se o valor de Eventos totais for maior que zero, verifique se existem eventos conhecidos (como falhas de rede) que podem ser a causa. A menos que esses erros tenham sido apagados (ou seja, a contagem foi redefinida para 0), os alarmes de Total de Eventos podem ser acionados. Quando um problema for resolvido, reponha o contador para apagar o alarme. Selecione **nós *site grid node* Eventos Redefinir contagens de eventos**. Para redefinir contagens de eventos, você deve ter a permissão Configuração de Página de topologia de Grade. Se o valor de Total de Eventos for zero ou o número aumentar e o problema persistir, contacte o suporte técnico.

Código	Nome	Serviço	Ação recomendada
SNST	Estado	CMN	Um alarme indica que há um problema ao armazenar os pacotes de tarefas da grade. Se o valor de Status for erro de Checkpoint ou Quórum não atingido, confirme que a maioria dos serviços ADC está conetada ao sistema StorageGRID (50% mais um) e aguarde alguns minutos. Se o problema persistir, entre em Contato com o suporte técnico.
SOSS	Estado do sistema operativo de armazenamento	SSM	Um alarme é acionado se o software SANtricity indicar que há um problema de "precisa de atenção" com um componente em um dispositivo StorageGRID. Selecione **nós**. Em seguida, selecione **nó de armazenamento do dispositivo hardware**. Role para baixo para ver o status de cada componente. No software SANtricity, verifique outros componentes do dispositivo para isolar o problema.

Código	Nome	Serviço	Ação recomendada
SSMA	Estado SSM	SSM	Se o valor do Status SSM for erro, selecione **suporte Ferramentas topologia de grade** e, em seguida, selecione ***site grid node*** **SSM Visão geral Principal** e **SSM Visão geral Alarmes** para determinar a causa do alarme. Se o problema persistir, entre em Contato com o suporte técnico.
SSME	Estado SSM	SSM	Se o valor do estado SSM for Standby (em espera), continue a monitorização e, se o problema persistir, contacte a assistência técnica. Se o valor do estado SSM for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.

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

Código	Nome	Serviço	Ação recomendada
SVST	Estado	SSM	Este alarme é apagado quando outros alarmes relacionados a um serviço que não está em execução são resolvidos. Acompanhe os alarmes de serviço de origem para restaurar a operação. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **SSM Serviços Visão geral Principal**. Quando o status de um serviço é mostrado como não em execução, seu estado é administrativamente inativo. O status do serviço pode ser listado como não em execução pelos seguintes motivos: • O serviço foi interrompido manualmente (`/etc/init.d/<service\> stop`). • Há um problema com o banco de dados MySQL e o Server Manager desliga o serviço MI. • Um nó de grade foi adicionado, mas não iniciado. • Durante a instalação, um nó de grade ainda não se conetou ao nó Admin. Se um serviço estiver listado como não em execução, reinicie o serviço (`/etc/init.d/<service\> restart`). Esse alarme também pode indicar que o armazenamento de metadados (banco de dados Cassandra) para um nó de armazenamento

Código	Nome	Serviço	Ação recomendada
TMEM	Memória instalada	SSM	Os nós executados com menos de 24 GiB de memória instalada podem levar a problemas de performance e instabilidade do sistema. A quantidade de memória instalada no sistema deve ser aumentada para pelo menos 24 GiB.
TPOP	Operações pendentes	ADC	Uma fila de mensagens pode indicar que o serviço ADC está sobrecarregado. Poucos serviços ADC podem ser conetados ao sistema StorageGRID. Em uma grande implantação, o serviço ADC pode exigir a adição de recursos computacionais, ou o sistema pode exigir serviços ADC adicionais.
UMEM	Memória disponível	SSM	Se a RAM disponível ficar baixa, determine se este é um problema de hardware ou software. Se não for um problema de hardware ou se a memória disponível for inferior a 50 MB (o limite de alarme predefinido), contacte o suporte técnico.
VMFI	Entradas disponíveis	SSM	Esta é uma indicação de que é necessário um armazenamento adicional. Entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
VMFR	Espaço disponível	SSM	Se o valor de espaço disponível ficar muito baixo (consulte limiares de alarme), ele precisa ser investigado se há arquivos de log crescendo fora de proporção, ou objetos ocupando muito espaço em disco (veja limiares de alarme) que precisam ser reduzidos ou excluídos. Se o problema persistir, entre em Contato com o suporte técnico.
VMST	Estado	SSM	Um alarme é acionado se o valor de Status para o volume montado for desconhecido. Um valor desconhecido ou Offline pode indicar que o volume não pode ser montado ou acessado devido a um problema com o dispositivo de armazenamento subjacente.
VPRI	Prioridade de verificação	BLDR, BARC	Por padrão, o valor da prioridade de verificação é adaptável. Se a prioridade de verificação estiver definida como alta, um alarme é acionado porque a verificação do armazenamento pode retardar as operações normais do serviço.

Código	Nome	Serviço	Ação recomendada
VSTU	Estado Verificação Objeto	ERRO	Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site grid node*** **LDR Storage Overview Main**. Verifique se existem sinais de erros no sistema operativo ou no sistema de ficheiros. Se o valor do Status de Verificação de Objeto for erro desconhecido, ele geralmente indica um problema de hardware ou sistema de arquivos de baixo nível (erro de e/S) que impede que a tarefa de Verificação de armazenamento acesse conteúdo armazenado. Entre em Contato com o suporte técnico.
XAMS	Repositórios de auditoria inalcançáveis	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Verifique a conetividade de rede ao servidor que hospeda o nó Admin. Se o problema persistir, entre em Contato com o suporte técnico.

Alarmes que geram notificações SNMP (sistema legado)

A tabela a seguir lista os alarmes legados que geram notificações SNMP. Ao contrário dos alertas, nem todos os alarmes geram notificações SNMP. Apenas os alarmes listados geram notificações SNMP e apenas com a gravidade indicada ou superior.

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

Código	Nome	Gravidade
ACMS	Serviços de metadados disponíveis	Crítico
AITE	Recuperar Estado	Menor

Código	Nome	Gravidade
AITU	Recuperar Estado	Maior
AMQS	Mensagens de auditoria enfileiradas	Aviso
AOTE	Estado da loja	Menor
AOTU	Estado da loja	Maior
AROQ	Objetos em fila de espera	Menor
ARRF	Falhas de solicitação	Maior
ARRV	Falhas de verificação	Maior
ARVF	Falhas de armazenamento	Maior
ASXP	Compartilhamentos de auditoria	Menor
AUMA	Estado AMS	Menor
AUXS	Estado exportação Auditoria	Menor
BTOF	Desvio	Aviso
CAHP	Porcentagem de uso do Java Heap	Maior
CAQH	Número de destinos disponíveis	Aviso
CASA	Estado do armazenamento de dados	Maior
CDLP	Espaço usado (porcentagem)	Maior
CLBE	Estado CLB	Crítico
DNST	Estado DNS	Crítico
ECST	Estado de verificação	Maior
HSTE	Estado HTTP	Maior
HTAS	Auto-Iniciar HTTP	Aviso

Código	Nome	Gravidade
PERDIDO	Objetos perdidos	Maior
MINQ	Notificações de e-mail na fila	Aviso
MIN	Estado das notificações por e-mail	Menor
NANG	Configuração de negociação automática de rede	Aviso
NDUP	Configuração Duplex de rede	Menor
NLNK	Detecção de ligação de rede	Menor
NRER	Receber erros	Aviso
VELOCIDADE MÁXIMA	Velocidade	Aviso
NTER	Transmitir erros	Aviso
NTFQ	Desvio de frequência NTP	Menor
NTLK	Bloqueio NTP	Menor
NTOF	Desvio horário NTP	Menor
NTSJ	Jitter de fonte de tempo escolhido	Menor
NTSU	Estado NTP	Maior
OPST	Estado geral da alimentação	Maior
ORSU	Estado replicação saída	Aviso
PSAS	Estado da fonte de alimentação A.	Maior
PSB	Estado da fonte de alimentação B.	Maior
RDTE	Estado do Tivoli Storage Manager	Aviso
RDTU	Status do Tivoli Storage Manager	Maior
SAVP	Espaço utilizável total (percentagem)	Aviso

Código	Nome	Gravidade
SHLH	Saúde	Aviso
SLSA	Média de carga da CPU	Aviso
SMTT	Total de eventos	Aviso
SNST	Estado	
SOSS	Estado do sistema operativo de armazenamento	Aviso
SSTS	Estado de armazenamento	Aviso
SVST	Estado	Aviso
TMEM	Memória instalada	Menor
UMEM	Memória disponível	Menor
VMST	Estado	Menor
VPRI	Prioridade de verificação	Aviso
VSTU	Estado Verificação Objeto	Aviso

Referência de ficheiros de registo

As seções a seguir listam os logs 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.

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

> As tabelas nesta seção 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 deste guia.

Para acessar esses logs, você pode coletar arquivos de log e dados do sistema (**suporte Ferramentas Logs**). Ou, se o nó de administração principal não estiver disponível ou não conseguir alcançar um nó específico, você poderá acessar os logs de 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.

Informações relacionadas

"Coletando arquivos de log e dados do sistema"

Registos do software StorageGRID

Você pode usar logs do StorageGRID para solucionar problemas.

Registos gerais do StorageGRID

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

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

Logs do Server Manager

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

Logs para serviços StorageGRID

Nome do ficheiro	Notas	Encontrado em
`/var/local/log/acct.errlog`		Nós de storage executando o serviço ADC
`/var/local/log/adc.errlog`	Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de storage executando o serviço ADC
`/var/local/log/ams.errlog`		Nós de administração
`/var/local/log/arc.errlog`		Nós de arquivamento

Nome do ficheiro	Notas	Encontrado em
`/var/local/log/cassandra/system.log`	Informações para o armazenamento de metadados (banco de dados Cassandra) que podem ser usadas se ocorrerem problemas ao adicionar novos nós de armazenamento ou se a tarefa de reparo nodetool for interrompida.	Nós de storage
`/var/local/log/cassandra-reaper.log`	Informações para o serviço Cassandra Reaper, que executa reparos dos dados no banco de dados Cassandra.	Nós de storage
`/var/local/log/cassandra-reaper.errlog`	Informações de erro para o serviço Cassandra Reaper.	Nós de storage
`/var/local/log/chunk.errlog`		Nós de storage
`/var/local/log/clb.errlog`	Informações de erro para o serviço CLB. **Nota:** o serviço CLB está obsoleto.	Nós de gateway
`/var/local/log/cmn.errlog`		Nós de administração
`/var/local/log/cms.errlog`	Esse arquivo de log pode estar presente em sistemas que foram atualizados a partir de uma versão mais antiga do StorageGRID. Ele contém informações legadas.	Nós de storage
`/var/local/log/cts.errlog`	Esse arquivo de log só será criado se o tipo de destino for **Cloud Tiering - Simple Storage Service (S3).**	Nós de arquivamento
`/var/local/log/dds.errlog`		Nós de storage
`/var/local/log/dmv.errlog`		Nós de storage
`/var/local/log/dynip*`	Contém logs relacionados ao serviço dynip, que monitora a grade para alterações dinâmicas de IP e atualiza a configuração local.	Todos os nós

Nome do ficheiro	Notas	Encontrado em
`/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/ldr.errlog`		Nós de storage
`/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

Nome do ficheiro	Notas	Encontrado em
`/var/local/log/nginx-gw/*.log`	Contém logs para as portas de administração restritas em nós de administração e para o serviço Load Balancer, que fornece balanceamento de carga de tráfego S3 e Swift de clientes para nós de storage.	Nós de administração e nós de gateway
`/var/local/log/persistence*`	Contém logs para o serviço Persistence, que gerencia arquivos no disco raiz que precisam persistir durante uma reinicialização.	Todos os nós
`/var/local/log/prometheus.log`	Para todos os nós, contém o log de serviço de exportador de nós e o log de serviço de métricas ade-exportador. For Admin node, também contém logs para os serviços Prometheus e Alert Manager.	Todos os nós
`/var/local/log/raft.log`	Contém a saída da biblioteca usada pelo serviço RSM para o protocolo Raft.	Nós de storage com serviço RSM
`/var/local/log/rms.errlog`	Contém registos para o serviço RSM (Serviço de Máquina de Estado replicado), que é utilizado para serviços de plataforma S3.	Nós de storage com serviço RSM
`/var/local/log/ssm.errlog`		Todos os nós
`/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

Nome do ficheiro	Notas	Encontrado em
`/var/local/log/update-traffic-classes.log`	Contém registos relacionados com alterações na configuração dos classificadores de tráfego.	Nós de administrador e gateway
`/var/local/log/update-utcn.log`	Contém registos relacionados com o modo rede Cliente não fidedigno neste nó.	Todos os nós

Registos NMS

Nome do ficheiro	Notas	Encontrado em
`/var/local/log/nms.log`	• Captura notificações do Grid Manager e do Tenant Manager. • Captura eventos relacionados à operação do serviço NMS, por exemplo, processamento de alarmes, notificações por e-mail e alterações de configuração. • Contém atualizações de pacotes XML resultantes de alterações de configuração feitas no sistema. • Contém mensagens de erro relacionadas ao atributo downsampling feito uma vez por dia. • Contém mensagens de erro do servidor Web Java, por exemplo, erros de geração de página e erros HTTP Status 500.	Nós de administração
`/var/local/log/nms.errlog`	Contém mensagens de erro relacionadas às atualizações do banco de dados MySQL. Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de administração

Nome do ficheiro	Notas	Encontrado em
`/var/local/log/nms.requestlog`	Contém informações sobre conexões de saída da API de gerenciamento para serviços internos do StorageGRID.	Nós de administração

Informações relacionadas

"Sobre o bycast.log"

"Use S3"

Logs de implantação e manutenção

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

Nome do ficheiro	Notas	Encontrado em
`/var/local/log/install.log`	Criado durante a instalação do software. Contém um registo dos eventos de instalação.	Todos os nós
`/var/local/log/expansion-progress.log`	Criado durante operações de expansão. Contém um Registro dos eventos de expansão.	Nós de storage
`/var/local/log/gdu-server.log`	Criado pelo serviço GDU. Contém eventos relacionados aos procedimentos de provisionamento e manutenção gerenciados pelo nó de administração principal.	Nó de administração principal
`/var/local/log/send_admin_hw.log`	Criado durante a instalação. Contém informações de depuração relacionadas às comunicações de um nó com o nó de administração principal.	Todos os nós
`/var/local/log/upgrade.log`	Criado durante a atualização de software. Contém um registo dos eventos de atualização de software.	Todos os nós

Logs para software de terceiros

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

Categoria	Nome do ficheiro	Notas	Encontrado em

apache2 registos	`/var/local/log/apache2/access.log` `/var/local/log/apache2/error.log`
	
	`/var/local/log/apache2/other_vhosts_access.log`
		Ficheiros de registo para apache2.	Nós de administração

Arquivamento	`/var/local/log/dsierror.log`	Informações de erro para as APIs do cliente TSM.	Nós de arquivamento
MySQL	/var/local/log/mysql.err' `/var/local/log/mysql.err` `/var/local/log/mysql-slow.log`	Arquivos de log gerados pelo MySQL. O arquivo mysql.err captura erros de banco de dados e eventos, como startups e paradas. O arquivo mysql-slow.log (o log de consulta lenta) captura as instruções SQL que levaram mais de 10 segundos para serem executadas.	Nós de administração
Sistema operacional	`/var/local/log/messages`	Este diretório contém ficheiros de registo para o sistema operativo. Os erros contidos nesses logs também são exibidos no Gerenciador de Grade. Selecione **Support Tools Grid Topology**. Em seguida, selecione **topologia *Site Node* SSM Eventos**.	Todos os nós

Categoria	Nome do ficheiro	Notas	Encontrado em

NTP	`/var/local/log/ntp.log`
	
	`/var/lib/ntp/var/log/ntpstats/`
		O `/var/local/log/ntp.log` contém o ficheiro de registo para mensagens de erro NTP.
		
		O `/var/lib/ntp/var/log/ntpstats/` diretório contém estatísticas de tempo NTP.
		
		`loopstats` registra informações estatísticas de filtro de loop.
		
		`peerstats` registra informações estatísticas de pares.
			Todos os nós

Samba	`/var/local/log/samba/`	O diretório de log do Samba inclui um arquivo de log para cada processo Samba (SMB, nmb e winbind) e cada nome de host/IP do cliente.	Admin Node configurado para exportar o compartilhamento de auditoria por CIFS

Sobre o bycast.log

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

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

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.

Informações relacionadas

"Coletando 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.

Este é um exemplo de uma mensagem ADE:

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

As mensagens ADE contêm as seguintes informações:

Segmento de mensagens	Valor no exemplo
ID de nó	12455685
ID do processo ADE	0357819531
Nome do módulo	SVMR
Identificador da mensagem	EVHR
Hora do sistema UTC	2019-05-05T27T17:10:29,784677 (AAAA-MM-DDTHH:MM:SS.UUUUUUUUUUUU)
Nível de gravidade	ERRO
Número de rastreamento interno	0906
Mensagem	SVMR: A verificação do estado do volume 3 falhou com o motivo "TOUT"

Severidades da mensagem em bycast.log

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

Por exemplo:

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

Códigos de erro no 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

Número de erro	Código de erro	Significado
041		
042	ENOMSG	Nenhuma mensagem do tipo desejado
043	EIDRM	Identificador removido
044	ECHRNG	Número do canal fora do intervalo
045	EL2NSYNC	Nível 2 não sincronizado
046	EL3HLT	Nível 3 interrompido
047	EL3RST	Reposição do nível 3
048	ELNRNG	Número da ligação fora do intervalo
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

Número de erro	Código de erro	Significado
061	ENODATA	Nenhum dado disponível
062	ETIME	O temporizador expirou
063	ENOSR	Recursos fora de fluxos
064	ENONET	A máquina não está na rede
065	ENOPKG	Pacote não instalado
066	EREMOTE	O objeto é remoto
067	ENOLINK	O link foi cortado
068	EADV	Erro de anúncio
069	ESRMNT	Erro Srmount
070	ECOMM	Erro de comunicação no envio
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

Número de erro	Código de erro	Significado
081	ELIBSCN	
082	ELIBMAX	Tentando vincular em muitas bibliotecas compartilhadas
083	ELIBEXEC	Não é possível executar uma biblioteca compartilhada diretamente
084	EILSEQ	Sequência de bytes ilegal
085	ERESTART	A chamada do sistema interrompida deve ser reiniciada
086	ESTRPIPE	Erro no tubo de fluxos
087	EUSERS	Demasiados utilizadores
088	ENOTSOCK	Funcionamento da tomada sem tomada
089	EDESTADDRREQ	Endereço de destino obrigatório
090	EMSGSIZE	Mensagem demasiado longa
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

Número de erro	Código de erro	Significado
099	EADDRNOTAVAIL	Não é possível atribuir o endereço solicitado
100	ENETDOWN	A rede está inativa
101	ENETUNREACH	A rede não está acessível
102	ENETRESET	A ligação à rede foi interrompida devido à reposição
103	ECONNABORTED	O software causou interrupção da ligação
104	ECONNRESET	Conexão redefinida por ponto
105	ENOBUFS	Nenhum espaço de buffer disponível
106	EISCONN	O terminal de transporte já está ligado
107	ENOTCONN	O terminal de transporte não está ligado
108	ESHUTDOWN	Não é possível enviar após o encerramento do terminal de transporte
109	ETOOMANYREFS	Demasiadas referências: Não é possível unir
110	ETIMEDOUT	Tempo de ligação esgotado
111	ECONNREFUSED	Ligação recusada
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		

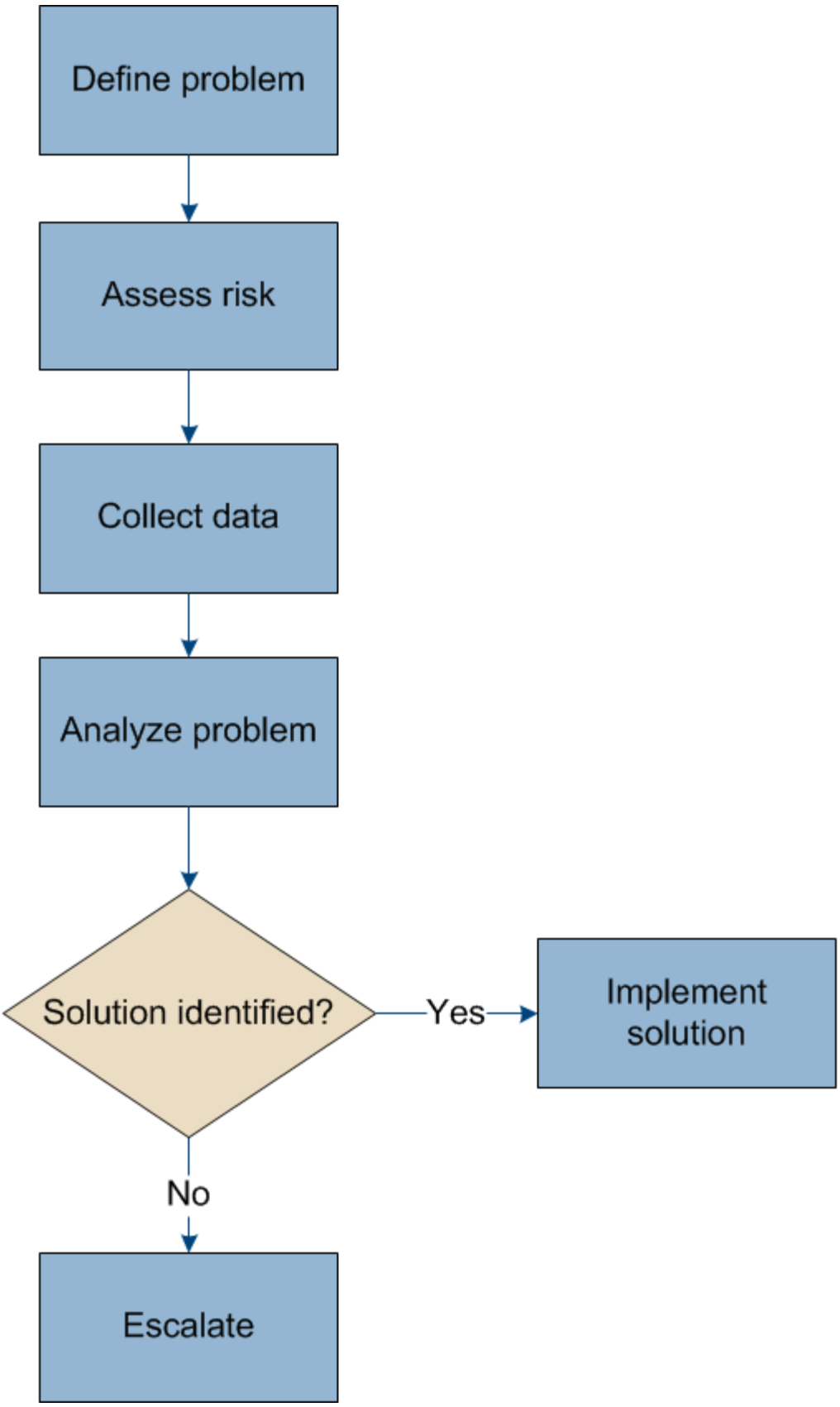
Número de erro	Código de erro	Significado
117	EUCLEAN	Estrutura precisa de limpeza
118	ENOTNAM	Não é um arquivo de tipo chamado XENIX
119	ENAVAIL	Não há semáforos XENIX disponíveis
120	EISNAM	É um arquivo de tipo nomeado
121	EREMOTEIO	Erro de e/S remota
122	EDQUOT	Quota excedida
123	ENOMEDIUM	Nenhum meio encontrado
124	EMEDIUMTYPE	Tipo médio errado
125	ECANCELED	Operação cancelada
126	ENOKEY	Chave necessária não disponível
127	EKEYEXPIRED	A chave expirou
128	EKEYREVOKED	A chave foi revogada
129	EKEYREJECTED	A chave foi rejeitada pelo serviço de revisão
130	EOWNERDEAD	Para mutexes robustos: O proprietário morreu
131	ENOTRECOVERABLE	Para mutexes robustos: Estado não recuperável

Solucionar problemas de um sistema StorageGRID

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

Visão geral da determinação do problema

Se você encontrar um problema ao administrar um sistema StorageGRID, você pode usar o processo descrito nesta figura para identificar e analisar o problema. Em muitos casos, você pode resolver problemas sozinho. No entanto, talvez seja necessário encaminhar alguns problemas para o suporte técnico.



Definir o problema

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

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

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

Avaliar o risco e o impactos no sistema

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

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

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

Coleta de 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.	• Criando uma linha do tempo de mudanças recentes
Reveja alertas e alarmes	Alertas e alarmes podem ajudá-lo a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre os problemas subjacentes que podem estar causando isso. Revise a lista de alertas e alarmes atuais para ver se o StorageGRID identificou a causa raiz de um problema para você. Reveja alertas e alarmes acionados no passado para obter informações adicionais.	• "Visualização de alertas atuais" • "Visualização de alarmes legados" • "Visualização de alertas resolvidos" • "Revisão de alarmes históricos e frequência de alarmes (sistema legado)"
Monitorar eventos	Os eventos incluem qualquer erro de sistema ou eventos de falha para um nó, incluindo erros como erros de rede. Monitore eventos para saber mais sobre problemas ou para ajudar na solução de problemas.	• "Visualizar o separador Eventos" • "Monitoramento de eventos"
Identificar tendências, usando relatórios de gráfico e 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.	• "Usando gráficos e relatórios"
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.	• Estabelecendo 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.	• "Monitorar O PUT e obter 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"

Tipo de dados a recolher	Por que coletar esses dados	Instruções
Verifique os locais dos objetos e a integridade do armazenamento	Se você estiver tendo problemas de armazenamento, verifique se os objetos estão sendo colocados onde você espera. Verifique a integridade dos dados do objeto em um nó de storage.	"Monitoramento de operações de verificação de objetos".
Coletar dados para suporte técnico	O suporte técnico pode solicitar que você colete dados ou revise informações específicas para ajudar a solucionar problemas.	• "Coletando arquivos de log e dados do sistema" • "Acionando manualmente uma mensagem AutoSupport" • "Revisão das métricas de suporte"

Criando uma linha do tempo de mudanças recentes

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

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

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

Hora da mudança	Tipo de alteração	Detalhes
Por exemplo: • Quando você iniciou a recuperação do nó? • Quando a atualização de software foi concluída? • Interrompeu o processo?	O que aconteceu? O que fez?	Documente todos os detalhes relevantes sobre a alteração. Por exemplo: • Detalhes das alterações de rede. • Qual hotfix foi instalado. • Como as cargas de trabalho do cliente mudaram. Certifique-se de observar se mais de uma mudança estava acontecendo ao mesmo tempo. Por exemplo, essa alteração foi feita enquanto uma atualização estava em andamento?

Exemplos de mudanças recentes significativas

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi recentemente instalado, expandido ou recuperado?
- O sistema foi atualizado recentemente? Foi aplicado um hotfix?
- Algum hardware foi reparado ou alterado recentemente?
- A política ILM foi atualizada?
- A carga de trabalho do cliente mudou?
- O aplicativo cliente ou seu comportamento mudou?
- Você alterou balanceadores de carga ou adicionou ou removeu um grupo de alta disponibilidade de nós de administrador ou nós de gateway?
- Foram iniciadas tarefas que podem demorar muito tempo a concluir? Os exemplos incluem:
  - Recuperação de um nó de storage com falha
  - Desativação do nó de storage
- Alguma alteração foi feita à autenticação do usuário, como adicionar um locatário ou alterar a configuração LDAP?
- A migração de dados está ocorrendo?
- Os serviços de plataforma foram recentemente ativados ou alterados?
- A conformidade foi ativada recentemente?
- Os pools de armazenamento em nuvem foram adicionados ou removidos?
- Alguma alteração foi feita na compactação ou criptografia de armazenamento?
- Houve alguma alteração na infra-estrutura de rede? Por exemplo, VLANs, roteadores ou DNS.
- Alguma alteração foi feita em fontes NTP?
- Alguma alteração foi feita nas interfaces Grid, Admin ou Client Network?
- Alguma alteração de configuração foi feita no nó Arquivo?
- Alguma outra alteração foi feita ao sistema StorageGRID ou ao seu ambiente?

Estabelecendo 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. Passe o cursor sobre o gráfico para estimar a quantidade de armazenamento consumida todos os dias Você pode coletar essas informações para todo o sistema ou para um data center específico.

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. Passe o cursor sobre o gráfico para estimar quanto armazenamento de metadados é consumido diariamente Você pode coletar essas informações para todo o sistema ou para um data center específico.
Taxa de operações S3/Swift	Operações/segundo	Vá para o Painel no Gerenciador de Grade. Na seção Protocol Operations (operações de protocolo), visualize os valores da taxa S3 e da taxa Swift. Para ver as taxas de ingestão e recuperação e contagens para um site ou nó específico, selecione **nós *site ou nó de armazenamento* objetos**. Passe o cursor sobre o gráfico de ingestão e recuperação para S3 ou Swift.
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. Passe 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. Passe 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. Passe o cursor sobre o gráfico para estimar um valor de linha de base para **objetos enfileirados (de operações do cliente)** para o seu sistema.
Latência média da consulta	Milissegundos	Selecione **nós *Storage Node* Objects**. Na tabela consultas, exiba o valor da latência média.

Analisando dados

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

A análise é dependente de problemas, mas em geral:

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

Lista de verificação de informações de encaminhamento

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

✔	Item	Notas
	Declaração do problema	Quais são os sintomas do problema? Quando o problema começou? Isso acontece de forma consistente ou intermitente? Se intermitentemente, que horas ocorreu? "Definir 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 **Manutenção sistema Licença**. A ID do sistema StorageGRID é apresentada como parte da licença atual.
	Versão do software	Clique em **Ajuda sobre** para ver a versão do StorageGRID.
	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 para apagamento? O ILM garante a redundância do site? As regras do ILM usam os comportamentos de ingestão estritos, balanceados ou Dual Commit?

✔	Item	Notas
	Ficheiros de registo e dados do sistema	Recolha ficheiros de registo e dados do sistema para o seu sistema. Selecione **suporte Ferramentas 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.) "Coletando 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. "Estabelecendo linhas de base"
	Cronograma das mudanças recentes	Crie uma linha do tempo que resume quaisquer alterações recentes ao sistema ou ao seu ambiente. "Criando uma linha do tempo de 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.

Informações relacionadas

"Administrar o StorageGRID"

Solução de problemas de objetos e storage

Há várias tarefas que você pode executar para ajudar a determinar a origem dos problemas de armazenamento e objeto.

Confirmar localizações de dados do objeto

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

O que você vai precisar

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

- * Nome do contentor e objeto Swift*: Quando um objeto é ingerido através da interface Swift, o aplicativo cliente usa uma combinação de nome de contentor e objeto para armazenar e identificar o objeto.

Passos

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

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

3. Clique em **Procurar**.

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

   - Metadados do sistema, incluindo o ID do objeto (UUID), o 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",
```


Informações relacionadas

"Gerenciar objetos com ILM"

"Use S3"

"Use Swift"

Falhas no armazenamento de objetos (volume de storage)

O storage subjacente em um nó de storage é dividido em armazenamentos de objetos. Esses armazenamentos de objetos são partições físicas que atuam como pontos de montagem para o armazenamento do sistema StorageGRID. 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
croot(8:1,sda1)	N/A	1.62%	0 bytes/s	177 KB/s
cvloc(8:2,sda2)	N/A	17.28%	0 bytes/s	2 MB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	11 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	0 bytes/s
sds(8:48,sdd)	N/A	0.00%	0 bytes/s	0 bytes/s

Volumes

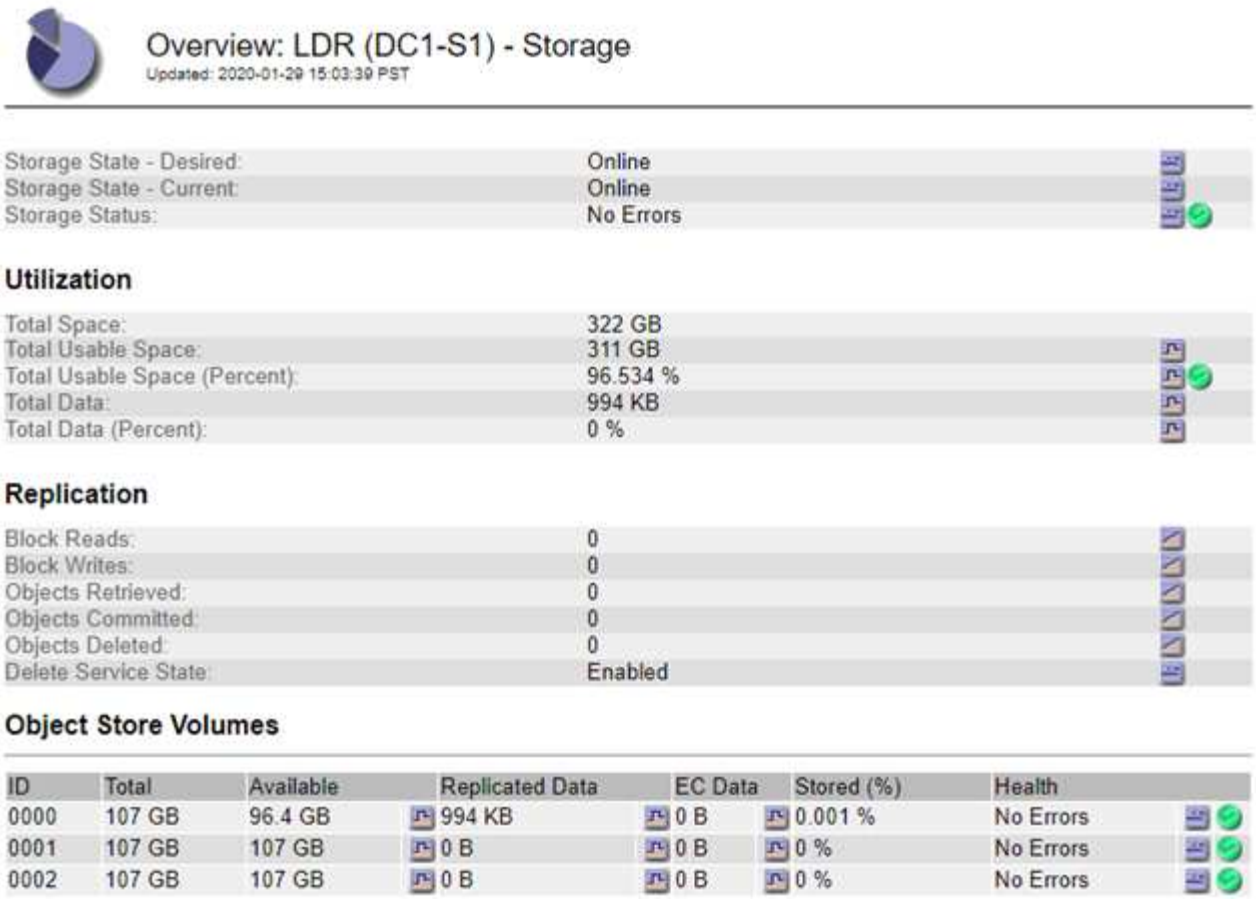
Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	21.00 GB	14.25 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sds	Online	107.32 GB	107.18 GB	Enabled

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	107.32 GB	96.45 GB	994.37 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

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

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site Storage Node*** **LDR Storage Overview Main**.



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

Informações relacionadas

"Manter recuperar"

Verificando 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 em segundo plano e verificação em 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. A verificação de primeiro plano pode ser acionada por um usuário, para verificar mais rapidamente a existência (embora não a correção) de objetos.

O que é a verificação de antecedentes

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

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

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

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

- **Objetos codificados por apagamento**: Se o processo de verificação em segundo plano 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, o atributo cópias corrompidas detetadas (ECOR) é incrementado por um, e uma tentativa é feita para recuperar outra cópia do objeto. Se a recuperação for bem-sucedida, uma avaliação ILM será executada para criar uma cópia de substituição do objeto codificado de apagamento.

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

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

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

Se o sistema detetar um objeto corrompido que não possa 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** e o alarme legado PERDIDO (objetos perdidos) são acionados.

Alterar a taxa de verificação em segundo plano

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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

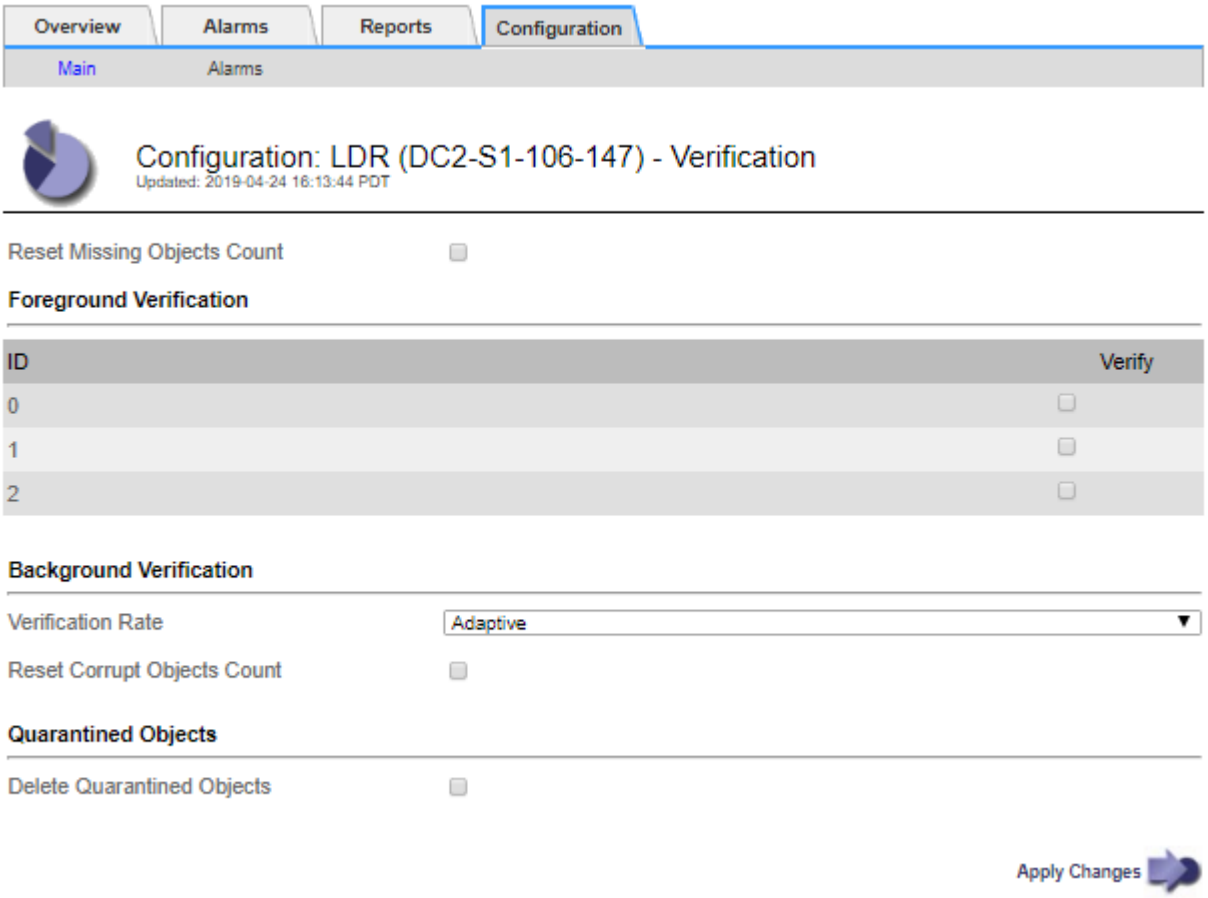
- Adaptive (adaptável): Predefinição. A tarefa foi projetada para verificar no máximo 4 MB/s ou 10 objetos/s (o que for excedido primeiro).

- Alta: A verificação do armazenamento prossegue rapidamente, a uma taxa que pode retardar as atividades normais do sistema.

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

Passos

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



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

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

Se a verificação em segundo plano encontrar dados de objeto replicados corrompidos, a métrica **objetos corrompidos** será incrementada e o StorageGRID tentará extrair o identificador de objeto dos dados, da seguinte forma:

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

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

3. 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).

4. 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 Verification Configuration**.
   c. Selecione **Redefinir contagem de objetos corrompidos**.
   d. Clique em **aplicar alterações**.
5. Se você estiver confiante de que objetos em quarentena não são necessários, você pode excluí-los.

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

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Storage Node*** **LDR Verificação Configuração**.
3. Selecione **Excluir objetos em quarentena**.
4. Clique em **aplicar alterações**.

O que é a verificação de primeiro plano

A verificação em primeiro plano é um processo iniciado pelo usuário que verifica se todos os dados de objeto esperados existem em um nó de armazenamento. A verificação de primeiro plano é usada para verificar a integridade de um dispositivo de armazenamento.

A verificação em primeiro plano é uma alternativa mais rápida à verificação em segundo plano que verifica a existência, mas não a integridade, de dados de objetos em um nó de armazenamento. Se a verificação de primeiro plano descobrir que muitos itens estão faltando, pode haver um problema com a totalidade ou parte de um dispositivo de armazenamento associado ao nó de armazenamento.

A verificação em primeiro plano verifica os dados de objetos replicados e os dados de objetos codificados por apagamento, da seguinte forma:

- **Objetos replicados**: Se uma cópia dos dados de objetos replicados estiver ausente, o StorageGRID tentará substituir automaticamente a cópia de cópias armazenadas 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 a cópia ausente não existe mais no local esperado. Uma nova cópia é gerada e colocada para satisfazer a política ILM ativa do sistema. Esta nova cópia pode não ser colocada no mesmo local em que a cópia em falta foi armazenada.
- **Objetos 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 armazenamento usando os fragmentos restantes. Se o fragmento ausente não puder ser reconstruído (porque muitos fragmentos foram perdidos), o atributo cópias corrompidas detetadas (ECOR) é incrementado por um. O ILM então tenta encontrar outra cópia do objeto, que ele pode usar para gerar uma nova cópia codificada por apagamento.

  Se a verificação em primeiro plano identificar um problema com a codificação de apagamento em um volume de armazenamento, a tarefa de verificação em primeiro plano será interrompida com uma mensagem de erro que identifique o volume afetado. Você deve executar um procedimento de recuperação para todos os volumes de armazenamento afetados.

Se nenhuma outra cópia de um objeto replicado em falta ou de um objeto codificado de apagamento corrompido puder ser encontrada na grade, o alerta **objetos perdidos** e o alarme legado PERDIDO (objetos perdidos) serão acionados.

A executar a verificação de primeiro plano

A verificação em primeiro plano permite verificar a existência de dados em um nó de armazenamento. Dados de objeto ausentes podem indicar que existe um problema com o dispositivo de armazenamento subjacente.

O que você vai precisar

- Você garantiu que as seguintes tarefas de grade não estão sendo executadas:
  - Expansão da grade: Adicione servidor (GEXP), ao adicionar um nó de armazenamento
  - Desativação do nó de armazenamento (LDCM) no mesmo nó de armazenamento se estas tarefas de grade estiverem em execução, aguarde que elas sejam concluídas ou liberem seu bloqueio.
- Você garantiu que o armazenamento está online. (Selecione **Support Tools Grid Topology**. Em seguida, selecione ***Storage Node* LDR Storage Overview Main**. Certifique-se de que **Estado de armazenamento - atual** está online.)
- Você garantiu que os seguintes procedimentos de recuperação não estão sendo executados no mesmo nó de storage:
  - Recuperação de um volume de armazenamento com falha
  - A recuperação de um nó de armazenamento com uma falha na verificação de primeiro plano da unidade do sistema não fornece informações úteis enquanto os procedimentos de recuperação estão em andamento.

Sobre esta tarefa

Verificações de primeiro plano para dados de objetos replicados em falta e dados de objetos codificados por apagamento em falta:

- Se a verificação em primeiro plano encontrar grandes quantidades de dados de objetos em falta, provavelmente há um problema com o armazenamento do nó de armazenamento que precisa ser

investigado e resolvido.

- Se a verificação em primeiro plano encontrar um erro de armazenamento grave associado a dados codificados por apagamento, ela o notificará. Você deve executar a recuperação do volume de armazenamento para reparar o erro.

Você pode configurar a verificação de primeiro plano para verificar todos os armazenamentos de objetos de um nó de armazenamento ou apenas armazenamentos de objetos específicos.

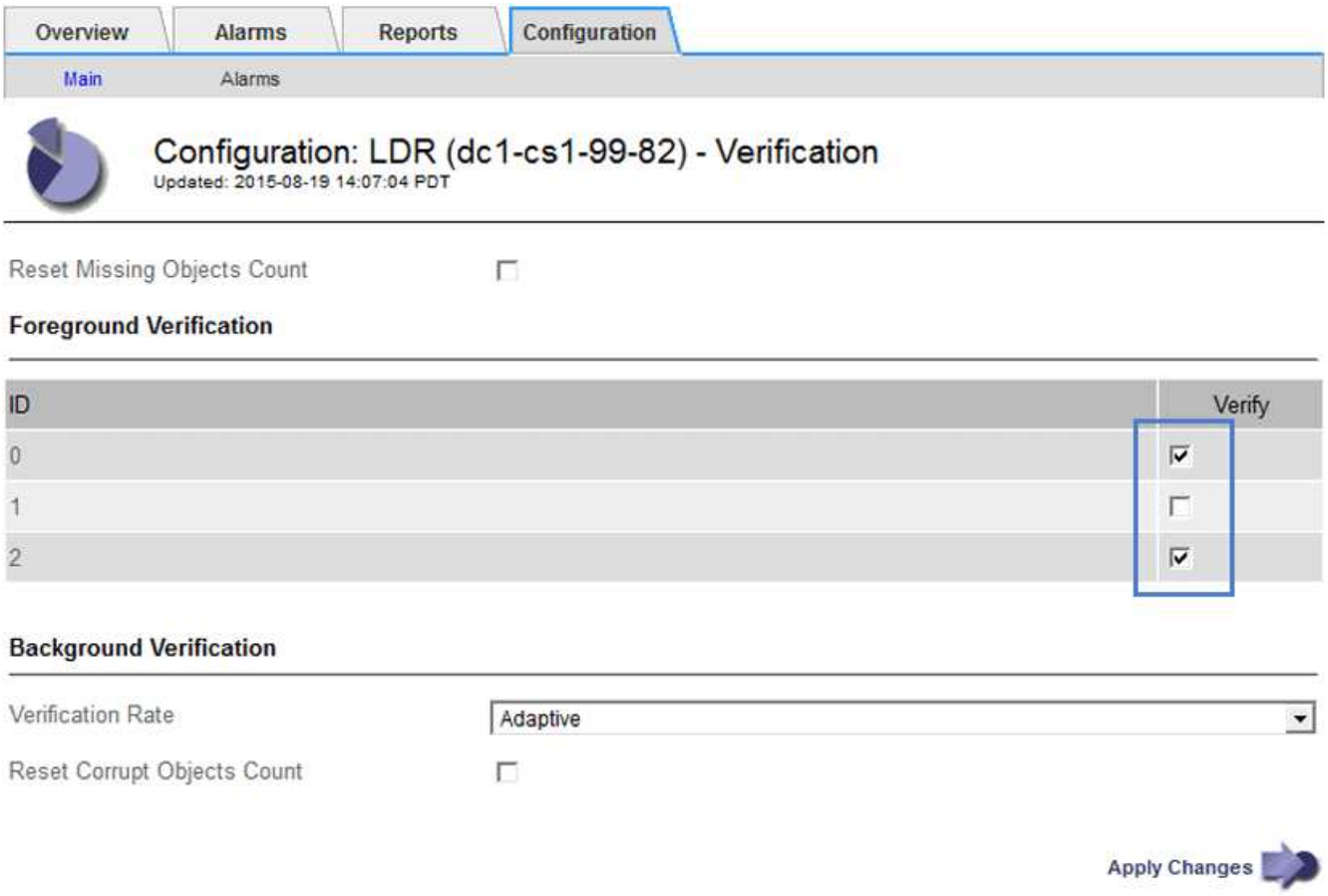
Se a verificação de primeiro plano encontrar dados de objeto em falta, o sistema StorageGRID tentará substituí-los. Se não for possível efetuar uma cópia de substituição, o alarme PERDIDO (objetos perdidos) poderá ser acionado.

A verificação em primeiro plano gera uma tarefa de grade de verificação em primeiro plano LDR que, dependendo do número de objetos armazenados em um nó de armazenamento, pode levar dias ou semanas para ser concluída. É possível selecionar vários nós de storage ao mesmo tempo; no entanto, essas tarefas de grade não são executadas simultaneamente. Em vez disso, eles são enfileirados e executados um após o outro até a conclusão. Quando a verificação em primeiro plano está em andamento em um nó de armazenamento, você não pode iniciar outra tarefa de verificação em primeiro plano nesse mesmo nó de armazenamento, mesmo que a opção para verificar volumes adicionais possa parecer estar disponível para o nó de armazenamento.

Se um nó de armazenamento diferente daquele em que a verificação de primeiro plano está sendo executada ficar off-line, a tarefa de grade continuará sendo executada até que o atributo **% completo** atinja 99,99%. O atributo **% complete** então volta para 50 por cento e espera que o nó de armazenamento retorne ao status online. Quando o estado do nó de armazenamento regressa à linha, a tarefa da grelha de verificação de primeiro plano do LDR continua até ser concluída.

Passos

1. Selecione ***Storage Node* LDR Verification**.
2. Selecione **Configuração** > **Principal**.
3. Em **Verificação de primeiro plano**, marque a caixa de seleção para cada ID de volume de armazenamento que deseja verificar.



4. Clique em **aplicar alterações**.

   Aguarde até que a página seja atualizada automaticamente e recarregada antes de sair da página. Uma vez atualizados, os armazenamentos de objetos ficam indisponíveis para seleção nesse nó de armazenamento.

   Uma tarefa de grade de verificação de primeiro plano do LDR é gerada e executada até que ela seja concluída, pausa ou abortada.

5. Monitorar objetos em falta ou fragmentos em falta:

   a. Selecione ***Storage Node* LDR Verification**.

   b. Na guia Visão geral em **resultados da verificação**, observe o valor de **objetos ausentes detetados**.

      Nota: O mesmo valor é relatado como **objetos perdidos** na página de nós. Vá para **nodes *Storage Node*** e selecione a guia **Objects**.

      Se o número de **objetos ausentes detetados** for grande (se houver centenas de objetos ausentes), provavelmente há um problema com o armazenamento do nó de armazenamento. Entre em Contato com o suporte técnico.

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

   d. Na guia Visão geral em **resultados da verificação**, observe o valor de **fragmentos ausentes detetados**.

      Se o número de **fragmentos ausentes detetados** for grande (se houver centenas de fragmentos ausentes), provavelmente há um problema com o armazenamento do nó de armazenamento. Entre

em Contato com o suporte técnico.

Se a verificação em primeiro plano não detetar um número significativo de cópias de objetos replicados em falta ou um número significativo de fragmentos ausentes, o storage estará operando normalmente.

6. Monitorize a conclusão da tarefa de grelha de verificação em primeiro plano:
   a. Selecione **Support Tools Grid Topology**. Em seguida, selecione **site *Admin Node* CMN Grid Task Overview Main**.
   b. Verifique se a tarefa da grade de verificação de primeiro plano está progredindo sem erros.

      Nota: Um alarme de nível de aviso é acionado no status da tarefa de grade (SCAs) se a tarefa de grade de verificação de primeiro plano for interrompida.

   c. Se a tarefa de grade parar com um `critical storage error`, recupere o volume afetado e execute a verificação de primeiro plano nos volumes restantes para verificar se há erros adicionais.

      Atenção: Se a tarefa da grade de verificação de primeiro plano for interrompida com a mensagem `Encountered a critical storage error in volume volID`, você deverá executar o procedimento para recuperar um volume de armazenamento com falha. Consulte as instruções de recuperação e manutenção.

Depois de terminar

Se você ainda tiver dúvidas sobre a integridade dos dados, vá para **LDR Verificação Configuração Principal** 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.

Informações relacionadas

"Manter recuperar"

Solução de 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** e o alarme legado PERDIDO (objetos perdidos) são acionados, da seguinte forma:

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

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

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

Informações relacionadas

"Investigando objetos perdidos"

"Repor contagens de objetos perdidas e em falta"

Investigando objetos perdidos

Quando o alerta **objetos perdidos** e o alarme legado PERDIDO (objetos perdidos) são acionados, você deve investigar imediatamente. Colete informações sobre os objetos afetados e entre em Contato com o suporte técnico.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

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

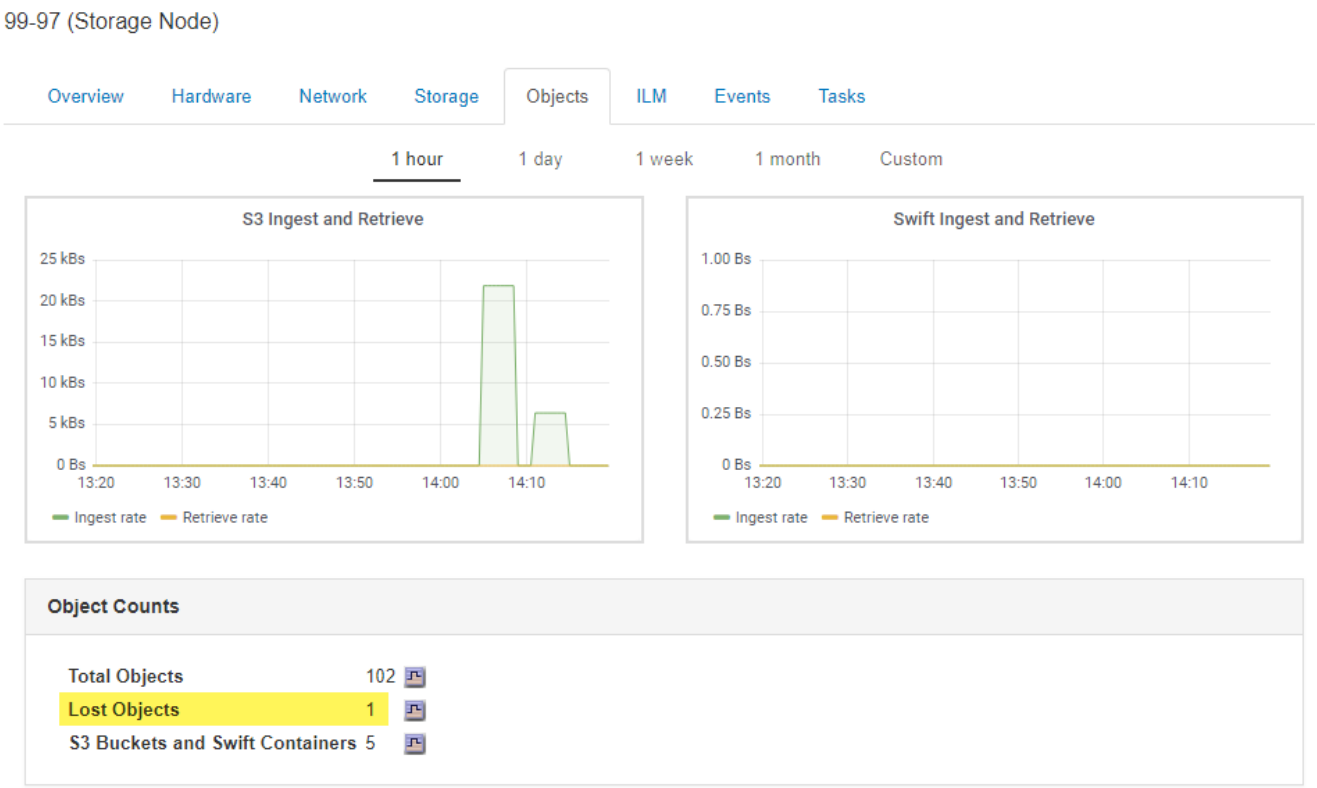
Investigue alarmes ou alertas de objetos perdidos imediatamente. Talvez seja necessário tomar medidas para evitar mais perda de dados. Em alguns casos, você pode restaurar um objeto perdido se você tomar uma ação imediata.

O número de objetos perdidos pode ser visto no Gerenciador de Grade.

Passos

1. Selecione **nós**.
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** e o alarme PERDIDO:
   a. Faça login no nó da grade:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
   b. Mude para o diretório onde os logs de auditoria estão localizados. Introduza: `cd /var/local/audit/export/`
   c. Use grep para extrair as mensagens de auditoria OLST (Object Lost). Introduza: `grep OLST audit_file_name`
   d. Observe o valor UUID incluído na mensagem.

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

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

   a. Telnet para localhost 1402 para acessar o console LDR.

   b. Introduza: `/proc/OBRP/ObjectByUUID UUID_value`

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

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

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

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

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

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

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

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

Metadados	Conclusão
Nenhum objeto encontrado ("ERRO":"")	Se o objeto não for encontrado, a mensagem "ERROR":" é retornada. Se o objeto não for encontrado, é seguro ignorar o alarme. A falta de um objeto indica que o objeto foi intencionalmente excluído.
Locais 0	Se houver locais listados na saída, o alarme de 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 localizar objetos potencialmente perdidos explica como usar o ID do nó para encontrar o nó de armazenamento correto.) "Procurar e restaurar objetos potencialmente perdidos" Se existirem objetos, pode repor a contagem de objetos perdidos para limpar o alarme e o alerta.
Localização: 0	Se não houver locais listados na saída, o objeto está potencialmente ausente. Você pode tentar encontrar e restaurar o objeto você mesmo, ou você pode entrar em Contato com o suporte técnico. "Procurar e restaurar objetos potencialmente perdidos" O suporte técnico pode pedir-lhe para determinar se existe um procedimento de recuperação de armazenamento em curso. Ou seja, um comando *repair-data* foi emitido em qualquer nó de armazenamento e a recuperação ainda está em andamento? Consulte as informações sobre como restaurar dados de objetos para um volume de armazenamento nas instruções de recuperação e manutenção.

Informações relacionadas

"Manter recuperar"

"Rever registos de auditoria"

Procurar e restaurar objetos potencialmente perdidos

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

O que você vai precisar

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

Sobre esta tarefa

Você pode seguir este procedimento para procurar cópias replicadas do objeto perdido em outro lugar na grade. Na maioria dos casos, o objeto perdido não será encontrado. No entanto, em alguns casos, você pode encontrar e restaurar um objeto replicado perdido se você executar uma ação de prompt.

Contacte o suporte técnico para obter assistência com este procedimento.

Passos

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

      Por exemplo:

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

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

      Por exemplo:

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

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

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

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

Se presente, o valor de PCLD é o caminho completo no disco para a cópia de objeto replicado em falta. O valor de NOID é o id do nó do LDR onde uma cópia do objeto pode ser encontrada.

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

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

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

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

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

a. Faça login no nó da grade:

i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

iii. Digite o seguinte comando para mudar para root: `su -`

iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

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'
```

Nota: 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 Restaure o objeto para o StorageGRIDetapa . Você pode tentar restaurar o objeto encontrado de volta para o StorageGRID.

1. 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 a política ILM ativa, que faz cópias adicionais conforme especificado na política.

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

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

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

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

        Avance para o passo Verifique se foram criados novos locais

1. Se o objeto foi restaurado com sucesso para o StorageGRID, verifique se novos locais foram criados.
   a. Introduza: `cd /proc/OBRP`
   b. Introduza: `ObjectByUUID UUID_value`

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

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

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
```

```
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. Saia da consola LDR. Introduza: `exit`

2. 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/audit/export/`

   c. Use grep para extrair as mensagens de auditoria associadas ao objeto para um arquivo de saída. Introduza: `grep uuid-valueaudit_file_name > output_file_name`

      Por exemplo:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      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 essa mensagem de exemplo.

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

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.

b. Redefina a contagem de objetos perdidos no Gerenciador de Grade.

Informações relacionadas

"Investigando objetos perdidos"

"Confirmar localizações de dados do objeto"

"Repor contagens de objetos perdidas e em falta"

"Rever registos de auditoria"

Repor contagens de objetos perdidas e em falta

Depois de investigar o sistema StorageGRID e verificar se todos os objetos perdidos gravados são perdidos permanentemente ou se é um alarme falso, você pode redefinir o valor do atributo objetos perdidos para zero.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

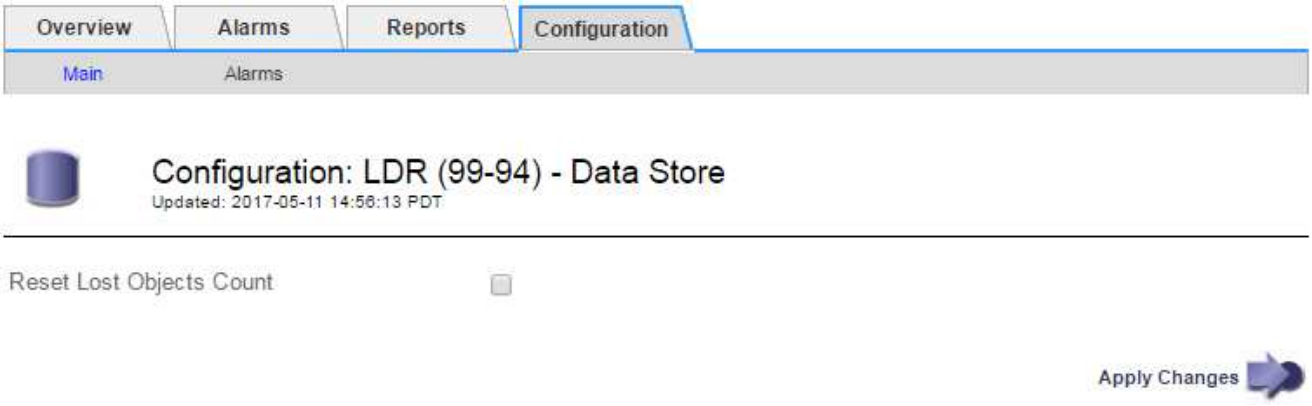
Você pode redefinir o contador de objetos perdidos a partir de uma das seguintes páginas:

- **Suporte Ferramentas topologia de Grade *Site Storage Node* LDR Data Store Overview Main**
- **Suporte Ferramentas topologia de Grade *Site Storage Node* DDS Data Store Visão geral Principal**

Estas instruções mostram a reposição do contador a partir da página **LDR Data Store**.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Site Storage Node* LDR Data Store Configuration** para o nó de armazenamento que tem o alerta **objetos perdidos** ou o alarme PERDIDO.
3. Selecione **Redefinir contagem de objetos perdidos**.



4. Clique em **aplicar alterações**.

   O atributo objetos perdidos é redefinido para 0 e o alerta **objetos perdidos** e o alarme PERDIDO são apagados, o que pode levar alguns minutos.

5. Opcionalmente, redefina outros valores de atributo relacionados que podem ter sido incrementados no processo de identificação do objeto perdido.

   a. Selecione ***Site Storage Node* LDR Erasure Coding Configuration**.

   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).

Informações relacionadas

"Administrar o StorageGRID"

Solução de problemas do alerta de armazenamento de dados de objetos baixos

O alerta **armazenamento de dados de objeto baixo** monitora quanto espaço está disponível para armazenar dados de objeto em cada nó de armazenamento.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

O **armazenamento de dados de objeto baixo** é acionado quando a quantidade total de dados de objeto codificados replicados e apagados em um nó de armazenamento atende a uma das condições configuradas na regra de alerta.

Por padrão, um alerta principal é acionado quando essa condição é avaliada como verdadeira:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Nesta condição:

- `storagegrid_storage_utilization_data_bytes` É uma estimativa do tamanho total dos dados de objetos codificados de apagamento e replicados para um nó de storage.
- `storagegrid_storage_utilization_usable_space_bytes` É a quantidade total de espaço de storage de objetos restante para um nó de storage.

Se um alerta maior ou menor **armazenamento de dados de objeto baixo** for acionado, você deve executar um procedimento de expansão o mais rápido possível.

Passos

1. Selecione **Alertas 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.

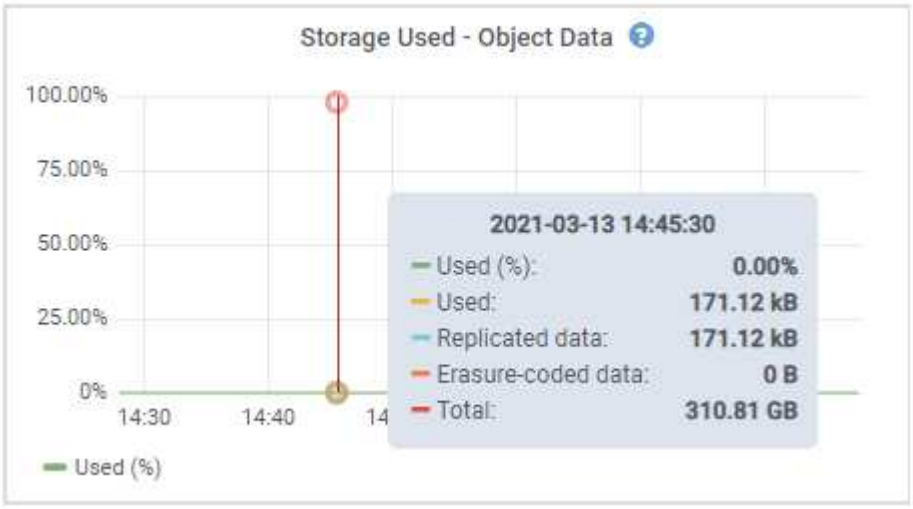
   Selecione o alerta e não o cabeçalho de um grupo de alertas.

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. Passe o cursor sobre o gráfico Storage Used - Object Data (armazenamento usado - dados do objeto).

   São apresentados os seguintes valores:

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

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



6. Selecione os controles de tempo acima do gráfico para exibir o uso do armazenamento em diferentes períodos de tempo.

   Analisar o uso do armazenamento ao longo do tempo pode ajudá-lo a entender quanto armazenamento foi usado antes e depois do alerta ser acionado e pode ajudá-lo a estimar quanto tempo pode levar para que o espaço restante do nó fique cheio.

7. Assim que possível, execute um procedimento de expansão para adicionar capacidade de armazenamento.

   Você pode adicionar volumes de storage (LUNs) aos nós de storage existentes ou adicionar novos nós de storage.

   > Para gerenciar um nó de storage completo, consulte as instruções de administração do StorageGRID.

Informações relacionadas

"Resolução de problemas do alarme de Estado de armazenamento (SSTS)"

"Expanda sua grade"

"Administrar o StorageGRID"

Resolução de problemas do alarme de Estado de armazenamento (SSTS)

O alarme de Estado de armazenamento (SSTS) é acionado se um nó de armazenamento tiver espaço livre insuficiente restante para armazenamento de objetos.

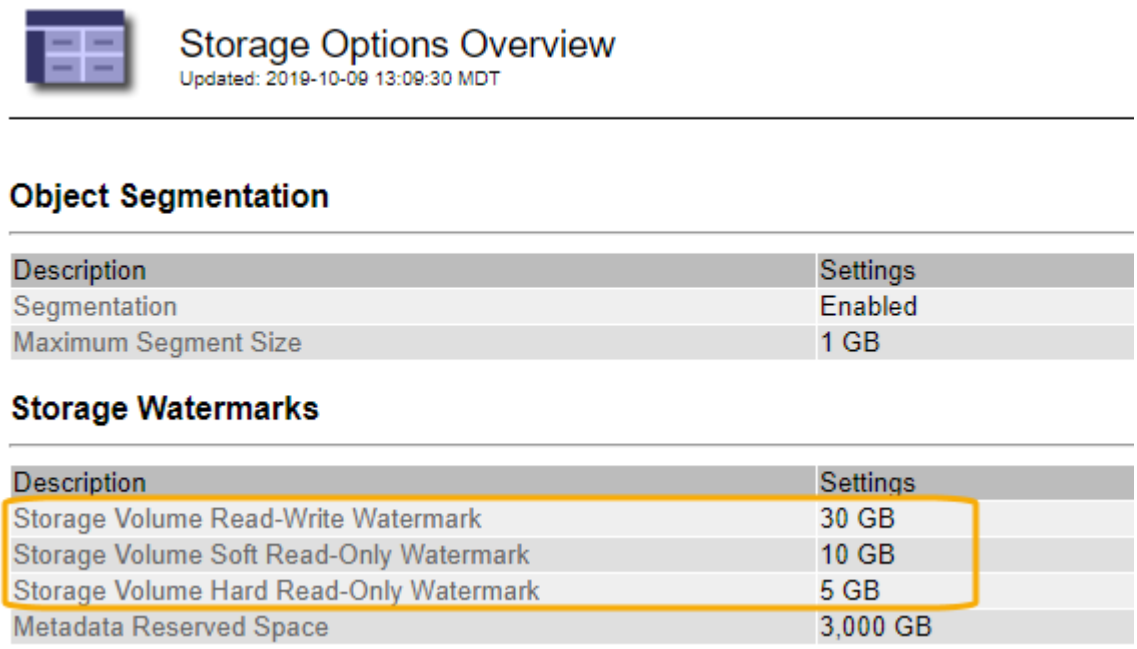
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

O alarme SSTS (Storage Status) é acionado no nível de Aviso quando a quantidade de espaço livre em cada

volume em um nó de armazenamento cai abaixo do valor do volume de armazenamento Soft Read Only Watermark (**Configuração Opções de armazenamento Visão geral**).



Storage Options Overview
Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

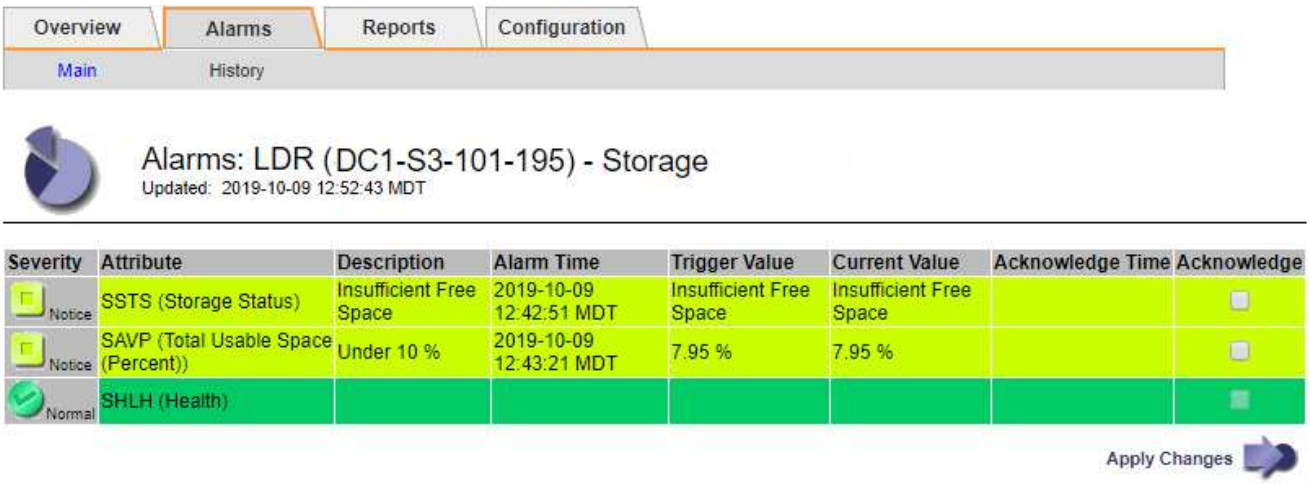
Por exemplo, suponha que o volume de armazenamento Soft Read-Only Watermark esteja definido como 10 GB, que é o valor padrão. O alarme SSTS é acionado se menos de 10 GB de espaço utilizável permanecer em cada volume de armazenamento no nó de armazenamento. Se algum dos volumes tiver 10 GB ou mais de espaço disponível, o alarme não será acionado.

Se um alarme SSTS tiver sido acionado, você pode seguir estes passos para entender melhor o problema.

Passos

1. Selecione **suporte Alarmes (legado) Alarmes atuais**.
2. Na coluna Serviço, selecione o data center, o nó e o serviço associados ao alarme SSTS.

   É apresentada a página Grid Topology (topologia de grelha). A guia Alarmes mostra os alarmes ativos para o nó e serviço selecionados.



Overview | Alarms | Reports | Configuration
Main | History

Alarms: LDR (DC1-S3-101-195) - Storage
Updated: 2019-10-09 12:52:43 MDT

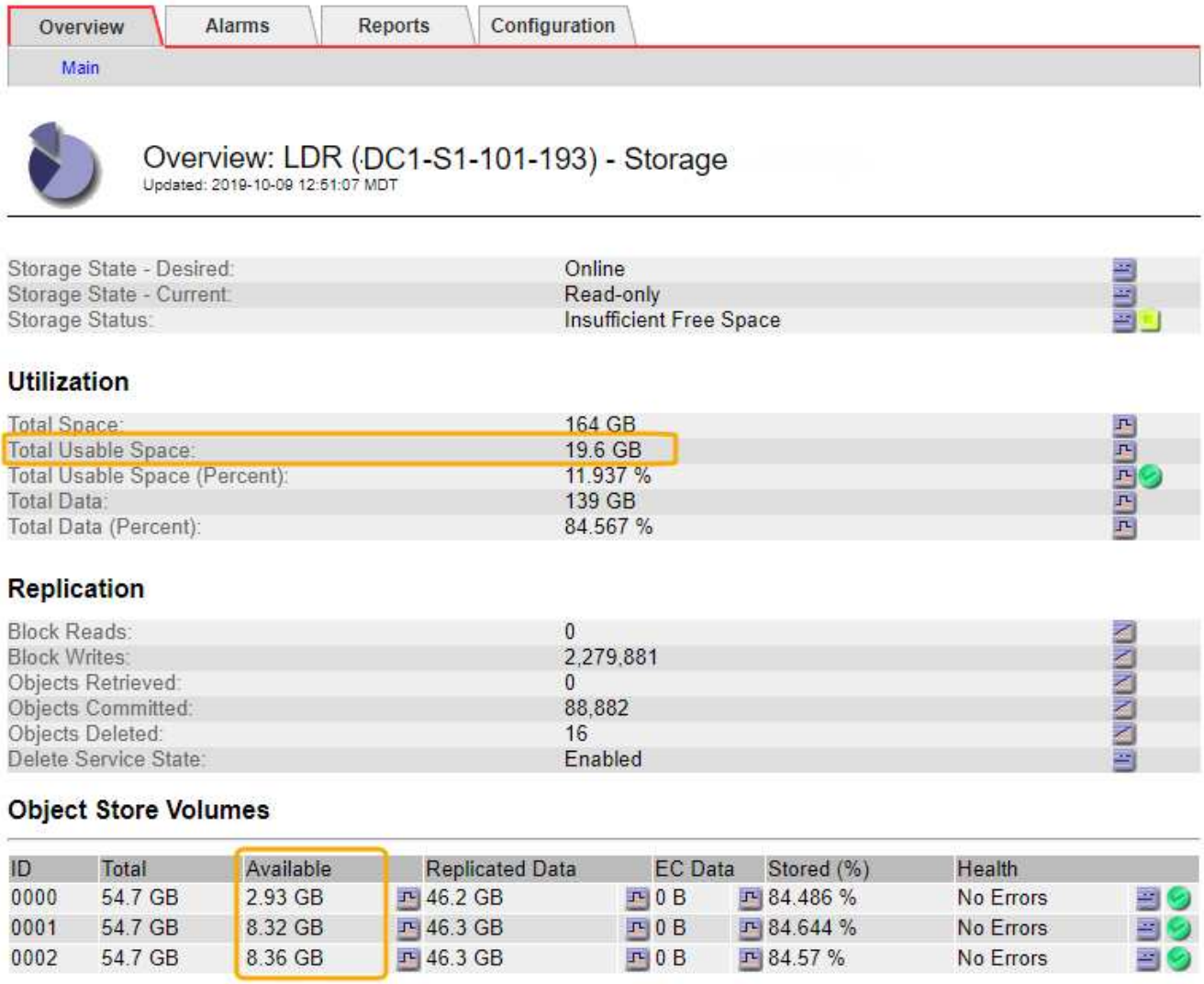
Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		
Normal	SHLH (Health)						

Apply Changes

   Neste exemplo, os alarmes SSTS (Storage Status) e SAVP (Total usable Space (Percent)) foram acionados no nível de Aviso.

Normalmente, tanto o alarme SSTS como o alarme SAVP são acionados aproximadamente ao mesmo tempo; no entanto, se ambos os alarmes são acionados depende da definição da marca d'água em GB e da definição do alarme SAVP em percentagem.

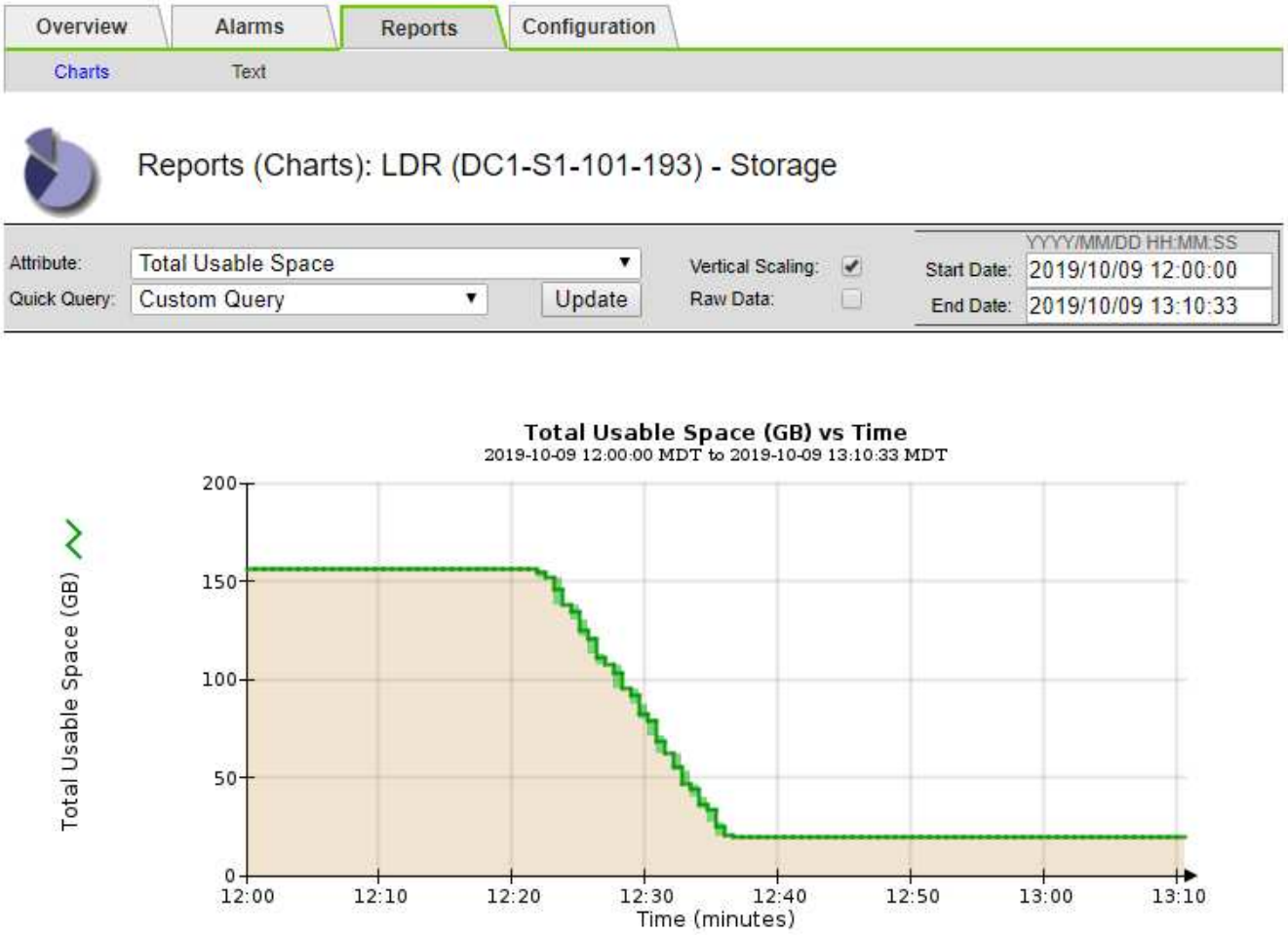
3. Para determinar quanto espaço utilizável está realmente disponível, selecione **LDR Storage Overview** e encontre o atributo espaço utilizável total (STAS).



Neste exemplo, apenas 19,6 GB dos 164 GB de espaço neste nó de armazenamento permanecem disponíveis. Observe que o valor total é a soma dos valores **disponíveis** para os três volumes de armazenamento de objetos. O alarme SSTS foi acionado porque cada um dos três volumes de armazenamento tinha menos de 10 GB de espaço disponível.

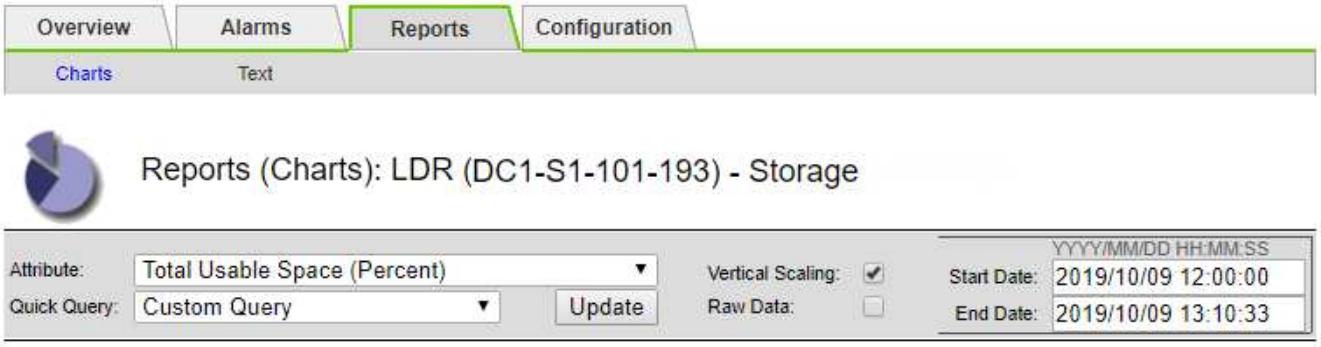
4. Para entender como o armazenamento foi usado ao longo do tempo, selecione a guia **relatórios** e plote o espaço utilizável total nas últimas horas.

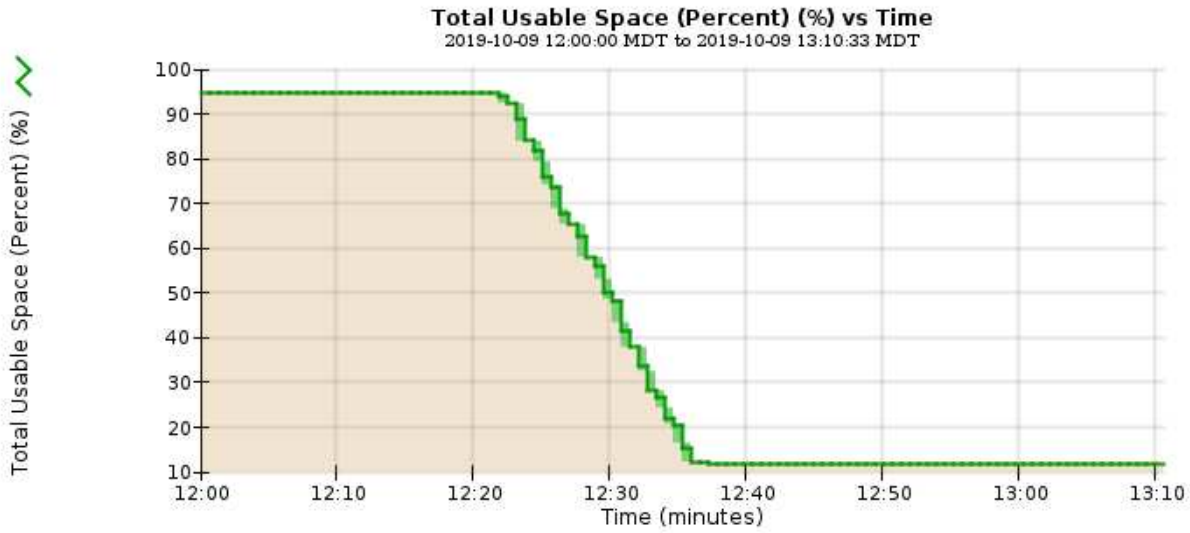
   Neste exemplo, o espaço utilizável total caiu de cerca de 155 GB em 12:00 para 20 GB em 12:35, o que corresponde ao momento em que o alarme SSTS foi acionado.



5. Para entender como o armazenamento está sendo usado como uma porcentagem do total, plote o espaço utilizável total (porcentagem) nas últimas horas.

   Neste exemplo, o espaço utilizável total caiu de 95% para pouco mais de 10%, aproximadamente ao mesmo tempo.





6. Conforme necessário, adicione capacidade de storage expandindo o sistema StorageGRID.

   Para obter procedimentos sobre como gerenciar um nó de armazenamento completo, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Expanda sua grade"

"Administrar o StorageGRID"

Solução de problemas de entrega de mensagens de serviços da plataforma (alarme SMTT)

O alarme Total Events (SMTT) é acionado no Grid Manager se uma mensagem de serviço da plataforma for entregue a um destino que não possa aceitar os dados.

Sobre esta tarefa

Por exemplo, um upload multipart S3 pode ser bem-sucedido, mesmo que a replicação ou a mensagem de notificação associada não possa ser entregue ao endpoint configurado. Ou, uma mensagem para replicação do CloudMirror pode não ser entregue se os metadados forem muito longos.

O alarme SMTT contém uma mensagem de último evento que diz, `Failed to publish notifications for bucket-name object key` para o último objeto cuja notificação falhou.

Para obter informações adicionais sobre os serviços de plataforma de solução de problemas, consulte as

instruções de administração do StorageGRID. Talvez seja necessário acessar o locatário do Gerenciador do Locatário para depurar um erro de serviço de plataforma.

Passos

1. Para visualizar o alarme, selecione **nós *site grid node* Eventos**.
2. Veja o último evento na parte superior da tabela.

   As mensagens de evento também são listadas em `/var/local/log/bycast-err.log`.

3. Siga as orientações fornecidas no conteúdo do alarme SMTT para corrigir o problema.
4. Clique em **Redefinir contagens de eventos**.
5. Notificar o locatário dos objetos cujas mensagens de serviços da plataforma não foram entregues.
6. Instrua o locatário a acionar a replicação ou notificação com falha atualizando os metadados ou as tags do objeto.

Informações relacionadas

"Administrar o StorageGRID"

"Use uma conta de locatário"

"Referência de ficheiros de registo"

"Repor contagens de eventos"

Solução de problemas de metadados

Há várias tarefas que você pode executar para ajudar a determinar a origem dos problemas de metadados.

Solução de problemas do alerta de armazenamento de metadados baixos

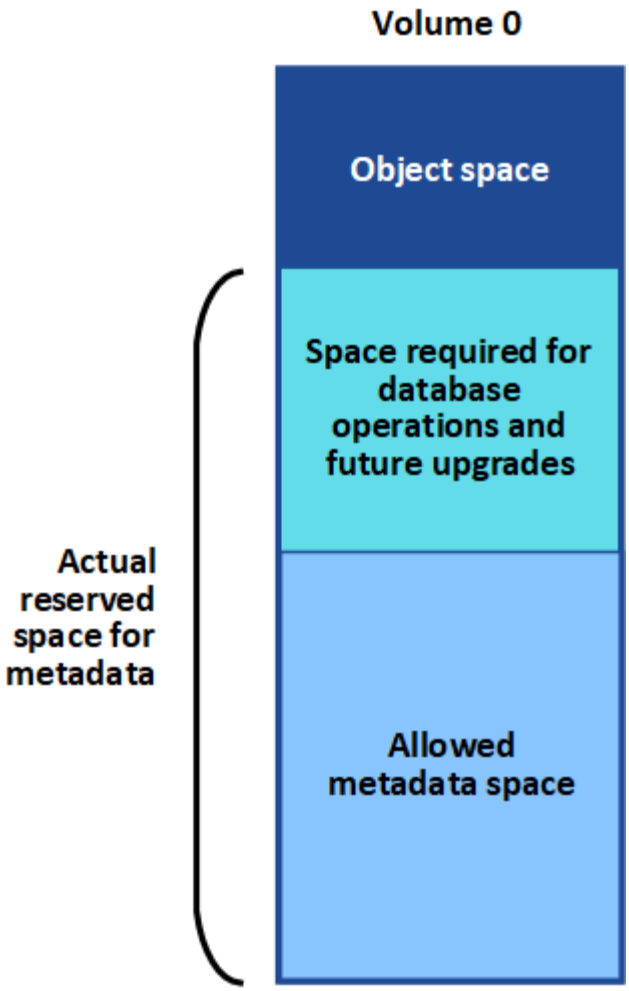
Se o alerta **armazenamento de metadados baixo** for acionado, você deverá adicionar novos nós de armazenamento.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

O StorageGRID reserva uma certa quantidade de espaço no volume 0 de cada nó de storage para metadados de objetos. Esse espaço é conhecido como espaço reservado real, e é subdividido no espaço permitido para metadados de objetos (o espaço permitido de metadados) e o espaço necessário para operações essenciais de banco de dados, como compactação e reparo. O espaço de metadados permitido rege a capacidade geral do objeto.



Se os metadados de objetos consumirem mais de 100% do espaço permitido para metadados, as operações do banco de dados não poderão ser executadas de forma eficiente e ocorrerão erros.

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 Dashboard. Se esse aviso for exibido, você deverá adicionar novos nós de storage imediatamente. Você nunca deve permitir que os metadados de objetos usem mais de 100% do espaço permitido.

- **Crítico**: Metadados de objetos estão usando 100% ou mais do espaço permitido de metadados e estão começando a consumir o espaço necessário para operações essenciais de banco de dados. Você deve interromper a ingestão de novos objetos e adicionar novos nós de storage imediatamente.

No exemplo a seguir, metadados de objetos estão usando mais de 100% do espaço permitido de metadados. Esta é uma situação crítica, o que resultará em erros e operações ineficientes do banco de dados.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.

Se o tamanho do volume 0 for menor do que a opção de armazenamento de espaço reservado de metadados (por exemplo, em um ambiente não-produção), o cálculo do alerta **armazenamento de metadados baixo** pode ser impreciso.

Passos

1. Selecione **Alertas 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 expandir 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.

Informações relacionadas

"Monitoramento da capacidade dos metadados de objetos para cada nó de storage"

"Expanda sua grade"

Solução de problemas dos Serviços: Status - alarme Cassandra (SVST)

O alarme Serviços: Status - Cassandra (SVST) indica que você pode precisar reconstruir o banco de dados Cassandra para um nó de armazenamento. O Cassandra é usado como o armazenamento de metadados do StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Se o Cassandra for interrompido por mais de 15 dias (por exemplo, o nó de armazenamento está desligado), o Cassandra não será iniciado quando o nó for colocado novamente on-line. Você deve reconstruir o banco de dados Cassandra para o serviço DDS afetado.

Você pode usar a página Diagnósticos para obter informações adicionais sobre o estado atual da grade.

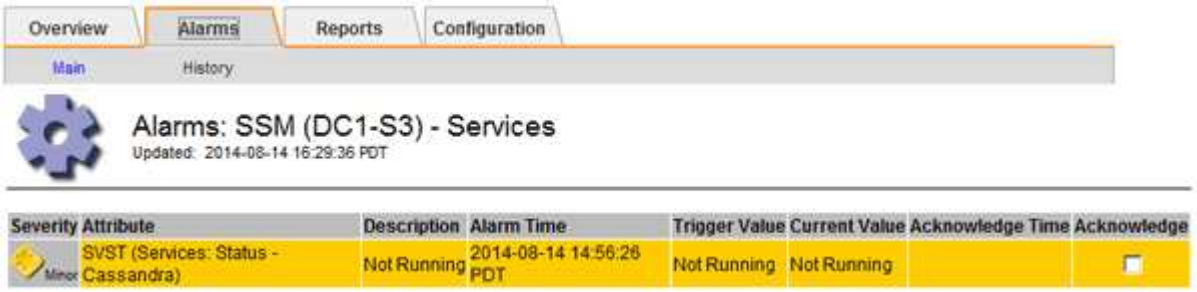
"A executar o diagnóstico"

Se dois ou mais serviços de banco de dados do Cassandra estiverem inativos por mais de 15 dias, entre em Contato com o suporte técnico e não prossiga com as etapas abaixo.

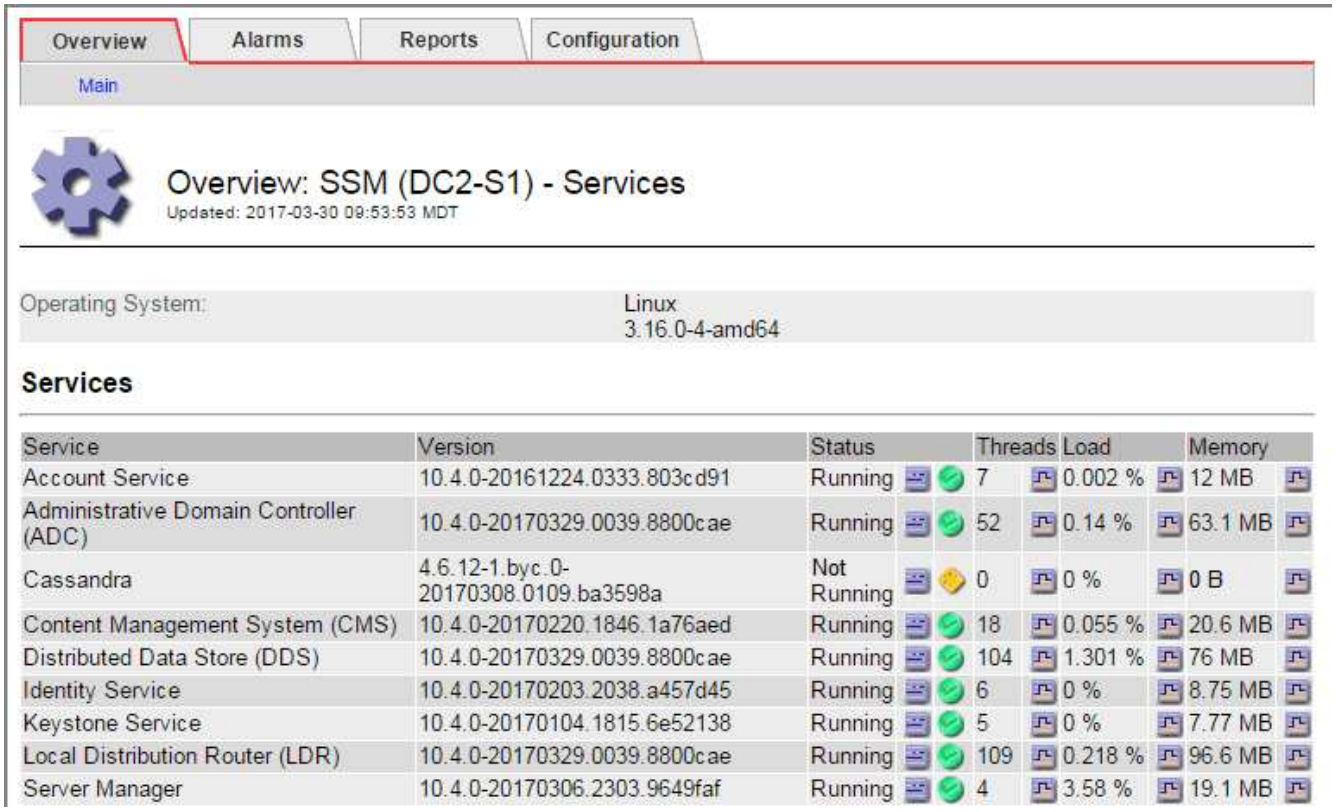
Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Site Storage Node*** **SSM Serviços Alarmes Main** para exibir alarmes.

   Este exemplo mostra que o alarme SVST foi acionado.



   A página principal dos Serviços de SSM também indica que o Cassandra não está em execução.



1. Tente reiniciar o Cassandra a partir do nó de storage:
   a. Faça login no nó da grade:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
   b. Introduza: `/etc/init.d/cassandra status`
   c. Se o Cassandra não estiver em execução, reinicie-o: `/etc/init.d/cassandra restart`
2. Se o Cassandra não reiniciar, determine quanto tempo o Cassandra esteve inativo. Se o Cassandra estiver inativo por mais de 15 dias, você deverá reconstruir o banco de dados do Cassandra.

   Se dois ou mais serviços de banco de dados do Cassandra estiverem inoperantes, entre em Contato com o suporte técnico e não prossiga com as etapas abaixo.

   Você pode determinar por quanto tempo o Cassandra ficou para baixo, traçando-o ou revisando o arquivo servermanager.log.

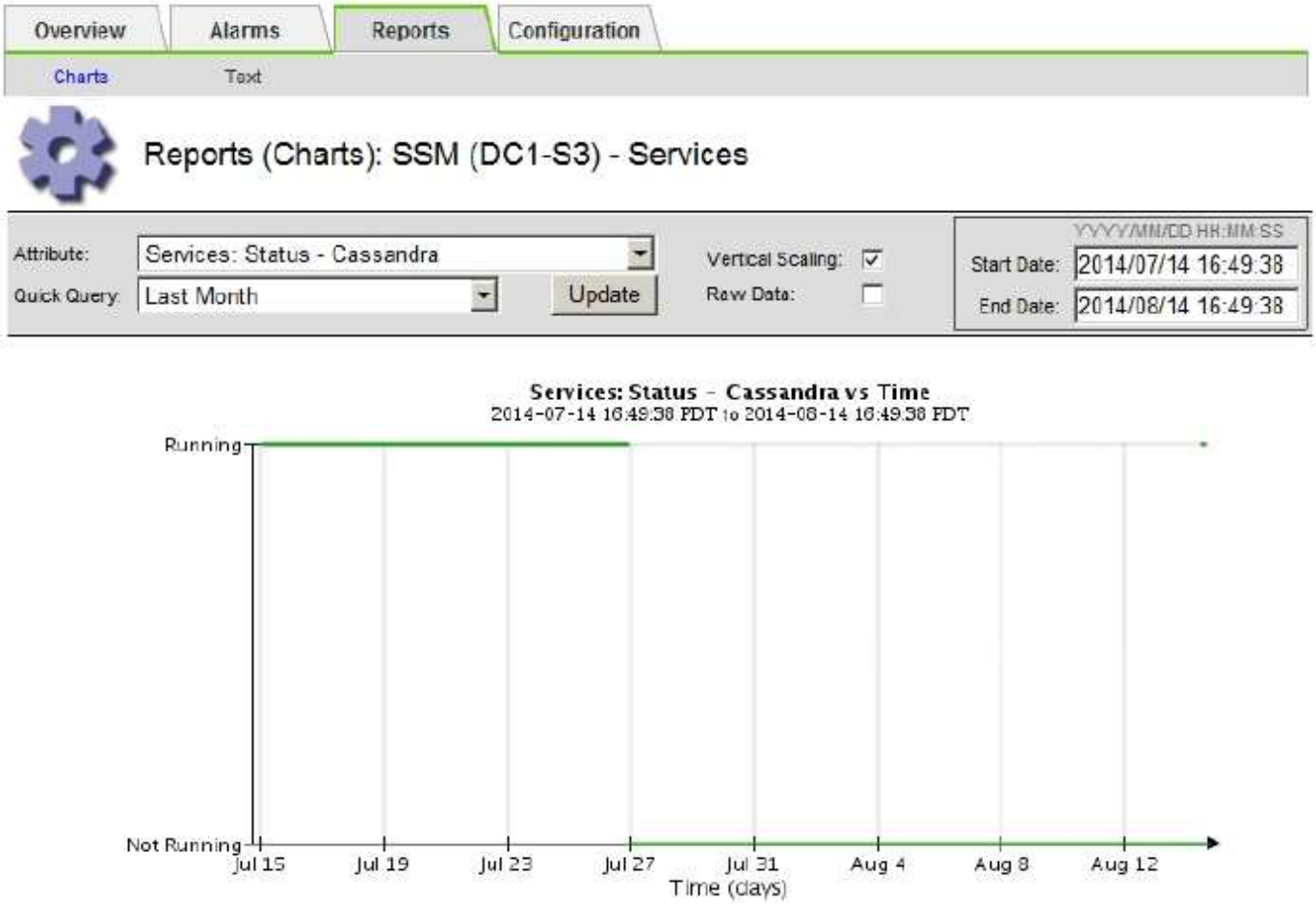
3. Para traçar o gráfico Cassandra:
   a. Selecione **Support Tools Grid Topology**. Em seguida, selecione ***site Storage Node* SSM Serviços relatórios gráficos**.
   b. Selecione **Atributo Serviço: Status - Cassandra**.
   c. Para **Data de Início**, insira uma data que seja pelo menos 16 dias antes da data atual. Para **Data de**

fim, insira a data atual.

d. Clique em **Atualizar**.

e. Se o gráfico mostrar que o Cassandra está inativo por mais de 15 dias, reconstrua o banco de dados do Cassandra.

O exemplo de gráfico a seguir mostra que o Cassandra esteve inativo por pelo menos 17 dias.



1. Para analisar o arquivo servermanager.log no nó de storage:

   a. Faça login no nó da grade:

      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      iii. Digite o seguinte comando para mudar para root: `su -`

      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

   b. Introduza: `cat /var/local/log/servermanager.log`

      O conteúdo do arquivo servermanager.log é exibido.

      Se o Cassandra estiver inativo por mais de 15 dias, a seguinte mensagem é exibida no arquivo servermanager.log:

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

a. Certifique-se de que o carimbo de data/hora desta mensagem é o momento em que você tentou reiniciar o Cassandra conforme instruído na etapa Reinicie o Cassandra a partir do nó de storage.

   Pode haver mais de uma entrada para Cassandra; você deve localizar a entrada mais recente.

b. Se o Cassandra estiver inativo por mais de 15 dias, você deverá reconstruir o banco de dados do Cassandra.

   Para obter instruções, consulte ""recuperação de um único nó de armazenamento para baixo mais de 15 dias"" nas instruções de recuperação e manutenção.

c. Entre em Contato com o suporte técnico se os alarmes não forem apagados após a reconstrução do Cassandra.

Informações relacionadas

"Manter recuperar"

Solução de problemas de erros de memória sem Cassandra (alarme SMTT)

Um alarme de Eventos totais (SMTT) é acionado quando o banco de dados Cassandra tem um erro de memória fora. Se este erro ocorrer, contacte o suporte técnico para resolver o problema.

Sobre esta tarefa

Se ocorrer um erro de falta de memória para o banco de dados do Cassandra, um despejo de heap é criado, um alarme de Eventos totais (SMTT) é acionado e a contagem de erros de memória do Cassandra é incrementada por um.

Passos

1. Para exibir o evento, selecione **nós *grid node* Eventos**.
2. Verifique se a contagem de erros de memória do Cassandra Heap é 1 ou superior.

   Você pode usar a página Diagnósticos para obter informações adicionais sobre o estado atual da grade.

   "A executar o diagnóstico"

3. Vá para `/var/local/core/`, compacte o `Cassandra.hprof` arquivo e envie-o para o suporte técnico.
4. Faça um backup do `Cassandra.hprof` arquivo e exclua-o do `/var/local/core/ directory`.

   Este arquivo pode ter até 24 GB, então você deve removê-lo para liberar espaço.

5. Quando o problema for resolvido, clique em **Redefinir contagens de eventos**.

   Para redefinir contagens de eventos, você deve ter a permissão Configuração de Página de topologia de Grade.

Informações relacionadas

"Repor contagens de eventos"

Solução de problemas de erros de certificado

Se você vir um problema de segurança ou certificado ao tentar se conetar ao StorageGRID usando um navegador da Web, um cliente S3 ou Swift ou uma ferramenta de monitoramento externa, você deve verificar o certificado.

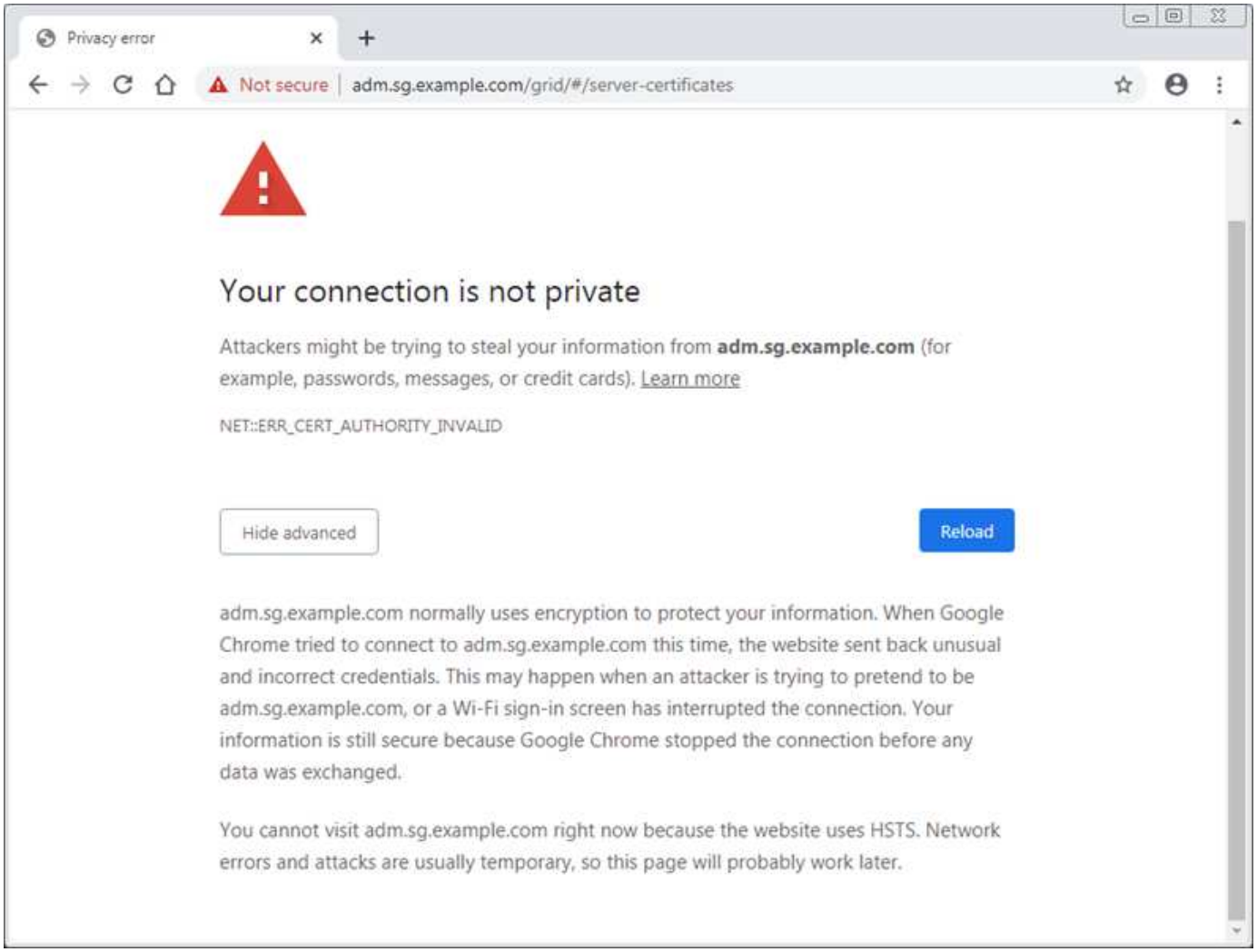
Sobre esta tarefa

Os erros de certificado podem causar problemas quando você tenta se conetar ao StorageGRID usando o Gerenciador de Grade, a API de Gerenciamento de Grade, o Gerenciador de Locatário ou a API de Gerenciamento de Locatário. Erros de certificado também podem ocorrer quando você tenta se conetar com um cliente S3 ou Swift ou ferramenta de monitoramento externa.

Se você estiver acessando o Gerenciador de Grade ou o Gerenciador de locatário usando um nome de domínio em vez de um endereço IP, o navegador mostrará um erro de certificado sem uma opção para ignorar se uma das seguintes situações ocorrer:

- O certificado do servidor de interface de gerenciamento personalizado expira.
- Você reverte de um certificado de servidor de interface de gerenciamento personalizado para o certificado de servidor padrão.

O exemplo a seguir mostra um erro de certificado quando o certificado do servidor 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 do servidor da interface de gerenciamento do StorageGRID ou por certificados de cliente. O alerta **expiração de certificados configurados na página certificados de cliente** é acionado quando um certificado de cliente está prestes a expirar.

Passos

1. Se você recebeu uma notificação de alerta sobre um certificado expirado, acesse os detalhes do certificado:
   - Para um certificado de servidor, selecione **Configuração Configurações de rede certificados de servidor**.
   - Para um certificado de cliente, selecione **Configuração Controle de Acesso certificados de Cliente**.
2. Verifique o período de validade do certificado.

   Alguns navegadores web e clientes S3 ou Swift não aceitam certificados com um período de validade superior a 398 dias.

3. Se o certificado tiver expirado ou expirar em breve, carregue ou gere um novo certificado.

- Para obter um certificado de servidor, consulte as etapas para configurar um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de Locatário nas instruções para administrar o StorageGRID.
- Para obter um certificado de cliente, consulte as etapas para configurar um certificado de cliente nas instruções para administrar o StorageGRID.

4. 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 **Configuração Configurações de rede certificados de servidor** para instalar um novo certificado personalizado ou continuar com o certificado padrão.
     iii. Nas instruções de administração do StorageGRID, consulte as etapas para configurar um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de Locatário.

Informações relacionadas

"Administrar o StorageGRID"

Solucionando problemas de nó de administração e interface do usuário

Existem várias tarefas que você pode executar para ajudar a determinar a origem dos problemas relacionados aos nós de administração e à interface de usuário do StorageGRID.

Solução de problemas de erros de logon

Se ocorrer um erro ao iniciar sessão num nó de administração do StorageGRID, o sistema poderá ter um problema com a configuração da federação de identidade, um problema de rede ou hardware, um problema com os serviços do nó de administração ou um problema com o banco de dados Cassandra nos nós de armazenamento conetados.

O que você vai precisar

- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Use estas diretrizes de solução de problemas se você vir qualquer uma das seguintes mensagens de erro ao tentar entrar em um nó de administrador:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Passos

1. Aguarde 10 minutos e tente iniciar sessão novamente.

   Se o erro não for resolvido automaticamente, vá para a próxima etapa.

2. Se o seu sistema StorageGRID tiver mais de um nó de administrador, tente fazer login no Gerenciador de Grade de outro nó de administrador.
   - Se você conseguir entrar, use as opções **Dashboard**, **Nodes**, **Alerts** e **Support** para ajudar a determinar a causa do erro.
   - Se você tiver apenas um nó Admin ou ainda não conseguir entrar, vá para a próxima etapa.
3. Determine se o hardware do nó está offline.
4. Se o logon único (SSO) estiver ativado para o sistema StorageGRID, consulte as etapas para configurar o logon único nas instruções de administração do StorageGRID.

   Talvez seja necessário desativar e reativar temporariamente o SSO para um único nó de administração para resolver quaisquer problemas.

   > ⓘ Se o SSO estiver ativado, você não poderá fazer logon usando uma porta restrita. Tem de utilizar a porta 443.

5. Determine se a conta que você está usando pertence a um usuário federado.

   Se a conta de usuário federada não estiver funcionando, tente fazer login no Gerenciador de Grade como um usuário local, como root.

   - Se o utilizador local puder iniciar sessão:
     i. Reveja todos os alarmes apresentados.
     ii. Selecione **Configuração Federação de identidade**.
     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 servidor web Apache está em execução: `# service apache2 status`

1. 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.

1. Reveja os seguintes registos:

   - `/var/local/log/bycast.log`
   - `/var/local/log/bycast-err.log`
   - `/var/local/log/nms.log`

◦ `**/*commands.txt`

2. Se você não conseguir identificar nenhum problema com o nó Admin, emita um dos seguintes comandos para determinar os endereços IP dos três nós de armazenamento que executam o serviço ADC em seu site. Em geral, esses são os primeiros três nós de storage instalados no local.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

Os nós de administração usam o serviço ADC durante o processo de autenticação.

3. A partir do nó Admin, efetue login em cada um dos nós de armazenamento ADC, usando os endereços IP identificados.
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

4. 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.

5. Repita as etapas Use Lumberjack para coletar logs e Rever registos para revisar os logs nos nós de storage.
6. Se você não conseguir resolver o problema, entre em Contato com o suporte técnico.

   Forneça os Registros que você coletou para o suporte técnico.

Informações relacionadas

"Administrar o StorageGRID"

"Referência de ficheiros de registo"

Solução de problemas na interface do usuário

Você pode ver problemas com o Gerenciador de Grade ou o Gerenciador do Locatário após atualizar para uma nova versão do software StorageGRID.

A interface Web não responde como esperado

O Gerenciador de Grade ou o Gerente do Locatário podem não responder como esperado depois que o software StorageGRID for atualizado.

Se você tiver problemas com a interface da Web:

- Certifique-se de que está a utilizar um browser suportado.

  > O suporte do navegador foi alterado para o StorageGRID 11,5. Confirme que está a utilizar uma versão suportada.

- Limpe o cache do navegador da Web.

  Limpar o cache remove recursos desatualizados usados pela versão anterior do software StorageGRID e permite que a interface do usuário funcione corretamente novamente. Para obter instruções, consulte a documentação do navegador da Web.

Informações relacionadas

"Requisitos do navegador da Web"

"Administrar o StorageGRID"

Verificando o status de um nó Admin indisponível

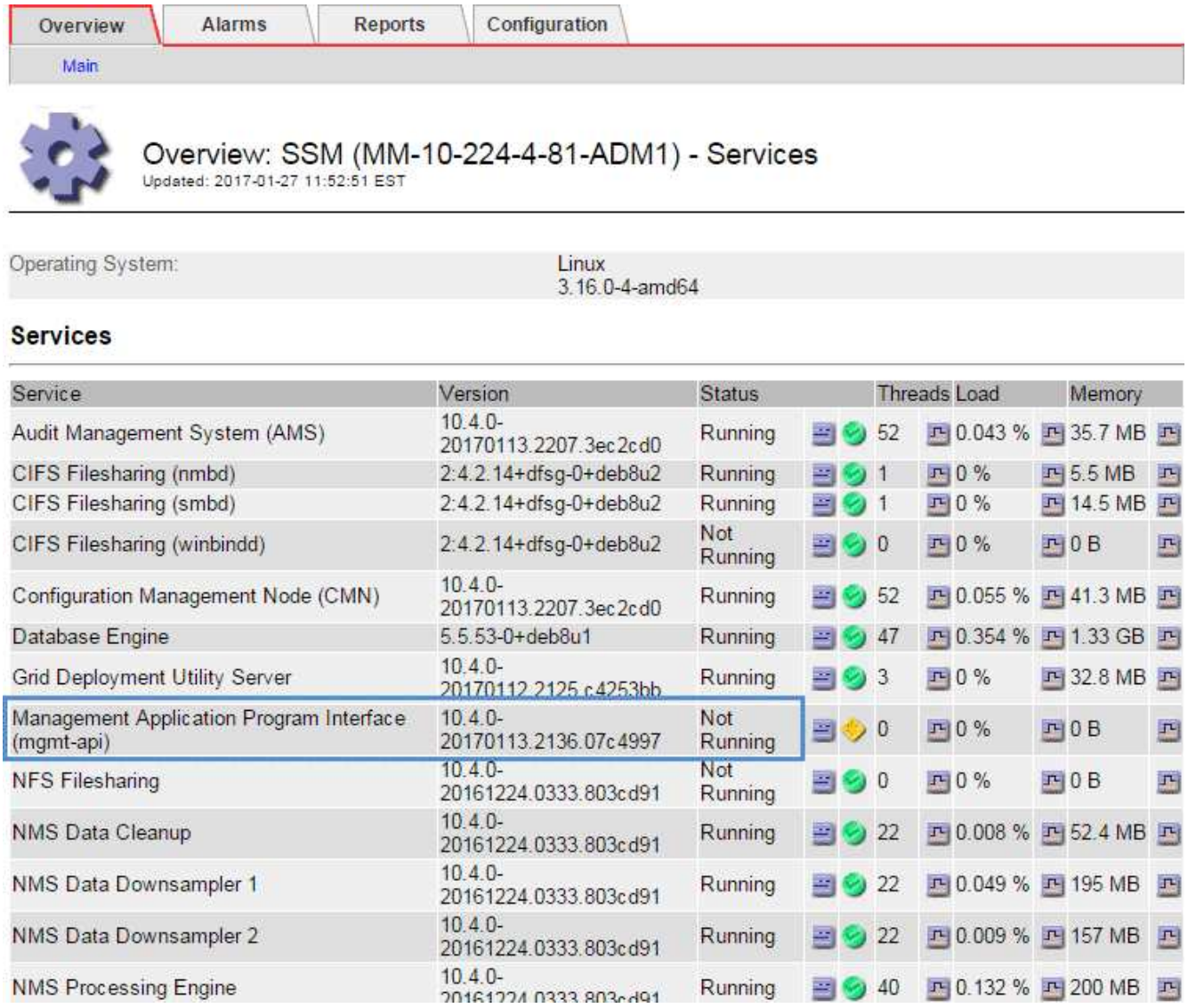
Se o sistema StorageGRID incluir vários nós de administração, você poderá usar outro nó de administração para verificar o status de um nó de administração indisponível.

O que você vai precisar

Você deve ter permissões de acesso específicas.

Passos

1. Em um nó Admin disponível, faça login no Gerenciador de Grade usando um navegador compatível.
2. Selecione **Support** > **Tools** > **Grid Topology**.
3. Selecione ***Site* nó Admin indisponível SSM Serviços Visão geral Principal**.
4. Procure serviços que tenham um status de não execução e que também possam ser exibidos em azul.



5. Determine se os alarmes foram acionados.
6. Tome as medidas apropriadas para resolver o problema.

Informações relacionadas

"Administrar o StorageGRID"

Solução de 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.

Solução de problemas de erros "'422: Entidade não processável'"

O erro 422: Entidade não processável pode ocorrer em várias circunstâncias. Verifique a mensagem de erro para determinar o que causou o problema.

Se você vir uma das mensagens de erro listadas, execute a ação recomendada.

Mensagem de erro	Causa raiz e ação corretiva

`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 uma das cifras suportadas pelo StorageGRID para conexões TLS de saída, como mostrado nas instruções de administração do StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Solução de problemas do alerta de incompatibilidade da MTU da rede de Grade

O alerta **Grid Network MTU mismatch** é acionado quando a configuração MTU (unidade máxima de transmissão) para a interface Grid Network (eth0) difere significativamente entre nós na grade.

Sobre esta tarefa

As diferenças nas configurações de MTU podem indicar que algumas, mas não todas, redes eth0 são

configuradas para quadros jumbo. Uma incompatibilidade de tamanho da MTU superior a 1000 pode causar problemas de desempenho da rede.

Passos

1. Liste as configurações de MTU para eth0 em todos os nós.
   - Use a consulta fornecida no Gerenciador de Grade.
   - Navegue para *`primary Admin Node IP address`*`/metrics/graph` e insira a seguinte consulta: `node_network_mtu_bytes{interface='eth0'}`
2. Modifique as configurações de MTU conforme necessário para garantir que elas sejam as mesmas para a interface de rede de Grade (eth0) em todos os nós.
   - Para os nós do dispositivo, consulte as instruções de instalação e manutenção do seu dispositivo.
   - Para nós baseados em Linux e VMware, use o seguinte comando: `/usr/sbin/change-mtu.py [-h] [-n node] mtu network [network...]`

     Exemplo: `change-mtu.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-mtu.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.

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

Resolução de problemas do alarme Network Receive Error (NRER)

Os alarmes de erro de receção de rede (NRER) podem ser causados por problemas de conetividade entre o StorageGRID e o hardware da rede. Em alguns casos, erros NRER podem ser claros sem intervenção manual. Se os erros não forem claros, execute as ações recomendadas.

Sobre esta tarefa

Os alarmes NRER podem ser causados pelos seguintes problemas com o hardware de rede que se coneta ao StorageGRID:

- A correção de erro de avanço (FEC) é necessária e não está em uso
- Incompatibilidade da MTU da porta do switch e da NIC
- Altas taxas de erro de link
- Buffer de anel NIC excedido

Passos

1. Siga as etapas de solução de problemas para todas as possíveis causas do alarme NRER, dada a configuração da rede.

   - Se o erro for causado por incompatibilidade de FEC, execute as seguintes etapas:

     Nota: Estas etapas são aplicáveis apenas para erros NRER causados por incompatibilidade FEC em aparelhos StorageGRID.

     i. Verifique o status do FEC da porta no switch conetado ao seu dispositivo StorageGRID.

     ii. Verifique a integridade física dos cabos do aparelho ao interrutor.

     iii. Se pretender alterar as definições do FEC para tentar resolver o alarme NRER, certifique-se primeiro de que o aparelho está configurado para o modo **Auto** na página Configuração de ligação do Instalador de dispositivos StorageGRID (consulte as instruções de instalação e manutenção do seu aparelho). Em seguida, altere as configurações do FEC nas portas do switch. As portas do dispositivo StorageGRID ajustarão suas configurações FEC para corresponder, se possível.

     (Não é possível configurar as definições FEC nos dispositivos StorageGRID. Em vez disso, os aparelhos tentam descobrir e espelhar as configurações FEC nas portas do switch às quais estão 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 comum de FEC, a rede voltará ao modo "no-FEC". Quando o FEC não está ativado, as conexões são mais suscetíveis a erros causados por ruído elétrico.)

     Nota: A StorageGRID Appliances apoia a FEC (FC) e a FEC (RS), bem como a FEC.

   - Se o erro for causado por uma falha de correspondência entre a porta do switch e a MTU da NIC, verifique se o tamanho da MTU configurado no nó é o mesmo que a configuração da MTU para a porta do switch.

     O tamanho da MTU configurado no nó pode ser menor do que a configuração na porta do switch à qual o nó está conetado. Se um nó StorageGRID receber um quadro Ethernet maior que o MTU, o que é possível com esta configuração, o alarme NRER pode ser comunicado. Se você acredita que isso

está acontecendo, altere a MTU da porta do switch para corresponder à MTU da interface de rede da StorageGRID ou altere a MTU da interface de rede StorageGRID para corresponder à porta do switch, dependendo dos seus objetivos ou requisitos de MTU de ponta a ponta.

> Para obter o melhor desempenho de rede, todos os nós devem ser configurados com valores MTU semelhantes em suas interfaces de rede de Grade. O alerta **incompatibilidade de MTU da rede de Grade** é acionado se houver uma diferença significativa nas configurações de MTU para a rede de Grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede.

> Para alterar a definição MTU, consulte o guia de instalação e manutenção do seu aparelho.

- Se o erro for causado por altas taxas de erro de link, execute as seguintes etapas:
  i. Ative o FEC, se ainda não estiver ativado.
  ii. Verifique se o cabeamento de rede é de boa qualidade e não está danificado ou conetado incorretamente.
  iii. Se os cabos parecerem não ser o problema, contacte o suporte técnico.

  > Você pode notar altas taxas de erro em um ambiente com alto ruído elétrico.

- Se o erro for uma sobrecarga do buffer do anel da NIC, entre em Contato com o suporte técnico.

  O buffer de anel pode ser excedido quando o sistema StorageGRID está sobrecarregado e não consegue processar eventos de rede em tempo hábil.

2. Depois de resolver o problema subjacente, redefina o contador de erros.
   a. Selecione **Support** > **Tools** > **Grid Topology**.
   b. Selecione ***site grid node*** **SSM Resources Configuration Main**.
   c. Selecione **Redefinir contagem de erros de recebimento** e clique em **aplicar alterações**.

Informações relacionadas

"Solução de problemas do alerta de incompatibilidade da MTU da rede de Grade"

"Referência de alarmes (sistema legado)"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Aparelhos de serviços SG100 SG1000"

Solução de problemas de sincronização de tempo

Você pode ver problemas com a sincronização de tempo em sua grade.

Se você encontrar problemas de sincronização de tempo, verifique se você especificou pelo menos quatro fontes de NTP externas, cada uma fornecendo uma referência estrato 3 ou melhor, e se todas as fontes de NTP externas estão operando normalmente e são acessíveis por seus nós de StorageGRID.

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

Informações relacionadas

"Manter recuperar"

Linux: Problemas de conetividade de rede

Você pode ver problemas com a conetividade de rede para nós de grade StorageGRID hospedados em hosts Linux.

Clonagem de endereços MAC

Em alguns casos, os problemas de rede podem ser resolvidos usando a clonagem de endereços MAC. Se você estiver usando hosts virtuais, defina o valor da chave de clonagem de endereços MAC para cada uma de suas redes como "verdadeiro" no arquivo de configuração do nó. Esta configuração faz com que o endereço MAC do contentor StorageGRID use o endereço MAC do host. Para criar arquivos de configuração de nó, consulte as instruções no guia de instalação da sua plataforma.

Crie interfaces de rede virtuais separadas para uso pelo sistema operacional host Linux. Usar as mesmas interfaces de rede para o sistema operacional host Linux e o contentor StorageGRID pode fazer com que o sistema operacional do host se torne inacessível se o modo promíscuo não tiver sido ativado no hypervisor.

Para obter mais informações sobre como ativar a clonagem MAC, consulte as instruções no guia de instalação da sua plataforma.

Modo promíscuo

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

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Linux: O status do nó é "órfão"

Um nó Linux em um estado órfão geralmente indica que o serviço StorageGRID ou o daemon de nó StorageGRID que controla o contentor do nó morreram inesperadamente.

Sobre esta tarefa

Se um nó Linux relata que ele está em um estado órfão, você deve:

- Verifique os logs para ver se há erros e mensagens.

- Tente iniciar o nó novamente.
- Se necessário, use comandos Docker para parar o contentor de 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 contentor Docker e qualquer processo de controle do StorageGRID-node:`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).

   ```
   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
   ```

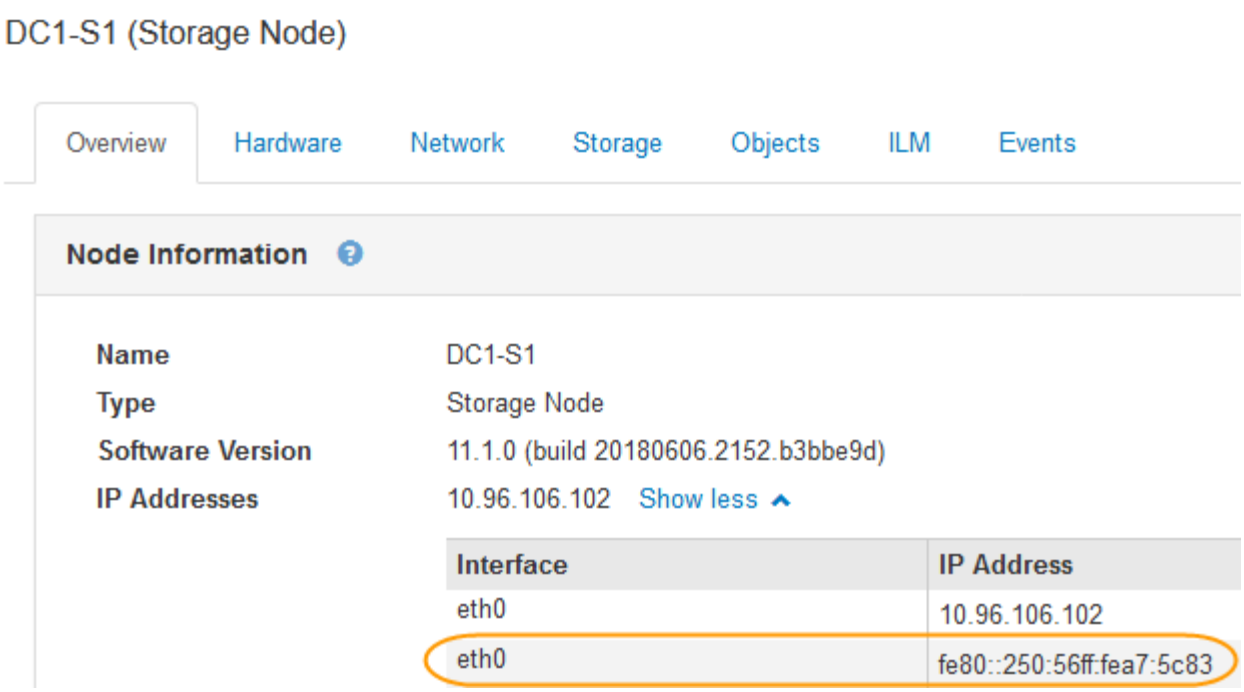
Linux: Solução de problemas de suporte IPv6

Talvez seja necessário habilitar o suporte IPv6 no kernel se você tiver instalado nós do StorageGRID em hosts Linux e notar que os endereços IPv6 não foram atribuídos aos contentores do nó como esperado.

Sobre esta tarefa

Você pode ver o endereço IPv6 que foi atribuído a um nó de grade nos seguintes locais no Gerenciador de Grade:

- Selecione **nós** e selecione o nó. Em seguida, clique em **Mostrar mais** ao lado de **endereços IP** na guia Visão geral.



- Selecione **Support Tools Grid Topology**. Em seguida, selecione ***node* SSM Resources**. Se um endereço IPv6 tiver sido atribuído, ele será listado abaixo do endereço IPv4 na seção **endereços de rede**.

Se o endereço IPv6 não for exibido e o nó estiver instalado em um host Linux, siga estas etapas para habilitar o suporte a IPv6 no kernel.

Passos

1. Faça login no host como root ou usando uma conta com permissão sudo.
2. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

O resultado deve ser 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

Se o resultado não for 0, consulte a documentação do sistema operacional para alterar `sysctl` as configurações. Em seguida, altere o valor para 0 antes de continuar.

3. Insira o contentor do nó StorageGRID: `storagegrid node enter node-name`
4. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

O resultado deve ser 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

Se o resultado não for 1, este procedimento não se aplica. Entre em Contato com o suporte técnico.

5. Saia do recipiente: `exit`

```
root@DC1-S1:~ # exit
```

6. Como root, edite o seguinte arquivo: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localize as duas linhas a seguir e remova as tags de comentário. Em seguida, salve e feche o arquivo.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Execute estes comandos para reiniciar o contentor StorageGRID:

```
storagegrid node stop node-name
```

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

Rever registos de auditoria

Conheça os logs de auditoria do sistema StorageGRID e veja uma lista de todas as mensagens de auditoria.

- "Visão geral da mensagem de auditoria"
- "Faça auditoria de arquivos de log e formatos de mensagens"
- "Auditar mensagens e o ciclo de vida do objeto"
- "Auditar mensagens"

Visão geral da mensagem de auditoria

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.

Presume-se que você tenha uma boa compreensão da natureza das atividades auditadas dentro do sistema StorageGRID. Para usar o arquivo de log de texto, você deve ter acesso ao compartilhamento de auditoria configurado no nó Admin.

Informações relacionadas

"Administrar o StorageGRID"

Auditoria de fluxo e retenção de mensagens

Todos os serviços StorageGRID geram mensagens de auditoria durante a operação normal do sistema. Você deve entender como essas mensagens de auditoria se movem pelo sistema StorageGRID para `audit.log` o arquivo.

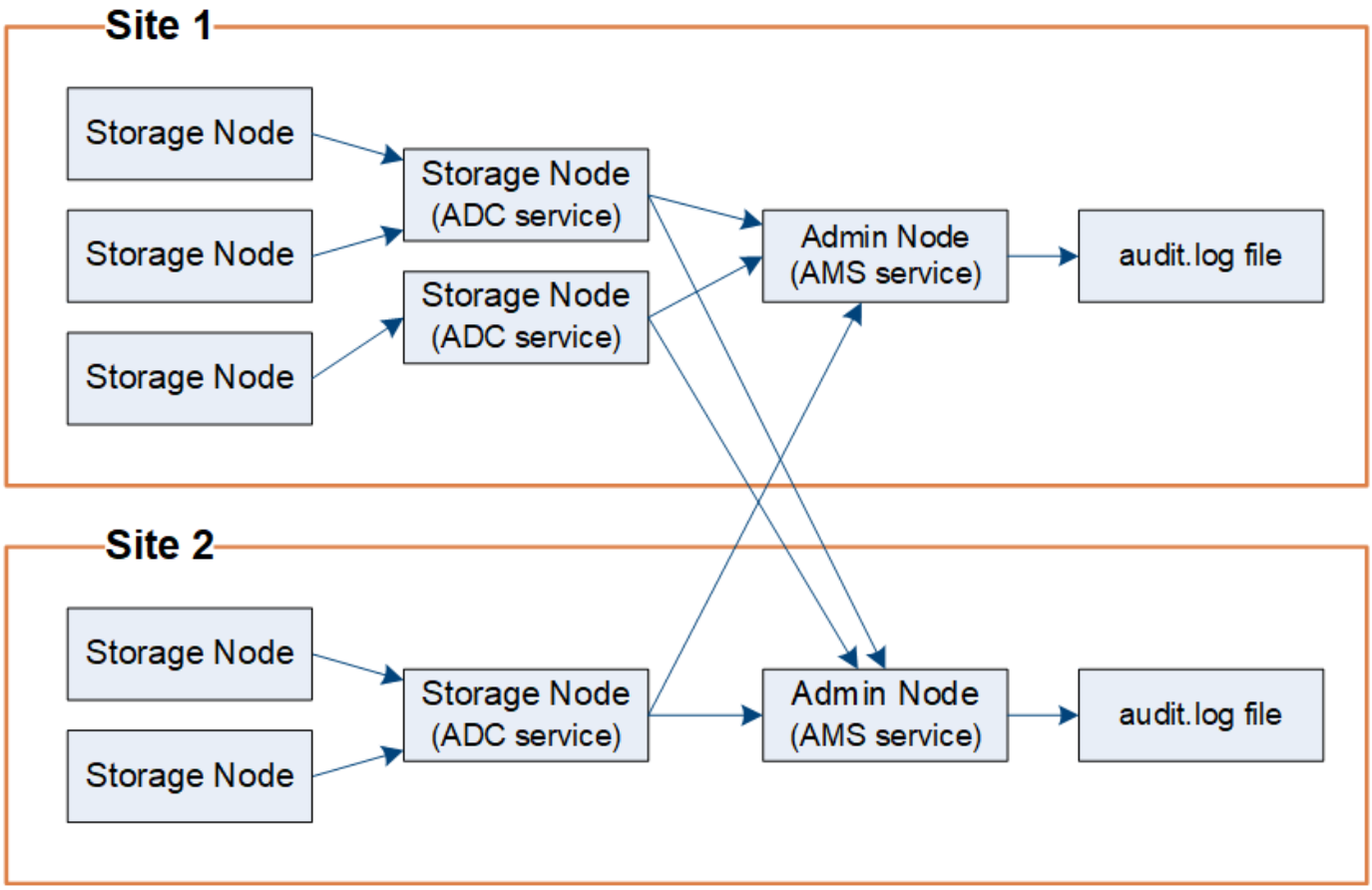
Auditoria do fluxo de mensagens

As mensagens de auditoria são processadas pelos nós de administração e pelos nós de armazenamento que têm um serviço de controlador de domínio administrativo (ADC).

Conforme mostrado no diagrama de fluxo de mensagens de auditoria, cada nó StorageGRID envia suas mensagens de auditoria para um dos serviços ADC no local do data center. O serviço ADC é ativado automaticamente para os três primeiros nós de storage instalados em cada local.

Por sua vez, cada serviço ADC atua como um relé e envia sua coleção de mensagens de auditoria para cada nó de administração no sistema StorageGRID, o que dá a cada nó de administração um Registro completo da atividade do sistema.

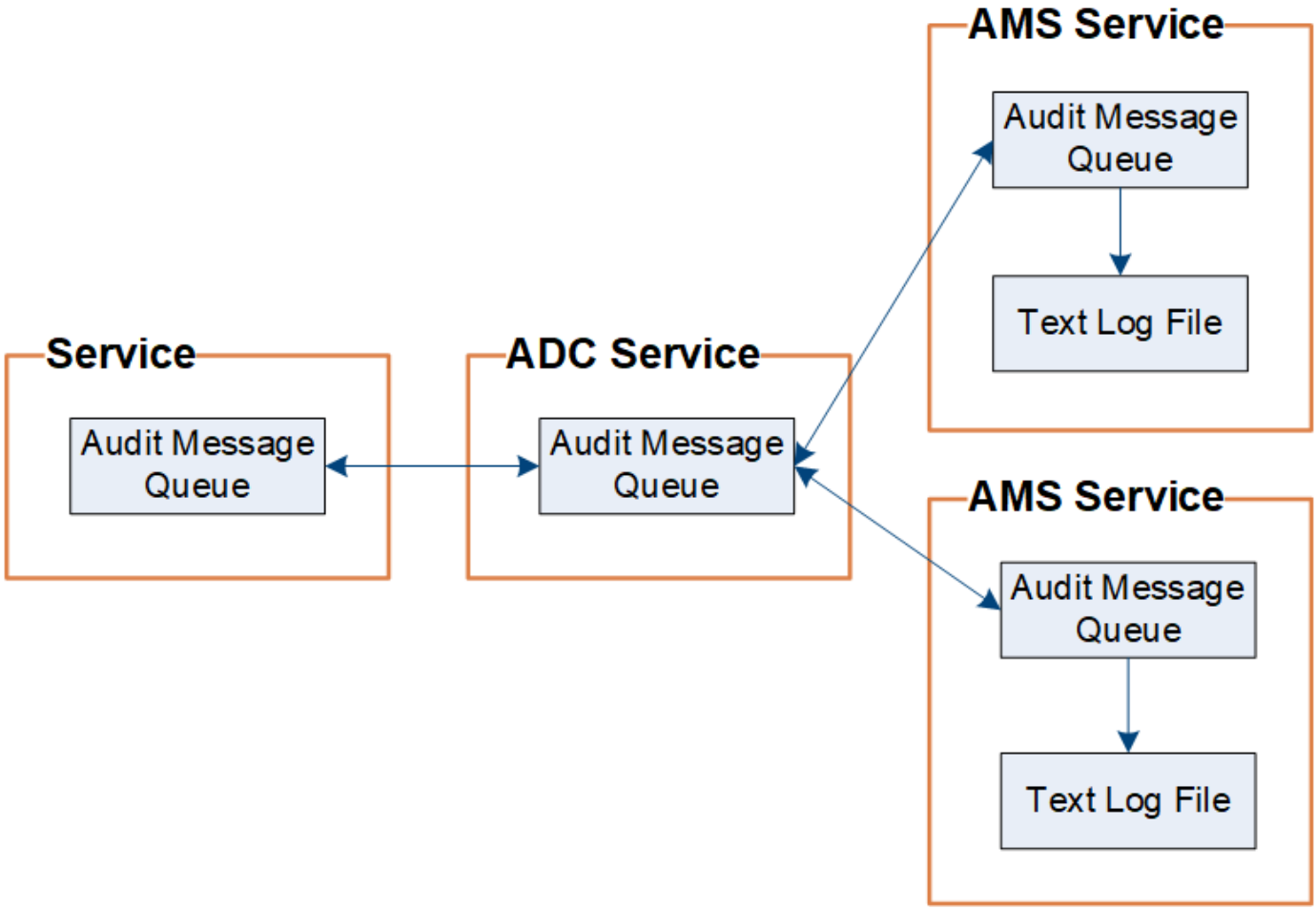
Cada nó Admin armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é `audit.log` nomeado .



Retenção de mensagens de auditoria

O StorageGRID usa um processo de cópia e exclusão para garantir que nenhuma mensagem de auditoria seja perdida antes que ela possa ser gravada no log de auditoria.

Quando um nó gera ou retransmite uma mensagem de auditoria, a mensagem é armazenada em uma fila de mensagens de auditoria no disco do sistema do nó da grade. Uma cópia da mensagem é sempre mantida em uma fila de mensagens de auditoria até que a mensagem seja gravada no arquivo de log de auditoria no diretório do Admin Node `/var/local/audit/export`. Isso ajuda a evitar a perda de uma mensagem de auditoria durante o transporte.



A fila de mensagens de auditoria pode aumentar temporariamente devido a problemas de 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/audit/export` diretório usado por um nó Admin ficar cheio, o nó Admin será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações de clientes S3 e Swift não são afetadas. O alarme XAMS (Unreachable Audit Repositories) é acionado quando um repositório de auditoria é inacessível.
- Se o `/var/local/` diretório usado por um nó de armazenamento com o serviço ADC ficar 92% cheio, o nó será sinalizado como indisponível para auditar mensagens até que o diretório esteja apenas 87% cheio. As solicitações de clientes S3 e Swift para outros nós não são afetadas. O alarme NRLY (relés de auditoria disponíveis) é acionado quando os relés de auditoria não são alcançáveis.

> ⓘ Se não houver nós de armazenamento disponíveis com o serviço ADC, os nós de armazenamento armazenam as mensagens de auditoria localmente.

- Se o `/var/local/` diretório usado por um nó de armazenamento ficar 85% cheio, o nó começará a recusar solicitações de cliente S3 e Swift com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria cresçam muito

grandes:

- A interrupção de um nó de administração ou de um nó de storage com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes podem ficar com backlogged.
- Uma taxa de atividade contínua que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC se torna cheio por razões não relacionadas às mensagens de auditoria. Quando isso acontece, o nó pára de aceitar novas mensagens de auditoria e prioriza seu backlog atual, o que pode causar backlogs em outros nós.

Alerta de fila de auditoria grande e alarme de mensagens de auditoria enfileiradas (AMQS)

Para ajudá-lo a monitorar o tamanho das filas de mensagens de auditoria ao longo do tempo, o alerta **fila de auditoria grande** e o alarme AMQS legado são acionados quando o número de mensagens em uma fila de nó de armazenamento ou fila de nó de administrador atinge determinados limites.

Se o alerta **fila de auditoria grande** ou o alarme AMQS legado for acionado, comece verificando a carga no sistema - se houver um número significativo de transações recentes, o alerta e o alarme devem ser resolvidos com o tempo e podem ser ignorados.

Se o alerta ou o alarme persistir e aumentar a gravidade, veja um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para gravações do cliente e leituras do cliente para erro ou Desativado. Consulte "'Alteração dos níveis de mensagens de auditoria"."

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.

Alteração dos níveis de mensagens de auditoria

Você pode ajustar os níveis de auditoria para aumentar ou diminuir o número de mensagens de auditoria registradas no log de auditoria para cada categoria de mensagens de auditoria.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

As mensagens de auditoria registradas no log de auditoria são filtradas com base nas configurações da página **Configuração** > **Monitoramento** > **Auditoria**.

Você pode definir um nível de auditoria diferente para cada uma das seguintes categorias de mensagens:

- **Sistema**: Por padrão, esse nível é definido como normal.
- **Armazenamento**: Por padrão, esse nível é definido como erro.
- **Gerenciamento**: Por padrão, esse nível é definido como normal.
- **Leitura do cliente**: Por padrão, esse nível é definido como normal.

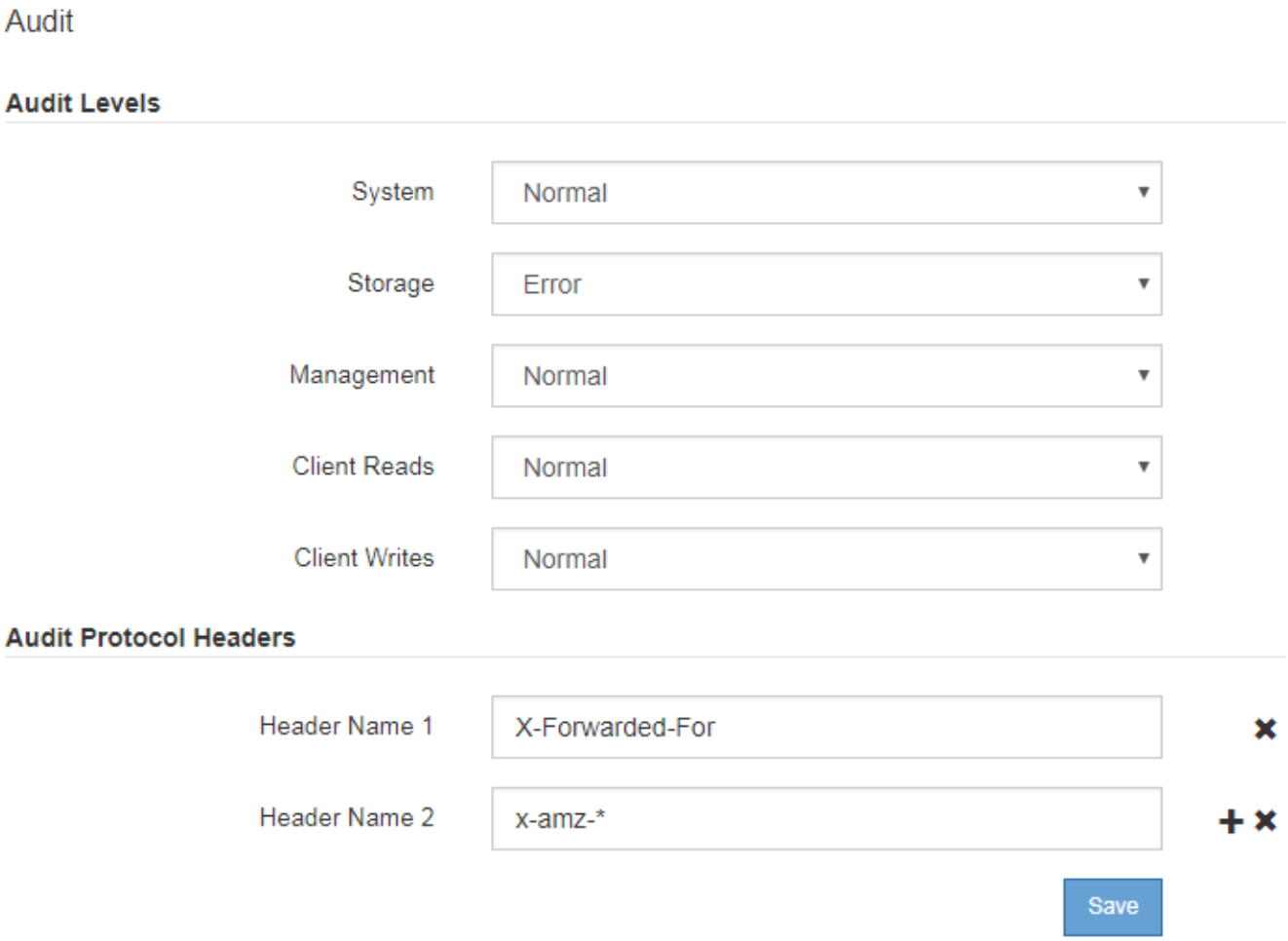
- * Gravações do cliente*: Por padrão, esse nível é definido como normal.

Esses padrões se aplicam se você instalou inicialmente o StorageGRID usando a versão 10,3 ou posterior. Se você atualizou de uma versão anterior do StorageGRID, o padrão para todas as categorias é definido como normal.

Durante as atualizações, as configurações de nível de auditoria não entrarão em vigor imediatamente.

Passos

1. Selecione **Configuração** > **Monitoramento** > **Auditoria**.



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).

Nível de auditoria	Descrição
Normal	As mensagens transacionais padrão são registradas - as mensagens listadas nestas instruções para a categoria.
Depurar	Obsoleto. Este nível comporta-se da mesma forma que o nível normal de auditoria.

As mensagens incluídas para qualquer nível particular incluem aquelas que seriam registradas nos níveis mais altos. Por exemplo, o nível normal inclui todas as mensagens de erro.

3. Em **Audit Protocol Headers**, insira o nome dos cabeçalhos de solicitação HTTP a serem incluídos nas mensagens de auditoria de leitura de cliente e gravação de cliente. Use um asterisco (**) como um curinga ou use a sequência de escape (**) como um asterisco literal. Clique no sinal de mais para criar uma lista de campos de nome de cabeçalho.

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

   Quando esses 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**.

4. Clique em **Salvar**.

Informações relacionadas

"Mensagens de auditoria do sistema"

"Mensagens de auditoria de armazenamento de objetos"

"Mensagem de auditoria de gerenciamento"

"O cliente lê mensagens de auditoria"

"Administrar o StorageGRID"

Acessando 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. Para facilitar o acesso aos logs de auditoria, você pode configurar o acesso do cliente para compartilhamentos de auditoria para NFS e CIFS (obsoleto). Você também pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:

   ```
   cd /var/local/audit/export
   ```

3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

Informações relacionadas

"Administrar o StorageGRID"

Rotação do arquivo de log de auditoria

Os arquivos de logs de auditoria são salvos no diretório de um nó de administrador `/var/local/audit/export`. Os arquivos de log de auditoria ativos são `audit.log` nomeados .

Uma vez por dia, o arquivo ativo `audit.log` é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato *`yyyy-mm-dd.txt`*. Se mais de um log de auditoria for criado em um único dia, os nomes de arquivo usarão a data em que o arquivo foi salvo, anexado por um número, no formato *`yyyy-mm-dd.txt.n`*. Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são os primeiros e segundos arquivos de log criados e salvos em 15 de abril de 2018.

Após um dia, o arquivo salvo é compactado e renomeado, no formato *`yyyy-mm-dd.txt.gz`*, que preserva a data original. Com o tempo, isso resulta no consumo de storage alocado para logs de auditoria no nó Admin. Um script monitora o consumo de espaço do log de auditoria e exclui arquivos de log conforme necessário para liberar espaço no `/var/local/audit/export` diretório. Os logs de auditoria são excluídos com base na data em que foram criados, sendo os mais antigos excluídos primeiro. Você pode monitorar as ações do script no seguinte arquivo: `/var/local/log/manage-audit.log`.

Este exemplo mostra o `audit.log` ficheiro ativo, o ficheiro do dia anterior (`2018-04-15.txt`) e o ficheiro comprimido para o dia anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Faça auditoria de arquivos de log e formatos de mensagens

Você pode usar logs de auditoria para coletar informações sobre o seu sistema e solucionar problemas. Você deve entender o formato do arquivo de log de auditoria e o formato geral usado para mensagens de auditoria.

Formato de arquivo de log de auditoria

Os arquivos de log de auditoria são encontrados em cada nó Admin e contêm uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O tempo Universal coordenado (UTC) do evento que acionou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido de um espaço:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, onde *UUUUUU* estão microssegundos.

- A própria mensagem de auditoria, entre colchetes e começando com `AUDT`.

O exemplo a seguir mostra três mensagens de auditoria em um arquivo de log de auditoria (quebras de linha adicionadas para legibilidade). Essas mensagens foram geradas quando um locatário criou um bucket do S3 e adicionou dois objetos a esse bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Em seu formato padrão, as mensagens de auditoria nos arquivos de log de auditoria não são fáceis de ler ou interpretar. Você pode usar a `audit-explain` ferramenta para obter resumos simplificados das mensagens de auditoria no log de auditoria. Você pode usar a `audit-sum` ferramenta para resumir quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.

Informações relacionadas

"Utilizando a ferramenta de auditoria-explicação"

"Usando a ferramenta audit-sum"

Você pode usar a `audit-explain` ferramenta para traduzir as mensagens de auditoria no log de auditoria em um formato fácil de ler.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

Sobre esta tarefa

A `audit-explain` ferramenta, disponível no nó de administração principal, fornece resumos simplificados das mensagens de auditoria em um log de auditoria.

> A `audit-explain` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-explain` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-explain` ferramenta. Essas quatro mensagens de auditoria do SPUT foram geradas quando o locatário S3 com ID de conta 92484777680322627870 usou S3 SOLICITAÇÕES PUT para criar um bucket chamado "bucket1" e adicionar três objetos a esse bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

A `audit-explain` ferramenta pode processar logs de auditoria simples ou compatados. Por exemplo:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

A `audit-explain` ferramenta também pode processar vários arquivos de uma só vez. Por exemplo:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

Finalmente, a `audit-explain` ferramenta pode aceitar entrada de um pipe, que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Como os logs de auditoria podem ser muito grandes e lentos para analisar, você pode economizar tempo filtrando partes que você deseja olhar e executar `audit-explain` nas partes, em vez de todo o arquivo.

> ⓘ A `audit-explain` ferramenta não aceita arquivos 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.
2. Digite o seguinte comando, onde `/var/local/audit/export/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   A `audit-explain` ferramenta imprime interpretações humanamente legíveis de todas as mensagens no arquivo ou arquivos especificados.

   > ⓘ Para reduzir o comprimento das linhas e facilitar a legibilidade, os carimbos de data/hora não são apresentados por predefinição. Se você quiser ver os carimbos de data/hora, use a opção carimbo de data/hora (`-t`).

Informações relacionadas

"SPUT: S3 PUT"

Usando a ferramenta audit-sum

Você pode usar a `audit-sum` ferramenta para contar as mensagens de auditoria de

gravação, leitura, cabeçalho e exclusão e ver o tempo mínimo, máximo e médio (ou tamanho) para cada tipo de operação.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

Sobre esta tarefa

A `audit-sum` ferramenta, disponível no nó de administração principal, resume quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.

> A `audit-sum` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-sum` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações de protocolo demoraram.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

A `audit-sum` ferramenta fornece contagens e tempos para as seguintes mensagens de auditoria S3, Swift e ILM em um log de auditoria:

Código	Descrição	Consulte
ARCT	Recuperação de arquivamento do Cloud-Tier	"ARCT: Recuperação de arquivos do Cloud-Tier"
ASCT	Archive Store Cloud-Tier	"ASCT: Archive Store Cloud-Tier"
IDEL	ILM iniciado Excluir: Registra quando ILM inicia o processo de exclusão de um objeto.	"IDEL: ILM iniciou Excluir"

Código	Descrição	Consulte
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket.	"SDEL: S3 DELETE"
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	"SHEA: S3 CABEÇA"
SPUT	S3 put: Registra uma transação bem-sucedida para criar um novo objeto ou bucket.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contentor.	"WDEL: Swift DELETE"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contentor.	"WGET: Rápido"
BEM-VINDO	Swift head: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contentor.	"WHEA: CABEÇA rápida"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contentor.	"WPUT: Swift PUT"

A `audit-sum` ferramenta pode processar logs de auditoria simples ou compatados. Por exemplo:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

A `audit-sum` ferramenta também pode processar vários arquivos de uma só vez. Por exemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

Finalmente, a `audit-sum` ferramenta também pode aceitar entrada de um pipe, que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

> Esta ferramenta não aceita arquivos 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.
2. Se você quiser analisar todas as mensagens relacionadas às operações de gravação, leitura, cabeçalho e exclusão, siga estas etapas:
   a. Digite o seguinte comando, onde `/var/local/audit/export/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

      Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as

operações de protocolo demoraram.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Neste exemplo, as operações de SGET (S3 GET) são as mais lentas em média em 1,13 segundos, mas as operações de SGET e SPUT (S3 PUT) mostram tempos piores longos de cerca de 1.770 segundos.

b. Para mostrar as operações de recuperação 10 mais lentas, use o comando grep para selecionar apenas mensagens SGET e adicionar a opção de saída longa (`-l`) para incluir caminhos de objeto: `grep SGET audit.log | audit-sum -l`

   Os resultados incluem o tipo (objeto ou bucket) e o caminho, que permite que você grep o log de auditoria para outras mensagens relacionadas a esses objetos específicos.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/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 a `audit-explain` ferramenta para revisar todas as operações SGET durante essa hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se a saída do comando grep for esperada para ser muitas linhas, adicione o `less` comando para mostrar o conteúdo do arquivo de log de auditoria uma página (uma tela) de cada vez.

5. Se você quiser determinar se as operações do SPUT em buckets são mais lentas do que as operações do SPUT para objetos:

a. Comece usando a `-go` opção, que agrupa as mensagens para operações de objeto e bucket separadamente:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Os resultados mostram que as operações do SPUT para buckets têm 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
```

Informações relacionadas

"Utilizando a ferramenta de auditoria-explicação"

Formato da mensagem de auditoria

As mensagens de auditoria trocadas no sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico que descreve o evento ou a atividade que está sendo relatada.

Se as informações resumidas fornecidas pelas `audit-explain` ferramentas e `audit-sum` forem insuficientes, consulte esta secção para compreender o formato geral de todas as mensagens de auditoria.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no arquivo de log de auditoria:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(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 .

Informações relacionadas

"Utilizando a ferramenta de auditoria-explicação"

"Usando a ferramenta audit-sum"

"Auditar mensagens"

"Elementos comuns em mensagens de auditoria"

"Tipos de dados"

"Exemplos de mensagens de auditoria"

Tipos de dados

Diferentes tipos de dados são usados para armazenar informações em mensagens de auditoria.

Tipo	Descrição
UI32	Inteiro longo não assinado (32 bits); ele pode armazenar os números de 0 a 4.294.967.295.
UI64	Número inteiro duplo longo não assinado (64 bits); pode armazenar os números de 0 a 18.446.744.073.709.551.615.
FC32	Constante de quatro carateres; um valor inteiro não assinado de 32 bits representado como quatro carateres ASCII, como "ABCD".
IPAD	Usado para endereços IP.

Tipo	Descrição
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:

`2018-12-05T08:24:45.921845` **`[AUDT:[RSLT(FC32):SUCS]`** Mais
`[TIME(UI64):11454] [SAIP(IPAD):"10.224.0.100"]`
`[S3AI(CSTR):"60025621595611246499"]`
`[`**`SACC(CSTR):"account"]`**
`[S3AK(CSTR):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA==“]`
`[SUSR(CSTR):"urn:sgws:identity::60025621595611246499:root"]` uma
`[SBAI(CSTR):"60025621595611246499"] [SBAC(CSTR):"account"] [S3BK(CSTR):"bucket"]`
vez
`[S3KY(CSTR):"object"] [CBID(UI64):0xCC128B9B9E428347]`
`[UUID(CSTR):"B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"] [CSIZ(UI64):30720]`
`[AVER(UI32):10]`
`[ATIM(UI64):1543998285921845] [ATYP(FC32):SHEA] [ANID(UI32):12281045]`
`[AMID(FC32):S3RQ]`
`[ATID(UI64):15552417629170647261]]`

O `ATYP` elemento (sublinhado no exemplo) identifica qual evento gerou a mensagem. Esta mensagem de exemplo inclui o código de mensagem SHEA ([ATYP(FC32):SHEA]), indicando que foi gerado por uma solicitação DE CABEÇALHO S3 bem-sucedida.

Informações relacionadas

"Elementos comuns em mensagens de auditoria"

"Auditar mensagens"

Elementos comuns em mensagens de auditoria

Todas as mensagens de auditoria contêm os elementos comuns.

Código	Tipo	Descrição
NO MEIO	FC32	ID do módulo: Um identificador de quatro 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. Este ID não pode ser alterado.
ASES	UI64	Identificador de sessão de auditoria: Em versões anteriores, este elemento indicou o momento em que o sistema de auditoria foi inicializado após o início do serviço. Este valor de tempo foi medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). **Nota:** este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ASQN	UI64	Contagem de sequência: Em versões anteriores, esse contador foi incrementado para cada mensagem de auditoria gerada no nó de grade (ANID) e redefinido para zero na reinicialização do serviço. **Nota:** este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ATID	UI64	ID de rastreamento: Um identificador que é compartilhado pelo conjunto de mensagens que foram acionadas por um único evento.
ATIM	UI64	Timestamp: A hora em que o evento foi gerado, que acionou a mensagem de auditoria, medida em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o carimbo de data/hora para data e hora locais são baseadas em milissegundos. Pode ser necessário arredondar ou truncar o carimbo de data/hora registado. O tempo legível por humanos que aparece no início da mensagem de auditoria no `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.

Código	Tipo	Descrição
AVER	UI32	Versão: A versão da mensagem de auditoria. À medida que o software StorageGRID evolui, novas versões de serviços podem incorporar novos recursos em relatórios de auditoria. Este campo permite a compatibilidade retroativa no serviço AMS para processar mensagens de versões mais antigas de serviços.
RSLT	FC32	Resultado: O resultado de evento, processo ou transação. Se não for relevante para uma mensagem, NENHUM será usado em vez DE SUCS para que a mensagem não seja filtrada acidentalmente.

Exemplos de mensagens de auditoria

Você pode encontrar informações detalhadas em cada mensagem de auditoria. Todas as mensagens de auditoria usam o mesmo formato.

A seguir está uma mensagem de auditoria de exemplo, como ela pode aparecer no `audit.log` arquivo:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"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. O SPUT representa uma transação S3 PUT, que Registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o intervalo ao qual o objeto está associado:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"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.

Informações relacionadas

"SPUT: S3 PUT"

"Elementos comuns em mensagens de auditoria"

Auditar mensagens e o ciclo de vida do objeto

As mensagens de auditoria são geradas sempre que um objeto é ingerido, recuperado ou excluído. Você pode identificar essas transações no log de auditoria localizando mensagens de auditoria específicas da API (S3 ou Swift).

As mensagens de auditoria são vinculadas por meio de identificadores específicos a cada protocolo.

Protocolo	Código
Ligar S3 operações	S3BK (balde S3) e/ou S3KY (chave S3)
Ligando as operações Swift	WCON (Swift Container) e/ou WOBJ (Swift Object)
Vinculação de operações internas	CBID (Identificador Interno do Objeto)

Calendário das mensagens de auditoria

Devido a fatores como diferenças de tempo entre nós de grade, tamanho do objeto e atrasos na rede, a ordem das mensagens de auditoria geradas pelos diferentes serviços pode variar da mostrada nos exemplos nesta seção.

Configuração da política de gerenciamento do ciclo de vida das informações

Com a política ILM padrão (cópia de linha de base 2), os dados do objeto são copiados uma vez para um total de duas cópias. Se a política ILM exigir mais de duas cópias, haverá um conjunto adicional de mensagens CBRE, CBSE e SCMT para cada cópia extra. Para obter mais informações sobre políticas de ILM, consulte informações sobre como gerenciar objetos com gerenciamento do ciclo de vida das informações.

Nós de arquivamento

A série de mensagens de auditoria geradas quando um nó de arquivo envia dados de objeto para um sistema de armazenamento de arquivo externo é semelhante à dos nós de armazenamento, exceto que não há mensagem SCMT (Store Object Commit), e as mensagens ATCE (Archive Object Store Begin) e ASCE (Archive Object Store End) são geradas para cada cópia arquivada de dados de objeto.

A série de mensagens de auditoria geradas quando um nó de arquivo recupera dados de objetos de um sistema de armazenamento de arquivos externo é semelhante à dos nós de armazenamento, exceto que as mensagens ARCB (recuperação de objetos de arquivamento iniciada) e ARCE (fim de recuperação de objetos de arquivamento) são geradas para cada cópia recuperada de dados de objetos.

A série de mensagens de auditoria geradas quando um nó de arquivo exclui dados de objetos de um sistema de armazenamento de arquivos externo é semelhante à dos nós de armazenamento, exceto que não há nenhuma mensagem SREM (Object Store Remove) e há uma mensagem AREM (Archive Object Remove) para cada solicitação de exclusão.

Informações relacionadas

"Gerenciar objetos com ILM"

Transações de ingestão de objetos

Você pode identificar transações de ingestão de clientes no log de auditoria localizando mensagens de auditoria específicas da API (S3 ou Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de ingestão são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de ingestão são incluídas.

S3 ingira mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
SPUT	S3 COLOQUE a transação	Uma transação de ingestão de S3 PUT foi concluída com sucesso.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regras Objeto cumpridas	A política ILM foi satisfeita para este objeto.	CBID	"ORLM: Regras Objeto cumpridas"

Mensagens de auditoria de ingestão rápida

Código	Nome	Descrição	Traçado	Consulte
WPUT	Transação de COLOCAÇÃO rápida	Uma transação de ingestão Swift PUT foi concluída com sucesso.	CBID, WCON, WOBJ	"WPUT: Swift PUT"
ORLM	Regras Objeto cumpridas	A política ILM foi satisfeita para este objeto.	CBID	"ORLM: Regras Objeto cumpridas"

Exemplo: Ingestão de objeto S3

A série de mensagens de auditoria abaixo é um exemplo das mensagens de auditoria geradas e salvas no log de auditoria quando um cliente S3 ingere um objeto em um nó de armazenamento (serviço LDR).

Neste exemplo, a política ILM ativa inclui a regra ILM de estoque, faça 2 cópias.

> Nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Apenas os relacionados à transação de ingestão S3 (SPUT) estão listados.

Este exemplo assume que um bucket do S3 foi criado anteriormente.

SPUT: S3 PUT

A mensagem SPUT é gerada para indicar que uma transação S3 PUT foi emitida para criar um objeto em um intervalo específico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"]<strong
class="S3KY(CSTR):"testobject-0-
3"">[CBID(UI64):0x8EF52DF8025E63A8]</strong>[CSIZ(UI64):30720][AVER(UI32):
10]<strong
class="ATIM(UI64):150032627859669">[ATYP(FC32):SPUT]</strong>[ANID(UI32):1
2086324][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:
<strong>[CBID(UI64):0x50C4F7AC2BC8EDF7]</strong> [RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"]<strong class="LOCS(CSTR): *"CLDI 12828634
2148730112">[RSLT(FC32):SUCS][AVER(UI32):10] [ATYP(FC32):ORLM]</strong>
[ATIM(UI64):1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):131
00453][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][ATYP(FC32):ORLM][ANID(UI32):12355278][AMI
D(FC32):ILMX][ATID(UI64):4168559046473725560]]
```

O campo PATH inclui informações de bucket e chave do S3 ou informações de contentor e objeto do Swift, dependendo de qual API foi usada.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Eliminar transações

Você pode identificar transações de exclusão de objetos no log de auditoria localizando mensagens de auditoria específicas da API (S3 e Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de exclusão são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de exclusão são incluídas.

S3 exclua mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
SDEL	S3 Eliminar	Solicitação feita para excluir o objeto de um intervalo.	CBID, S3KY	"SDEL: S3 DELETE"

Swift delete mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
WDEL	Eliminação rápida	Solicitação feita para excluir o objeto de um recipiente ou do recipiente.	CBID, WOBJ	"WDEL: Swift DELETE"

Exemplo: Exclusão de objeto S3

Quando um cliente S3 exclui um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

> Nem todas as mensagens de auditoria geradas durante uma transação de exclusão são listadas no exemplo abaixo. Apenas os relacionados com a transação de exclusão S3 (SDEL) são listados.

SDEL: S3 Excluir

A exclusão de objeto começa quando o cliente envia uma solicitação DE EXCLUSÃO de objeto para um serviço LDR. A mensagem contém o intervalo do qual excluir o objeto e a chave S3 do objeto, que é usada para identificar o objeto.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"] <strong>[S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
7"][CBID(UI64):0x339F21C5A6964D89]</strong>
[CSIZ(UI64):30720][AVER(UI32):10][ATIM(UI64):150032627859669]
<strong>[ATYP(FC32):SDEL]</strong>[ANID(UI32):12086324][AMID(FC32):S3RQ][A
TID(UI64):4727861330952970593]]
```

Recuperar transações objeto

Você pode identificar transações de recuperação de objetos no log de auditoria localizando mensagens de auditoria específicas da API (S3 e Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de recuperação são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de recuperação são incluídas.

S3 mensagens de auditoria de recuperação

Código	Nome	Descrição	Traçado	Consulte
SGET	S3 GET	Solicitação feita para recuperar um objeto de um bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Mensagens de auditoria de recuperação rápida

Código	Nome	Descrição	Traçado	Consulte
WGET	Swift GET	Solicitação feita para recuperar um objeto de um contentor.	CBID, WCON, WOBJ	"WGET: Rápido"

Exemplo: Recuperação de objeto S3D.

Quando um cliente S3 recupera um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Apenas os relacionados à transação de recuperação S3 (SGET) estão listados.

SGET: S3 GET

A recuperação de objetos começa quando o cliente envia uma SOLICITAÇÃO GET Object a um serviço LDR. A mensagem contém o intervalo do qual recuperar o objeto e a chave S3 do objeto, que é usada para identificar o objeto.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-a"]
[S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947988782605][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]]
```

Se a política de bucket permitir, um cliente pode recuperar objetos anonimamente ou recuperar objetos de um bucket que é de propriedade de uma conta de locatário diferente. A mensagem de auditoria contém informações sobre a conta de locatário do proprietário do bucket para que você possa rastrear essas solicitações anônimas e entre contas.

Na mensagem de exemplo a seguir, o cliente envia uma SOLICITAÇÃO GET Object para um objeto

armazenado em um bucket que ele não possui. Os valores para SBAI e SBAC Registram o ID e o nome da conta do locatário do proprietário do bucket, que difere do ID da conta do locatário e do nome do cliente registrado em S3AI e SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]
<strong>[S3AI(CSTR):"17915054115450519830"][SACC(CSTR):"s3-account-
b"]</strong>[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="]<st
rong
class="SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"">[SBAI(CS
TR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]</strong>[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]]
```

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 foi configurado como um cabeçalho de protocolo de auditoria (**Configuração** > **Monitoramento** > **Auditoria**).

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Informações relacionadas

"Alteração dos níveis de mensagens de auditoria"

Auditar mensagens

Descrições detalhadas das mensagens de auditoria retornadas pelo sistema são listadas nas seções a seguir. Cada mensagem de auditoria é listada primeiramente em uma tabela que agrupa mensagens relacionadas pela classe de atividade que a mensagem representa. Esses agrupamentos são úteis tanto para entender os tipos de atividades auditadas quanto para selecionar o tipo desejado de filtragem de mensagens de auditoria.

As mensagens de auditoria também são listadas alfabeticamente por seus códigos de quatro 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, conforme mostrado na seguinte mensagem de exemplo:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][<stro
ng>ATYP\(FC32\):SYSU</strong>][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(
UI64):9445736326500603516]]
```

Informações relacionadas

"Auditar mensagens"

"Alteração dos níveis de mensagens de auditoria"

Auditar categorias de mensagens

Você deve estar familiarizado com as várias categorias nas quais as mensagens de auditoria são agrupadas. Esses grupos são organizados com base na classe de atividade que a mensagem representa.

Mensagens de auditoria do sistema

Você deve estar familiarizado com as mensagens de auditoria pertencentes à categoria de auditoria do sistema. Esses são eventos relacionados ao próprio sistema de auditoria, estados de nó de grade, atividade de tarefas em todo o sistema (tarefas de grade) e operações de backup de serviço, para que você possa lidar com possíveis problemas.

Código	Título e descrição da mensagem	Consulte
ECOC	Fragmento de dados codificado de apagamento corrompido: Indica que um fragmento de dados codificado de apagamento corrompido foi detetado.	"ECOC: Fragmento de dados codificado de apagamento corrompido"
ETAF	Falha na autenticação de segurança: Uma tentativa de conexão usando TLS (Transport Layer Security) falhou.	"ETAF: Falha na autenticação de segurança"
GNRG	Registro GNDS: Um serviço atualizado ou registrado informações sobre si mesmo no sistema StorageGRID.	"GNRG: Registro GNDS"
GNUR	GNDS Unregistration: Um serviço não se registrou a partir do sistema StorageGRID.	"GNUR: GNDS Unregistration"
GTED	Tarefa de grelha terminada: O serviço CMN terminou de processar a tarefa de grelha.	"GTED: Tarefa de grelha terminada"
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"

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"
LLST	Localização perdida: Esta mensagem de auditoria é gerada quando um local é perdido.	"LLST: Localização perdida"
OLST	Objeto perdido: Um objeto solicitado não pode ser localizado dentro do sistema StorageGRID.	"OLST: O sistema detetou Objeto perdido"
ORLM	Regras do objeto atendidas: Os dados do objeto são armazenados conforme especificado pelas regras do ILM.	"ORLM: Regras Objeto cumpridas"
ADICIONAR	Desativação da auditoria de segurança: O registo de mensagens de auditoria foi desativado.	"ADICIONAR: Desativação da auditoria de segurança"
SADE	Ativação da auditoria de segurança: O registo de mensagens de auditoria foi restaurado.	"SADE: Ativação da auditoria de segurança"
SVRF	Falha na verificação do armazenamento de objetos: Um bloco de conteúdo falhou verificações.	"SVRF: Falha na verificação do armazenamento de objetos"
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"

Código	Título e descrição da mensagem	Consulte
SIST	Parada do nó: Um serviço iniciou uma parada graciosa.	"SIST: Paragem do nó"
SYSU	Início do nó: Um serviço foi iniciado; a natureza do desligamento anterior é indicada na mensagem.	"SYSU: Início do nó"
VLST	Volume perdido iniciado pelo usuário: O `/proc/CMSI/Volume_Lost` comando foi executado.	"VLST: Volume iniciado pelo usuário perdido"

Informações relacionadas

"LKCU: Limpeza de objetos sobrescritos"

Mensagens de auditoria de armazenamento de objetos

Você deve estar familiarizado com as mensagens de auditoria pertencentes à categoria de auditoria de armazenamento de objetos. Estes são eventos relacionados ao armazenamento e gerenciamento de objetos no sistema StorageGRID. Isso inclui armazenamento de objetos e recuperações, transferências de nó de grade para nó de grade e verificações.

Código	Descrição	Consulte
APCT	Limpeza de arquivamento da camada da nuvem: Os dados de objetos arquivados são excluídos de um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.	"APCT: Purga de arquivamento do nível de nuvem"
ARCB	Início da recuperação de objetos de arquivamento: O serviço ARC inicia a recuperação de dados de objetos do sistema de armazenamento de arquivos externo.	"ARCB: Início da recuperação de objetos de arquivamento"
ARCE	Fim de recuperação de objetos de arquivamento: Os dados de objetos foram recuperados de um sistema de armazenamento de arquivos externo e o serviço ARC relata o status da operação de recuperação.	"ARCE: Fim de recuperação de objetos de arquivamento"

Código	Descrição	Consulte
ARCT	Recuperação de arquivos do Cloud-Tier: Os dados de objetos arquivados são recuperados de um sistema de armazenamento de arquivamento externo, que se coneta ao StorageGRID por meio da API S3.	"ARCT: Recuperação de arquivos do Cloud-Tier"
ACEM	Remoção de objeto de arquivamento: Um bloco de conteúdo foi excluído com sucesso ou sem sucesso do sistema de armazenamento de arquivos externo.	"AFEM: Remoção de objetos de Arquivo"
ASCE	Fim do armazenamento de objetos de arquivamento: Um bloco de conteúdo foi gravado no sistema de armazenamento de arquivos externo e o serviço ARC relata o status da operação de gravação.	"ASCE: Fim do armazenamento de objetos de Arquivo"
ASCT	Camada de nuvem: Os dados de objetos são armazenados em um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.	"ASCT: Archive Store Cloud-Tier"
ATCE	Início do armazenamento de objetos de arquivamento: A gravação de um bloco de conteúdo em um armazenamento de arquivamento externo foi iniciada.	"ATCE: Início do armazenamento de objetos de arquivo"
AVCC	Archive Validate Cloud-Tier Configuration: As configurações de conta e bucket fornecidas foram validadas com êxito ou sem sucesso.	"AVCC: Arquivamento Validar Configuração de nível de nuvem"
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"

Código	Descrição	Consulte
CBRE	Fim de recebimento de objeto: A entidade de destino concluiu uma operação de transferência de dados de nó de grade para nó de grade.	"CBRE: Fim de recebimento do objeto"
SCMT	Object Store commit: Um bloco de conteúdo foi completamente armazenado e verificado, e agora pode ser solicitado.	"SCMT: Confirmação de armazenamento de objetos"
SREM	Remoção do armazenamento de objetos: Um bloco de conteúdo foi excluído de um nó de grade e não pode mais ser solicitado diretamente.	"SREM: Armazenamento de objetos Remover"

O cliente lê mensagens de auditoria

As mensagens de auditoria de leitura do cliente são registradas quando um aplicativo cliente S3 ou Swift faz uma solicitação para recuperar um objeto.

Código	Descrição	Usado por	Consulte
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket. **Nota:** se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SGET: S3 GET"
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	Cliente S3	"SHEA: S3 CABEÇA"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contentor.	Cliente Swift	"WGET: Rápido"

Código	Descrição	Usado por	Consulte
BEM-VINDO	Swift head: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contentor.	Cliente Swift	"WHEA: CABEÇA rápida"

O cliente escreve mensagens de auditoria

As mensagens de auditoria de gravação do cliente são registradas quando um aplicativo cliente S3 ou Swift faz uma solicitação para criar ou modificar um objeto.

Código	Descrição	Usado por	Consulte
OVWR	Object Overwrite: Registra uma transação para sobrescrever um objeto com outro objeto.	S3 clientes Clientes Swift	"OVWR: Substituição de objetos"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket. **Nota:** se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SDEL: S3 DELETE"
SPOS	S3 POST: Registra uma transação bem-sucedida para restaurar um objeto do armazenamento do AWS Glacier para um pool de armazenamento em nuvem.	Cliente S3	"SPOS: S3 POST"
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"

Código	Descrição	Usado por	Consulte
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"

Auditar mensagens

Quando ocorrem eventos do sistema, o sistema StorageGRID gera mensagens de auditoria e as Registra no log de auditoria.

APCT: Purga de arquivamento do nível de nuvem

Essa mensagem é gerada quando os dados de objetos arquivados são excluídos de um sistema de storage de arquivamento externo, que se coneta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi excluído.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes. Sempre retorna 0.

Código	Campo	Descrição
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	Identificador exclusivo (UUID) do nível de nuvem do qual o objeto foi excluído.

ARCB: Início da recuperação de objetos de arquivamento

Esta mensagem é gerada quando uma solicitação é feita para recuperar dados de objetos arquivados e o processo de recuperação é iniciado. Os pedidos de recuperação são processados imediatamente, mas podem ser reordenados para melhorar a eficiência da recuperação de meios lineares, como fita.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de armazenamento de arquivos externo.
RSLT	Resultado	Indica o resultado do início do processo de recuperação do arquivo. O valor atualmente definido é:SUCS: A solicitação de conteúdo foi recebida e enfileirada para recuperação.

Esta mensagem de auditoria marca a hora de uma recuperação de arquivo. Ele permite que você combine a mensagem com uma mensagem final ARCE correspondente para determinar a duração da recuperação do arquivo e se a operação foi bem-sucedida.

ARCE: Fim de recuperação de objetos de arquivamento

Esta mensagem é gerada quando uma tentativa do nó de arquivo para recuperar dados de objetos de um sistema de armazenamento de arquivos externo é concluída. Se for bem-sucedida, a mensagem indica que os dados do objeto solicitado foram completamente lidos a partir do local do arquivo e foram verificados com sucesso. Depois que os dados do objeto forem recuperados e verificados, eles serão entregues ao serviço solicitante.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de armazenamento de arquivos externo.

Código	Campo	Descrição
VLID	Identificador de volume	O identificador do volume no qual os dados foram arquivados.se não for encontrada uma localização de arquivo para o conteúdo, é devolvida uma ID de volume de 0.
RSLT	Resultado de recuperação	O estado de conclusão do processo de recuperação do arquivo: • SUCS: Bem-sucedido • VRFL: Falhou (falha na verificação de objetos) • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • CANC: Falha (operação de recuperação cancelada) • GERR: Falhou (erro geral)

A correspondência desta mensagem com a mensagem ARCB correspondente pode indicar o tempo necessário para executar a recuperação do arquivo. Esta mensagem indica se a recuperação foi bem-sucedida e, em caso de falha, a causa da falha na recuperação do bloco de conteúdo.

ARCT: Recuperação de arquivos do Cloud-Tier

Essa mensagem é gerada quando os dados de objetos arquivados são recuperados de um sistema de armazenamento de arquivamento externo, que se coneta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi recuperado.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes. O valor só é preciso para recuperações bem-sucedidas.
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	Identificador único (UUID) do sistema de armazenamento de arquivos externo.

Código	Campo	Descrição
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.

AFEM: Remoção de objetos de Arquivo

A mensagem de auditoria Remover Objeto de Arquivo indica que um bloco de conteúdo foi excluído com sucesso ou sem sucesso de um nó de Arquivo. Se o resultado for bem-sucedido, o nó de arquivo informou com sucesso o sistema de armazenamento de arquivamento externo de que o StorageGRID liberou um local de objeto. Se o objeto é removido do sistema de armazenamento de arquivos externo depende do tipo de sistema e sua configuração.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de Mídia de arquivamento externo.
VLID	Identificador de volume	O identificador do volume no qual os dados do objeto foram arquivados.
RSLT	Resultado	O estado de conclusão do processo de remoção do arquivo: • SUCS: Bem-sucedido • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • GERR: Falhou (erro geral)

ASCE: Fim do armazenamento de objetos de Arquivo

Esta mensagem indica que a gravação de um bloco de conteúdo em um sistema de armazenamento de arquivos externo terminou.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador do bloco de conteúdo armazenado no sistema de armazenamento de arquivos externo.

Código	Campo	Descrição
VLID	Identificador de volume	O identificador exclusivo do volume de arquivo no qual os dados do objeto são gravados.
VREN	Verificação ativada	Indica se a verificação é realizada para blocos de conteúdo. Os valores atualmente definidos são: • VENA: A verificação está ativada • VDSA: A verificação está desativada
MCLS	Classe de Gestão	Uma cadeia de carateres que identifica a classe de gerenciamento TSM à qual o bloco de conteúdo é atribuído, se aplicável.
RSLT	Resultado	Indica o resultado do processo de arquivo. Os valores atualmente definidos são: • SUCS: Bem-sucedido (processo de arquivamento bem-sucedido) • OFFL: Falhou (o arquivamento está offline) • VRFL: Falhou (verificação de objeto falhou) • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • GERR: Falhou (erro geral)

Esta mensagem de auditoria significa que o bloco de conteúdo especificado foi gravado no sistema de armazenamento de arquivos externo. Se a gravação falhar, o resultado fornece informações básicas de solução de problemas sobre onde a falha ocorreu. Informações mais detalhadas sobre falhas de arquivo podem ser encontradas examinando os atributos do nó de arquivo no sistema StorageGRID.

ASCT: Archive Store Cloud-Tier

Essa mensagem é gerada quando os dados de objetos arquivados são armazenados em um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi recuperado.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	Identificador exclusivo (UUID) do nível de nuvem para o qual o conteúdo foi armazenado.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.

ATCE: Início do armazenamento de objetos de arquivo

Essa mensagem indica que a gravação de um bloco de conteúdo em um armazenamento de arquivamento externo foi iniciada.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser arquivado.
VLID	Identificador de volume	O identificador exclusivo do volume para o qual o bloco de conteúdo é escrito. Se a operação falhar, um ID de volume de 0 é retornado.

Código	Campo	Descrição
RSLT	Resultado	Indica o resultado da transferência do bloco de conteúdo. Os valores atualmente definidos são: • SUCS: Sucesso (bloco de conteúdo armazenado com sucesso) • EXIS: Ignorado (bloco de conteúdo já estava armazenado) • ISFD: Falha (espaço em disco insuficiente) • STER: Falhou (erro ao armazenar o CBID) • OFFL: Falhou (o arquivamento está offline) • GERR: Falhou (erro geral)

AVCC: Arquivamento Validar Configuração de nível de nuvem

Essa mensagem é gerada quando as configurações são validadas para um tipo de destino Cloud Tiering - Simple Storage Service (S3).

Código	Campo	Descrição
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	UUID associado ao sistema de armazenamento de arquivamento externo sendo validado.

CBRB: Início de recebimento de objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre nós diferentes à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, essa mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se for bem-sucedida, a transferência começa a partir desta contagem de sequência.
CTES	Contagem sequência fim esperado	Indica a última contagem de sequência solicitada. Se for bem-sucedida, a transferência é considerada concluída quando esta contagem de sequência tiver sido recebida.
RSLT	Estado Início transferência	Estado no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Essa mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único conteúdo, conforme identificado por seu Identificador de bloco de conteúdo. A operação solicita dados de "Start Sequence Count" (contagem de sequência de início) para "expected End Sequence Count" (contagem de sequência de fim esperado) Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBRE: Fim de recebimento do objeto

Quando a transferência de um bloco de conteúdo de um nó para outro for concluída, essa mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência com a qual a transferência foi iniciada.
CTAS	Contagem sequência fim Real	Indica a última contagem de sequência transferida com êxito. Se a contagem de sequência final real for a mesma que a contagem de sequência inicial e o resultado da transferência não tiver sido bem-sucedido, não foram trocados dados.

Código	Campo	Descrição
RSLT	Resultado da transferência	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: Transferência terminada devido à receção de dados corrompidos ou inválidos (pode indicar adulteração)

Essa mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi concluída. Se o resultado da transferência tiver sido bem-sucedido, a operação transferiu dados de "Start Sequence Count" (contagem de sequência de início) para "Real End Sequence Count" (contagem de sequência final real). Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, ele também pode ser usado para verificar contagens de réplicas.

CBSB: Início do envio de objetos

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre nós diferentes à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, essa mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.

Código	Campo	Descrição
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se for bem-sucedida, a transferência começa a partir desta contagem de sequência.
CTES	Contagem sequência fim esperado	Indica a última contagem de sequência solicitada. Se for bem-sucedida, a transferência é considerada concluída quando esta contagem de sequência tiver sido recebida.
RSLT	Estado Início transferência	Estado no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Essa mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único conteúdo, conforme identificado por seu Identificador de bloco de conteúdo. A operação solicita dados de "Start Sequence Count" (contagem de sequência de início) para "expected End Sequence Count" (contagem de sequência de fim esperado) Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBSE: Fim de envio de objeto

Quando a transferência de um bloco de conteúdo de um nó para outro for concluída, essa mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência com a qual a transferência foi iniciada.
CTAS	Contagem sequência fim Real	Indica a última contagem de sequência transferida com êxito. Se a contagem de sequência final real for a mesma que a contagem de sequência inicial e o resultado da transferência não tiver sido bem-sucedido, não foram trocados dados.

Código	Campo	Descrição
RSLT	Resultado da transferência	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: Transferência terminada devido à receção de dados corrompidos ou inválidos (pode indicar adulteração)

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.

ECOC: Fragmento de dados codificado de apagamento corrompido

Essa mensagem de auditoria indica que o sistema detetou um fragmento de dados codificado de apagamento corrompido.

Código	Campo	Descrição
VCCO	ID VCS	O nome do VCS que contém o bloco corrompido.
VLID	ID do volume	O volume RangeDB que contém o fragmento corrompido codificado de apagamento.
CCID	Código bloco	O identificador do fragmento codificado de apagamento corrompido.

Código	Campo	Descrição
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatória, mas não é relevante para esta mensagem em particular. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ETAF: Falha na autenticação de segurança

Esta mensagem é gerada quando uma tentativa de conexão usando TLS (Transport Layer Security) falhou.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP sobre a qual a autenticação falhou.
RUIDA	Identidade do usuário	Um identificador dependente do serviço que representa a identidade do utilizador remoto.

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.
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.

Código	Campo	Descrição
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 cancelada sem um erro de reversão. • ROLF: A tarefa de grade foi cancelada e não foi possível concluir o processo de reversão. • CANC: A tarefa de grade foi cancelada pelo usuário antes de ser iniciada. • EXPR: A tarefa de grade expirou antes de ser iniciada. • IVLD: A tarefa de grade era inválida. • AUTH: A tarefa de grade não foi autorizada. • DUPL: A tarefa de grade foi rejeitada como uma duplicata.

GTST: Tarefa de grade iniciada

Esta mensagem de auditoria indica que o serviço CMN começou a processar a tarefa de grade especificada. A mensagem de auditoria segue imediatamente a mensagem de tarefa de Grade enviada para tarefas de grade iniciadas pelo serviço de envio de tarefa de Grade interno e selecionadas para ativação automática. Para tarefas de grade enviadas para a tabela pendente, essa mensagem é gerada quando o usuário inicia a tarefa de grade.

Código	Campo	Descrição
TSID	Código tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Observação:** o ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.
RSLT	Resultado	O resultado. Este campo tem apenas um valor: • SUCS: A tarefa de grade foi iniciada com sucesso.

GTSU: Tarefa de grelha enviada

Esta mensagem de auditoria indica que uma tarefa de grade foi enviada ao serviço CMN.

Código	Campo	Descrição
TSID	Código tarefa	Identifica de forma única uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Observação:** o ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.
TTYP	Tipo tarefa	O tipo de tarefa de grade.

Código	Campo	Descrição
TVER	Versão da tarefa	Um número que indica a versão da tarefa de grade.
TDSC	Descrição tarefa	Uma descrição humanamente legível da tarefa de grade.
CUBAS	Válido após Timestamp	A primeira vez (UINT64 microssegundos a partir de 1 de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
VBTS	Válido antes do Timestamp	A última hora (UINT64 microssegundos a partir de 1 de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
TSRC	Fonte	A origem da tarefa: • TXTB: A tarefa de grade foi enviada pelo sistema StorageGRID como um bloco de texto assinado. • GRADE: A tarefa de grade foi enviada através do Serviço interno de envio de tarefa de Grade.
ACTV	Tipo de ativação	O tipo de ativação: • AUTO: A tarefa de grade foi submetida para ativação automática. • PEND: A tarefa de grade foi enviada para a tabela pendente. Esta é a única possibilidade para a fonte TXTB.
RSLT	Resultado	O resultado da submissão: • SUCS: A tarefa de grade foi enviada com sucesso. • FALHA: A tarefa foi movida diretamente para a tabela histórica.

IDEL: ILM iniciou Excluir

Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto.

A mensagem IDEL é gerada em qualquer uma destas situações:

- **Para objetos em buckets S3 compatíveis**: Esta mensagem é gerada quando o ILM inicia o processo de exclusão automática de um objeto porque seu período de retenção expirou (assumindo que a configuração de exclusão automática esteja ativada e a retenção legal esteja desativada).
- **Para objetos em buckets S3 não compatíveis ou contentores Swift**. Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto porque nenhuma instrução de posicionamento na política ILM ativa se aplica atualmente ao objeto.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CMPA	Conformidade: Eliminação automática	Apenas para objetos em buckets compatíveis com S3. 0 (falso) ou 1 (verdadeiro), indicando se um objeto compatível deve ser excluído automaticamente quando seu período de retenção terminar, a menos que o intervalo esteja sob uma retenção legal.
CMPL	Conformidade: Guarda legal	Apenas para objetos em buckets compatíveis com S3. 0 (falso) ou 1 (verdadeiro), indicando se o balde está atualmente sob uma retenção legal.
CMPR	Conformidade: Período de retenção	Apenas para objetos em buckets compatíveis com S3. O comprimento do período de retenção do objeto em minutos.
CTME	Conformidade: Tempo de ingestão	Apenas para objetos em buckets compatíveis com S3. O tempo de ingestão do objeto. Você pode adicionar o período de retenção em minutos a esse valor para determinar quando o objeto pode ser excluído do intervalo.
DMRK	Eliminar ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket com versão. As operações em buckets não incluem este campo.

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 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	• Se um objeto em um bucket compatível com S3 estiver sendo excluído automaticamente porque seu período de retenção expirou, esse campo estará em branco. • Se o objeto estiver sendo excluído porque não há mais instruções de posicionamento que se aplicam atualmente ao objeto, este campo mostra o rótulo legível por humanos da última regra ILM aplicada ao objeto.

Código	Campo	Descrição
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

LKCU: Limpeza de objetos sobrescritos

Essa mensagem é gerada quando o StorageGRID remove um objeto sobrescrito que antes era necessário limpar para liberar espaço de armazenamento. Um objeto é substituído quando um cliente S3 ou Swift grava um objeto em um caminho que já contém um objeto. O processo de remoção ocorre automaticamente e em segundo plano.

Código	Campo	Descrição
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LTYP	Tipo de limpeza	*Somente uso interno.*
LUID	UUUID Objeto removido	O identificador do objeto que foi removido.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
UUID	Identificador universal único	O identificador do objeto que ainda existe. Este valor só está disponível se o objeto não tiver sido excluído.

LLST: Localização perdida

Essa mensagem é gerada sempre que um local para uma cópia de objeto (replicado ou codificado de apagamento) não pode ser encontrado.

Código	Campo	Descrição
CBIL	CBID	O CBID afetado.
NOID	Código nó origem	O ID do nó no qual os locais foram perdidos.
UUID	ID universal única	O identificador do objeto afetado no sistema StorageGRID.
ECPR	Perfil de codificação de apagamento	Para dados de objetos codificados por apagamento. A ID do perfil de codificação de apagamento utilizado.
LTYP	Tipo de localização	CLDI (Online): Para dados de objeto replicados CLEC (Online): Para dados de objetos codificados por apagamento CLNL (Nearline): Para dados de objetos replicados arquivados
PCLD	Caminho para o objeto replicado	O caminho completo para a localização do disco dos dados do objeto perdido. Somente retornado quando LTYP tem um valor de CLDI (ou seja, para objetos replicados). Toma a forma `/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

MGAU: Mensagem de auditoria de gestão

A categoria Gerenciamento Registra as solicitações do usuário para a API de

gerenciamento. Cada solicitação que não é uma solicitação GET ou HEAD para a API Registra uma resposta com o nome de usuário, IP e tipo de solicitação para a API.

Código	Campo	Descrição
MDIP	Endereço IP de destino	O endereço IP do servidor (destino).
MDNA	Nome de domínio	O nome de domínio do host.
MPAT	PATH da solicitação	O caminho da solicitação.
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

Código	Campo	Descrição
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 nearline conhecida do objeto perdido. É possível ter apenas o ID do nó sem um ID de volume se as informações do volume não estiverem disponíveis.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	Se disponível, o nome do bucket S3 e o nome da chave S3 ou o nome do contentor Swift e o identificador do objeto Swift.

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.
UUID	ID universal única	O identificador do objeto perdido dentro do sistema StorageGRID.
VOLI	ID do volume	Se disponível, o ID de volume do nó de armazenamento ou nó de arquivo para a última localização conhecida do objeto perdido.

ORLM: Regras Objeto cumpridas

Esta mensagem é gerada quando o objeto é armazenado e copiado com sucesso, conforme especificado pelas regras ILM.

A mensagem ORLM não é gerada quando um objeto é armazenado com êxito pela regra de fazer cópias 2 padrão se outra regra na política usar o filtro avançado tamanho do objeto.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.

Código	Campo	Descrição
LOCALIZAÇÃO	Locais	O local de armazenamento de dados de objetos no sistema StorageGRID. O valor para LOCS é "" se o objeto não tiver locais (por exemplo, ele foi excluído). CLEC: Para objetos codificados por apagamento, o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento que é aplicado aos dados do objeto. CLDI: Para objetos replicados, o ID do nó LDR e o ID do volume da localização do objeto. CLNL: ARC node ID da localização do objeto se os dados do objeto forem arquivados.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	O rótulo legível por humanos dado à regra ILM aplicada a este objeto.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
SGCB	CBID do recipiente	CBID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.

Código	Campo	Descrição
STAT	Estado	O estado da operação ILM. Feito: Operações ILM contra o objeto foram concluídas. DFER: O objeto foi marcado para futura reavaliação ILM. PRGD: O objeto foi excluído do sistema StorageGRID. NLOC: Os dados do objeto não podem mais ser encontrados no sistema StorageGRID. Esse status pode indicar que todas as cópias dos dados do objeto estão ausentes ou danificadas.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.

A mensagem de auditoria ORLM pode ser emitida várias vezes para um único objeto. Por exemplo, ele é emitido sempre que um dos seguintes eventos ocorrer:

- As regras de ILM para o objeto são satisfeitas para sempre.
- As regras de ILM para o objeto são satisfeitas para esta época.
- As regras do ILM excluíram o objeto.
- O processo de verificação em segundo plano deteta que uma cópia dos dados de objetos replicados está corrompida. O sistema StorageGRID executa uma avaliação ILM para substituir o objeto corrompido.

Informações relacionadas

"Transações de ingestão de objetos"

"Eliminar transações"

OVWR: Substituição de objetos

Esta mensagem é gerada quando uma operação externa (solicitada pelo cliente) faz com que um objeto seja substituído por outro objeto.

Código	Campo	Descrição
CBID	Identificador de bloco de conteúdo (novo)	O CBID para o novo objeto.
CSIZ	Tamanho Objeto anterior	O tamanho, em bytes, do objeto que está sendo substituído.

Código	Campo	Descrição
OCBD	Identificador de bloco de conteúdo (anterior)	O CBID para o objeto anterior.
UUID	ID universal única (novo)	O identificador do novo objeto dentro do sistema StorageGRID.
OUID	ID universal única (anterior)	O identificador para o objeto anterior dentro do sistema StorageGRID.
CAMINHO	S3 ou Swift Object Path	O caminho de objeto S3 ou Swift usado para o objeto anterior e novo
RSLT	Código do resultado	Resultado da transação de Sobreposição de objetos. O resultado é sempre: SUCS: Bem-sucedido

ADICIONAR: Desativação da auditoria de segurança

Essa mensagem indica que o serviço de origem (ID do nó) desativou o Registro de mensagens de auditoria; as mensagens de auditoria não estão mais sendo coletadas ou entregues.

Código	Campo	Descrição
AETM	Ativar método	O método utilizado para desativar a auditoria.
AEUN	Nome de utilizador	O nome de usuário que executou o comando para desativar o log de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

A mensagem implica que o registo foi anteriormente ativado, mas agora foi desativado. Normalmente, isso é usado apenas durante a ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada (SADE) e a capacidade de desativar a auditoria é então permanentemente bloqueada.

SADE: Ativação da auditoria de segurança

Esta mensagem indica que o serviço de origem (ID do nó) restaurou o registo de mensagens de auditoria; as mensagens de auditoria estão novamente a ser recolhidas e entregues.

Código	Campo	Descrição
AETM	Ativar método	O método utilizado para ativar a auditoria.
AEUN	Nome de utilizador	O nome de usuário que executou o comando para ativar o log de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

A mensagem implica que o registo foi anteriormente desativado (SADD), mas foi agora restaurado. Isso geralmente é usado apenas durante a ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada e a capacidade de desativar a auditoria é então permanentemente bloqueada.

SCMT: Confirmação de armazenamento de objetos

O conteúdo da grade não é disponibilizado ou reconhecido como armazenado até que ele tenha sido comprometido (ou seja, ele foi armazenado persistentemente). O conteúdo armazenado persistentemente foi completamente gravado no disco e passou por verificações de integridade relacionadas. Essa mensagem é emitida quando um bloco de conteúdo é comprometido com o armazenamento.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo comprometido com o armazenamento permanente.
RSLT	Código do resultado	Status no momento em que o objeto foi armazenado no disco: SUCS: Objeto armazenado com sucesso.

Esta mensagem significa que um determinado bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado. Ele pode ser usado para rastrear o fluxo de dados dentro do sistema.

SDEL: S3 DELETE

Quando um cliente S3 emite uma transação DE EXCLUSÃO, uma solicitação é feita para remover o objeto ou bucket especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. As operações em buckets não incluem este campo.
DMRK	Eliminar ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket com versão. As operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.

Código	Campo	Descrição
RSLT	Código do resultado	Resultado da transação DE EXCLUSÃO. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos 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.

Código	Campo	Descrição
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SGET: S3 GET

Quando um cliente S3 emite uma transação GET, uma solicitação é feita para recuperar um objeto ou listar os objetos em um bucket. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RANG	Leitura de intervalo	Apenas para operações de leitura de gama. Indica o intervalo de bytes que foi lido por esta solicitação. O valor após a barra (/) mostra o tamanho de todo o objeto.
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.

Código	Campo	Descrição
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos 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.

SHEA: S3 CABEÇA

Quando um cliente S3 emite uma TRANSAÇÃO PRINCIPAL, uma solicitação é feita para verificar a existência de um objeto ou bucket e recuperar os metadados sobre um objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto verificado em bytes. As operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.

Código	Campo	Descrição
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos 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.

Código	Campo	Descrição
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPOS: S3 POST

Quando um cliente S3 emite uma solicitação de restauração PÓS-objeto, é feita uma solicitação para restaurar um objeto do armazenamento do AWS Glacier para um Cloud Storage Pool. 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.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da solicitação de restauração PÓS-objeto. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
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.

Código	Campo	Descrição
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPUT: S3 PUT

Quando um cliente S3 emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou bucket. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CMPS	Definições de conformidade	As configurações de conformidade usadas ao criar o bucket, se estiverem presentes na solicitação PUT Bucket (truncada para os primeiros 1024 carateres)

Código	Campo	Descrição
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
LKEN	Bloqueio Objeto ativado	Valor do cabeçalho da solicitação `x-amz-bucket-object-lock-enabled` , se estiver presente na solicitação COLOCAR balde.
LKLH	Bloqueio Objeto retenção legal	Valor do cabeçalho da solicitação `x-amz-object-lock-legal-hold` , se estiver presente na solicitação COLOCAR Objeto.
LKMD	Modo de retenção de bloqueio de objetos	Valor do cabeçalho da solicitação `x-amz-object-lock-mode` , se estiver presente na solicitação COLOCAR Objeto.
LKRU	Reter Data até bloqueio Objeto	Valor do cabeçalho da solicitação `x-amz-object-lock-retain-until-date` , se estiver presente na solicitação COLOCAR Objeto.
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.

Código	Campo	Descrição
RSLT	Código do resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	S3KY	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos 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).

Código	Campo	Descrição
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UID	ID de carregamento	Incluído apenas nas mensagens SPUT para operações de Upload de várias partes completas. Indica que todas as peças foram carregadas e montadas.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	A ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.
VSST	Estado de controle de versão	O novo estado de controle de versão de um bucket. Dois estados são usados: "Habilitado" ou "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 buckets não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação, ao atualizar as configurações de conformidade de um bucket.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em buckets não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos 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.

Código	Campo	Descrição
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `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.
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.

Nota: esta mensagem deve ser monitorada de perto. Falhas na verificação de conteúdo podem indicar tentativas de adulteração de conteúdo ou falhas iminentes de hardware.

Para determinar que operação acionou a mensagem, consulte o valor do campo AID (ID do módulo). Por exemplo, um valor SVFY indica que a mensagem foi gerada pelo módulo Storage Verifier, ou seja, verificação em segundo plano e STOR indica que a mensagem foi acionada pela recuperação de conteúdo.

SVRU: Verificação do armazenamento de objetos desconhecido

O componente de armazenamento do serviço LDR verifica continuamente todas as cópias de dados de objetos replicados no armazenamento de objetos. Esta mensagem é emitida quando uma cópia desconhecida ou inesperada de dados de objetos replicados é detetada no armazenamento de objetos e movida para o diretório de quarentena.

Código	Campo	Descrição
FPTH	Caminho do ficheiro	O caminho do arquivo da cópia de objeto inesperada.

Código	Campo	Descrição
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

Nota: a mensagem de auditoria SVRU: Object Store Verify Unknown deve ser monitorada de perto. Isso significa que cópias inesperadas de dados de objetos foram detetadas no armazenamento de objetos. Essa situação deve ser investigada imediatamente para determinar como essas cópias foram criadas, pois pode indicar tentativas de adulteração de conteúdo ou falhas iminentes de hardware.

SYSD: Parada do nó

Quando um serviço é parado graciosamente, essa mensagem é gerada para indicar que o desligamento foi solicitado. Normalmente, esta mensagem é enviada apenas após um reinício subsequente, porque a fila de mensagens de auditoria não é eliminada antes do encerramento. Procure a mensagem DO SISTEMA, enviada no início da sequência de encerramento, se o serviço não tiver sido reiniciado.

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O RSLT de um SYSD não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SIST: Paragem do nó

Quando um serviço é parado graciosamente, essa mensagem é gerada para indicar que o desligamento foi solicitado e que o serviço iniciou sua sequência de desligamento. O SYST pode ser usado para determinar se o desligamento foi solicitado, antes que o serviço seja reiniciado (ao contrário do SYSD, que normalmente é enviado após o reinício do serviço).

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O código RSLT de uma mensagem DO SISTEMA não pode indicar um desligamento "sujo", porque a mensagem é

gerada apenas por desligamentos "limpos".

SYSU: Início do nó

Quando um serviço é reiniciado, essa mensagem é gerada para indicar se o desligamento anterior foi limpo (comandado) ou desordenado (inesperado).

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa. DSDN: O sistema não foi desligado corretamente. VRGN: O sistema foi iniciado pela primeira vez após a instalação do servidor (ou reinstalação).

A mensagem não indica se o servidor host foi iniciado, apenas o serviço de relatórios. Esta mensagem pode ser usada para:

- Detecte a descontinuidade na trilha de auditoria.
- Determine se um serviço está falhando durante a operação (uma vez que a natureza distribuída do sistema StorageGRID pode mascarar essas falhas). O Server Manager reinicia automaticamente um serviço com falha.

VLST: Volume iniciado pelo usuário perdido

Esta mensagem é emitida sempre que o `/proc/CMSI/Volume_Lost` comando é executado.

Código	Campo	Descrição
VOLL	Identificador de volume inferior	A extremidade inferior do intervalo de volume afetado ou um único volume.
VOLU	Identificador de volume superior	A extremidade superior do intervalo de volume afetado. Igual a VOLL se um único volume.
NOID	Código nó origem	O ID do nó no qual os locais foram perdidos.
LTYP	Tipo de localização	'CLDI' (Online) ou 'CLNL' (Nearline). Se não for especificado, o padrão é 'CLDI'.

Código	Campo	Descrição
RSLT	Resultado	Sempre "NENHUM". RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

WDEL: Swift DELETE

Quando um cliente Swift emite uma transação DE EXCLUSÃO, uma solicitação é feita para remover o objeto ou contentor especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contentores não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. As operações em contentores não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.

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.
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 contêineres não incluem esse campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contas e contêineres não incluem esse campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO 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.

Código	Campo	Descrição
WCON	Contentor Swift	O nome do contentor Swift. As operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contas e contêineres não incluem esse campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WHEA: CABEÇA rápida

Quando um cliente Swift emite uma TRANSAÇÃO PRINCIPAL, uma solicitação é feita para verificar a existência de uma conta, contentor ou objeto e recuperar quaisquer metadados relevantes. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contas e contêineres não incluem esse campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contas e contêineres não incluem esse campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).

Código	Campo	Descrição
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 contêineres não incluem esse campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WPUT: Swift PUT

Quando um cliente Swift emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou contentor. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contentores não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contentores não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. **Nota:** `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
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.

Código	Campo	Descrição
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.

Manutenção

Expanda sua grade

Saiba como expandir um sistema StorageGRID sem interromper as operações do sistema.

- "Planejando uma expansão do StorageGRID"
- "Preparando-se para uma expansão"
- "Visão geral do procedimento de expansão"
- "Adição de volumes de storage aos nós de storage"
- "Adicionar nós de grade a um site existente ou adicionar um novo site"
- "Configurando seu sistema StorageGRID expandido"
- "Contactar o suporte técnico"

Planejando uma expansão do StorageGRID

Você pode expandir o StorageGRID para aumentar a capacidade de storage, adicionar capacidade de metadados, adicionar redundância ou novos recursos ou adicionar um novo site. O número, o tipo e o local dos nós que você precisa adicionar dependem do motivo da expansão.

- "Adição de capacidade de storage"
- "Adição de capacidade de metadados"
- "Adição de nós de grade para adicionar recursos ao seu sistema"
- "Adicionar um novo site"

Adição de capacidade de storage

Quando os nós de storage existentes ficarem cheios, você precisará aumentar a capacidade de storage do sistema StorageGRID.

Para aumentar a capacidade de storage, primeiro você precisa entender onde os dados são armazenados no momento e adicionar capacidade em todos os locais necessários. Por exemplo, se você armazenar cópias de dados de objetos no momento em vários locais, talvez seja necessário aumentar a capacidade de storage de cada local.

- "Diretrizes para adicionar capacidade de objeto"
- "Adição de capacidade de storage para objetos replicados"
- "Adição de capacidade de storage para objetos codificados por apagamento"
- "Considerações para rebalanceamento de dados codificados por apagamento"

Diretrizes para adicionar capacidade de objeto

Você pode expandir a capacidade de storage de objetos do seu sistema StorageGRID

adicionando volumes de storage a nós de storage existentes ou adicionando novos nós de storage a locais existentes. Você precisa adicionar capacidade de storage de forma que atenda aos requisitos da política de gerenciamento do ciclo de vida das informações (ILM).

Diretrizes para adicionar volumes de armazenamento

Antes de adicionar volumes de storage a nós de storage existentes, consulte as diretrizes e limitações a seguir:

- Você deve examinar suas regras atuais de ILM para determinar onde e quando adicionar volumes de storage para aumentar o storage disponível para objetos replicados ou codificados por apagamento. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.
- Você não pode aumentar a capacidade de metadados do sistema adicionando volumes de storage porque os metadados de objetos são armazenados apenas no volume 0.
- Cada nó de storage baseado em software pode dar suporte a um máximo de 16 volumes de storage. Se você precisar adicionar capacidade além disso, precisará adicionar novos nós de storage.
- Você pode adicionar uma ou duas gavetas de expansão a cada dispositivo SG6060. 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.
- Não é possível adicionar volumes de armazenamento a qualquer outro dispositivo de armazenamento.
- Não é possível aumentar o tamanho de um volume de armazenamento existente.
- Não é possível adicionar volumes de armazenamento a um nó de armazenamento ao mesmo tempo em que está a efetuar uma atualização do sistema, uma operação de recuperação ou outra expansão.

Depois de decidir adicionar volumes de storage e determinar quais nós de storage você deve expandir para atender à política de ILM, siga as instruções para seu tipo de nó de storage:

- Para adicionar prateleiras de expansão a um dispositivo de armazenamento SG6060, consulte as instruções para a instalação e manutenção do dispositivo SG6000.

  "SG6000 dispositivos de armazenamento"

- Para um nó baseado em software, siga as instruções para adicionar volumes de storage aos nós de storage.

  "Adição de volumes de storage aos nós de storage"

Diretrizes para a adição de nós de storage

Antes de adicionar nós de storage a sites existentes, consulte as diretrizes e limitações a seguir:

- Você deve examinar suas regras atuais de ILM para determinar onde e quando adicionar nós de storage para aumentar o storage disponível para objetos replicados ou codificados por apagamento.
- 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. Consulte os passos para verificar os

trabalhos de reparação de dados nas instruções de recuperação e manutenção.

- 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 um quórum de serviços ADC esteja disponível em cada local e em todos os momentos.

  Saiba mais sobre o quórum ADC nas instruções de recuperação e manutenção.

- Pelo menos três nós de storage em cada local devem incluir o serviço ADC.
- Adicionar o serviço ADC a cada nó de armazenamento não é recomendado. Incluir muitos serviços ADC pode causar lentidão devido ao aumento da quantidade de comunicação entre nós.
- Uma única grade não deve ter mais de 48 nós de storage com o serviço ADC. Isso equivale a 16 sites com três serviços ADC em cada local.
- Em geral, quando você seleciona a configuração **ADC Service** para um novo nó, você deve selecionar **Automatic**. Selecione **Sim** somente se o novo nó substituir outro nó de armazenamento que inclua o serviço ADC. Como você não pode desativar um nó de armazenamento se houver poucos serviços ADC, isso garante que um novo serviço ADC esteja disponível antes que o serviço antigo seja removido.
- Você não pode adicionar o serviço ADC a um nó depois que ele é implantado.

Informações relacionadas

"Gerenciar objetos com ILM"

"SG6000 dispositivos de armazenamento"

"Adição de volumes de storage aos nós de storage"

"Manter recuperar"

"Executando a expansão"

Adição de capacidade de storage para objetos replicados

Se a política de gerenciamento do ciclo de vida das informações (ILM) da implantação incluir uma regra que crie cópias replicadas de objetos, você deverá considerar quanto storage adicionar e onde adicionar os novos volumes de storage ou nós de storage.

Para obter orientação sobre onde adicionar armazenamento adicional, examine as regras do ILM que criam cópias replicadas. Se as regras do ILM criarem duas ou mais cópias de objetos, Planeje adicionar storage em cada local em que as cópias de objetos forem feitas. Como um exemplo simples, se você tiver uma grade de dois locais e uma regra ILM que crie uma cópia de objeto em cada local, você deve adicionar armazenamento a cada local para aumentar a capacidade geral de objeto da grade.

Por motivos de desempenho, você deve tentar manter a capacidade de storage e o poder de computação equilibrados em todos os locais. Portanto, para este exemplo, você deve adicionar o mesmo número de nós

de storage a cada local ou volumes de storage adicionais em cada local.

Se você tiver uma política de ILM mais complexa que inclua regras que coloquem objetos em locais diferentes com base em critérios como nome do bucket ou regras que alterem os locais do objeto ao longo do tempo, sua análise de onde o armazenamento é necessário para a expansão será semelhante, mas mais complexa.

Traçar a rapidez com que a capacidade geral de armazenamento está sendo consumida pode ajudá-lo a entender quanto armazenamento adicionar na expansão e quando o espaço de armazenamento adicional será necessário. Você pode usar o Gerenciador de Grade para monitorar e mapear a capacidade de armazenamento, conforme descrito nas instruções para monitoramento e solução de problemas do StorageGRID.

Ao Planejar o momento de uma expansão, lembre-se de considerar quanto tempo pode levar para adquirir e instalar armazenamento adicional.

Informações relacionadas

"Gerenciar objetos com ILM"

"Monitorizar Resolução de problemas"

Adição de 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 número de nós que você precisa adicionar também depende de quão cheios os nós existentes estão quando você executa a expansão.

Recomendação geral para adicionar capacidade de storage para objetos codificados por apagamento

Se você quiser evitar cálculos detalhados, pode adicionar dois nós de storage por local quando os nós de storage existentes atingirem 70% de capacidade.

Esta recomendação geral fornece resultados razoáveis em uma ampla variedade de esquemas de codificação de apagamento para grades de um único local e para grades onde a codificação de apagamento fornece proteção contra perda de site.

Para entender melhor os fatores que levam a esta recomendação ou para desenvolver um plano mais preciso para o seu site, revise a próxima seção. Para obter uma recomendação personalizada otimizada para a sua situação, entre em Contato com o representante da sua conta NetApp.

Calculando o número de nós de storage de expansão a serem adicionados para objetos codificados por apagamento

Para otimizar a forma como você expande uma implantação que armazena objetos codificados por apagamento, considere muitos fatores:

- Esquema de codificação de apagamento em uso
- Características do pool de storage usado para codificação de apagamento, incluindo o número de nós em cada local e a quantidade de espaço livre em cada nó
- Se a grade foi expandida anteriormente (porque a quantidade de espaço livre por nó de storage pode não ser aproximadamente a mesma em todos os nós)
- Natureza exata da política ILM, como se as regras ILM fazem objetos replicados e codificados por apagamento

Os exemplos a seguir podem ajudar você a entender o impacto do esquema de codificação de apagamento, o número de nós no pool de storage e a quantidade de espaço livre em cada nó.

Considerações semelhantes afetam os cálculos de uma política de ILM que armazena dados replicados e codificados por apagamento e os cálculos de uma grade que foi expandida anteriormente.

> Os exemplos nesta seção representam as práticas recomendadas para adicionar capacidade de storage a um sistema StorageGRID. Se você não conseguir adicionar o número recomendado de nós, talvez seja necessário executar o procedimento de rebalanceamento EC para permitir que objetos codificados de apagamento adicionais sejam armazenados.
>
> "Considerações para rebalanceamento de dados codificados por apagamento"

Exemplo 1: Expandindo uma grade de um local que usa codificação de apagamento de 2 a 1

Este exemplo mostra como expandir uma grade simples que inclui apenas três nós de storage.

> Este exemplo usa apenas três nós de storage para simplificar. No entanto, o uso de apenas três nós de storage não é recomendado: Uma grade de produção real deve usar um mínimo de 1 nós de storage para redundância, o que equivale a quatro nós de storage (2-1-1) para este exemplo.

Assuma o seguinte:

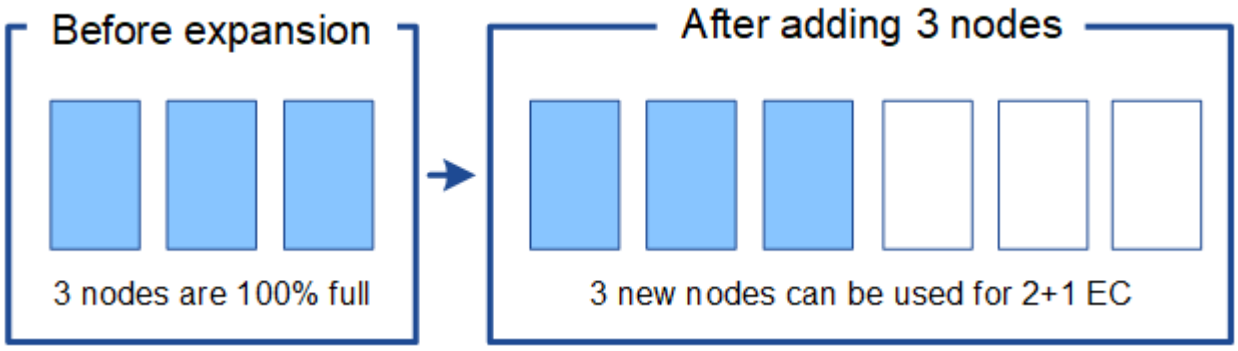
- Todos os dados são armazenados usando o esquema de codificação de apagamento 2-1. Com o esquema de codificação de apagamento 2-1, cada objeto é armazenado como três fragmentos e cada fragmento é salvo em um nó de storage diferente.
- Você tem um local com três nós de storage. Cada nó de storage tem uma capacidade total de 100 TB.
- Você deseja expandir adicionando novos nós de storage de 100 TB.
- No momento, você deseja equilibrar os dados codificados por apagamento entre os nós antigos e os novos.

Você tem várias opções, com base em quão cheios os nós de storage estão quando você executa a expansão.

- **Adicione três nós de storage de 100 TB quando os nós existentes estiverem 100% cheios**

Neste exemplo, os nós existentes estão 100% cheios. Como não há capacidade livre, você precisa adicionar imediatamente três nós para continuar a codificação de apagamento em mais de 1 horas por dia, 2 dias por semana.

Depois que a expansão for concluída, quando os objetos forem codificados para apagamento, todos os fragmentos serão colocados nos novos nós.

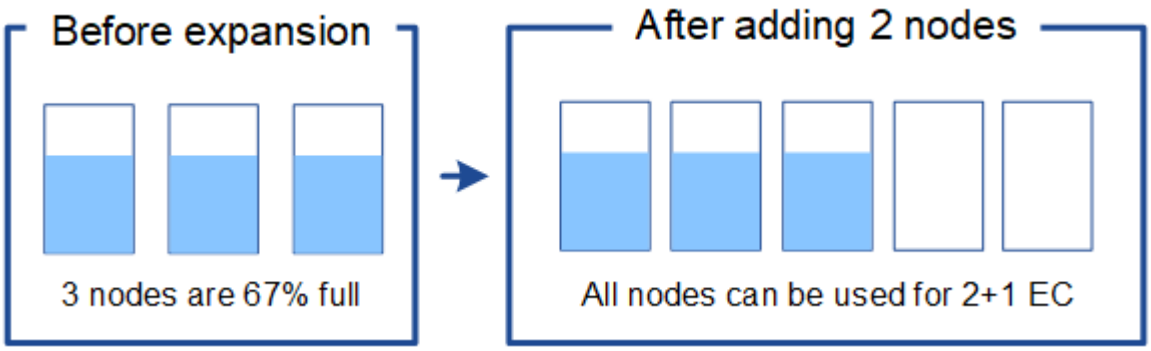


> Essa expansão adiciona nós *k m*. A adição de quatro nós é recomendada para redundância. Se você adicionar somente nós de armazenamento de expansão *k m* quando os nós existentes estiverem 100% cheios, todos os novos objetos deverão ser armazenados nos nós de expansão. Se algum dos novos nós ficar indisponível, mesmo temporariamente, o StorageGRID não poderá atender aos requisitos do ILM.

- **Adicione dois nós de storage de 100 TB, quando os nós de storage existentes estiverem 67% completos**

  Neste exemplo, os nós existentes estão 67% cheios. Como há 100 TB de capacidade livre nos nós existentes (33 TB por nó), você só precisa adicionar dois nós se você executar a expansão agora.

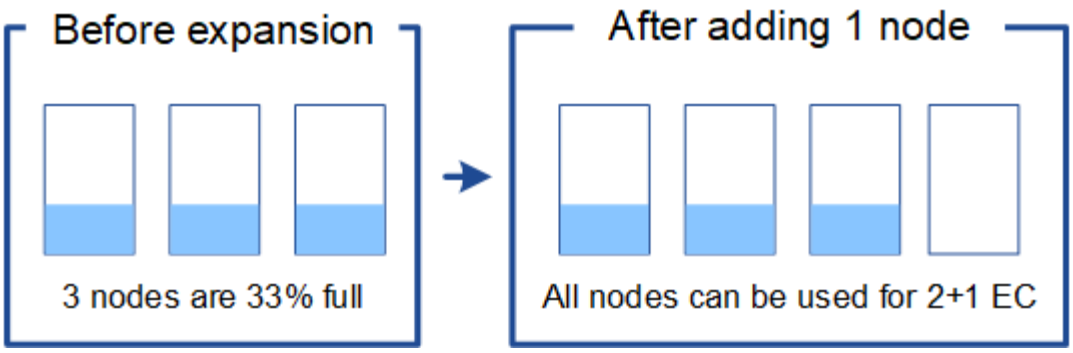
  A adição de 200 TB de capacidade adicional permite que você continue 2 a codificação de apagamento de mais de 1 TB e, eventualmente, equilibrar os dados codificados por apagamento em todos os nós.



- **Adicione um nó de storage de 100 TB quando os nós de storage existentes estiverem 33% cheios**

  Neste exemplo, os nós existentes estão 33% cheios. Como há 200 TB de capacidade livre nos nós existentes (67 TB por nó), você só precisa adicionar um nó se você executar a expansão agora.

  A adição de 100 TB de capacidade adicional permite que você continue 2 a codificação de apagamento de mais de 1 TB e, eventualmente, equilibrar os dados codificados por apagamento em todos os nós.



Exemplo 2: Expansão de uma grade de três locais que usa codificação de apagamento 6-3

Este exemplo mostra como desenvolver um plano de expansão para uma grade multi-site que tenha um esquema de codificação de apagamento com um número maior de fragmentos. Apesar das diferenças entre esses exemplos, o plano de expansão recomendado é muito semelhante.

Assuma o seguinte:

- Todos os dados são armazenados usando o esquema de codificação de apagamento 6-3. Com o esquema de codificação de apagamento 6-3, cada objeto é armazenado como 9 fragmentos e cada fragmento é salvo em um nó de storage diferente.
- Você tem três locais e cada local tem quatro nós de storage (12 nós no total). Cada nó tem uma capacidade total de 100 TB.
- Você deseja expandir adicionando novos nós de storage de 100 TB.
- No momento, você deseja equilibrar os dados codificados por apagamento entre os nós antigos e os novos.

Você tem várias opções, com base em quão cheios os nós de storage estão quando você executa a expansão.

- **Adicione nove nós de storage de 100 TB (três por local), quando os nós existentes estiverem 100% completos**

  Neste exemplo, os 12 nós existentes estão 100% cheios. Como não há capacidade livre, você precisa adicionar imediatamente nove nós (900 TB de capacidade adicional) para continuar a codificação de apagamento 6-3.

  Depois que a expansão for concluída, quando os objetos forem codificados para apagamento, todos os fragmentos serão colocados nos novos nós.

  > Essa expansão adiciona nós *k m*. A adição de 12 nós (quatro por local) é recomendada para redundância. Se você adicionar somente nós de armazenamento de expansão *k m* quando os nós existentes estiverem 100% cheios, todos os novos objetos deverão ser armazenados nos nós de expansão. Se algum dos novos nós ficar indisponível, mesmo temporariamente, o StorageGRID não poderá atender aos requisitos do ILM.

- **Adicione seis nós de storage de 100 TB (dois por local), quando os nós existentes estiverem 75% completos**

  Neste exemplo, os 12 nós existentes estão 75% cheios. Como há 300 TB de capacidade livre (25 TB por nó), você só precisa adicionar seis nós se você executar a expansão agora. Você adicionaria dois nós a

cada um dos três locais.

A adição de 600 TB de capacidade de storage permitirá que você continue 6 a codificação de apagamento de mais de 3 TB e, eventualmente, equilibrar os dados codificados por apagamento em todos os nós.

- **Adicione três nós de storage de 100 TB (um por local), quando os nós existentes estiverem 50% completos**

  Neste exemplo, os 12 nós existentes estão 50% cheios. Como há 600 TB de capacidade livre (50 TB por nó), você só precisa adicionar três nós se você executar a expansão agora. Você adicionaria um nó a cada um dos três locais.

  A adição de 300 TB de capacidade de storage permitirá que você continue 6 a codificação de apagamento de mais de 3 TB e, eventualmente, equilibrar os dados codificados por apagamento em todos os nós.

Informações relacionadas

"Gerenciar objetos com ILM"

"Monitorizar Resolução de problemas"

"Considerações para rebalanceamento de dados codificados por apagamento"

Considerações para rebalanceamento de dados codificados por apagamento

Se você estiver executando uma expansão para adicionar nós de storage e sua política de ILM incluir uma ou mais regras de ILM para apagar dados de código, talvez seja necessário executar o procedimento de rebalanceamento de EC após a conclusão da expansão.

Por exemplo, se você não puder adicionar o número recomendado de nós de storage em uma expansão, talvez seja necessário executar o procedimento de rebalanceamento EC para permitir que objetos codificados de apagamento adicionais sejam armazenados.

O que é o reequilíbrio CE?

O rebalanceamento EC é um procedimento StorageGRID que pode ser necessário após uma expansão do nó de storage. O procedimento é executado como um script de linha de comando a partir do nó de administração principal. Ao executar o procedimento de rebalancear, o StorageGRID redistribui fragmentos codificados por apagamento entre os nós de storage existentes e recém-expandidos em um local.

Quando o procedimento de reequilíbrio CE é executado:

- Ele apenas move dados de objetos codificados por apagamento. Ele não move dados de objetos replicados.
- Ele redistribui os dados em um local. Ele não move dados entre sites.
- Ele redistribui os dados entre todos os nós de storage em um local. Ele não redistribui dados dentro de volumes de storage.

Quando o procedimento de reequilíbrio CE estiver concluído:

- Os dados codificados por apagamento são movidos de nós de storage com menos espaço disponível para nós de storage com mais espaço disponível.

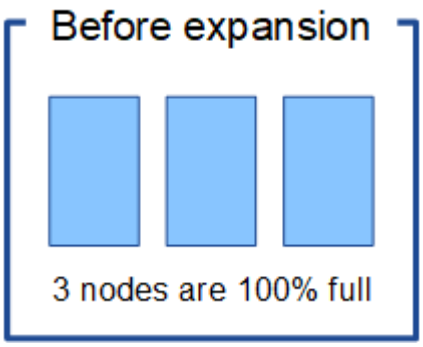
- Os valores usados (%) podem permanecer diferentes entre nós de storage porque o procedimento de rebalanceamento de EC não move cópias de objeto replicadas.
- A proteção de dados de objetos codificados por apagamento não será alterada.

Quando o procedimento de reequilíbrio EC está em execução, o desempenho das operações ILM e das operações dos clientes S3 e Swift provavelmente serão impactados. Por esse motivo, você só deve executar esse procedimento em casos limitados.

Quando não realizar um rebalanceamento EC

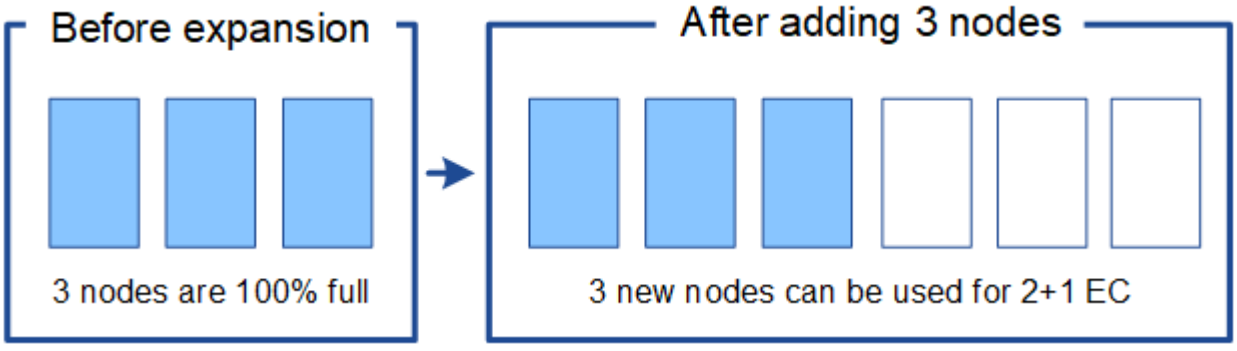
Como exemplo de quando você não precisa realizar um rebalanceamento EC, considere o seguinte:

- O StorageGRID é executado em um único local, que contém três nós de storage.
- A política ILM usa uma regra de codificação de apagamento de mais de 2 1 para todos os objetos com mais de 0,2 MB e uma regra de replicação de 2 cópias para objetos menores.
- Todos os nós de storage ficaram completamente cheios e o alerta **armazenamento de objetos baixos** foi acionado no nível de gravidade maior. A ação recomendada é executar um procedimento de expansão para adicionar nós de storage.



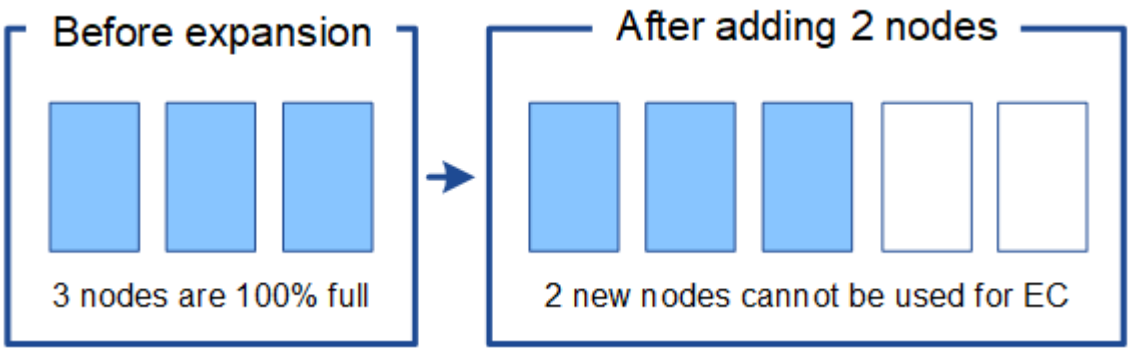
Para expandir o site neste exemplo, é recomendável adicionar três ou mais nós de storage novos. O StorageGRID precisa de três nós de storage para codificação de apagamento em mais de 1 horas por dia, 2 dias por semana, para que ele possa colocar os dois fragmentos de dados e um fragmento de paridade em nós diferentes.

Depois de adicionar os três nós de storage, os nós de storage originais permanecem cheios, mas os objetos podem continuar sendo ingeridos no 1 esquema de codificação de apagamento de mais de 2% nos novos nós. A execução do procedimento de reequilíbrio EC não é recomendada para este caso: A execução do procedimento diminuirá temporariamente o desempenho, o que pode afetar as operações do cliente.

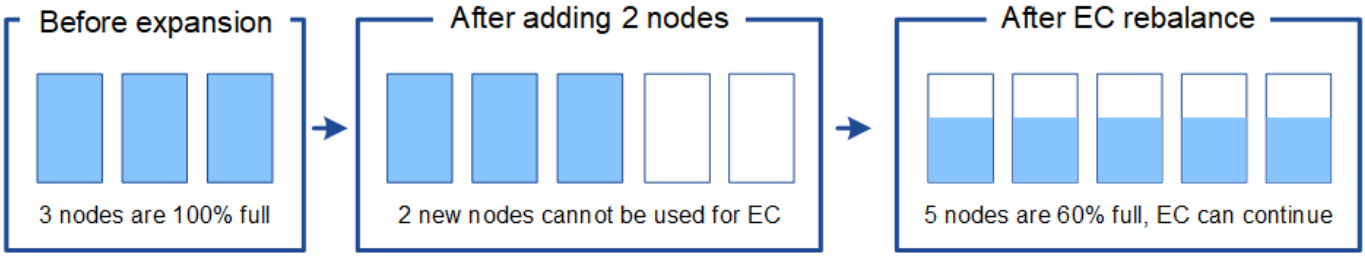


Quando realizar um rebalanceamento EC

Como exemplo de quando você deve executar o procedimento de rebalanceamento de EC, considere o mesmo exemplo, mas suponha que você só pode adicionar dois nós de storage. Como a codificação de apagamento de mais de 2 vezes por dia requer pelo menos 1 nós de storage, os novos nós não podem ser usados para dados codificados por apagamento.



Para resolver esse problema e usar os novos nós de storage, é possível executar o procedimento de rebalanceamento de EC. Quando esse procedimento é executado, o StorageGRID redistribui dados codificados de apagamento e fragmentos de paridade entre todos os nós de storage no local. Neste exemplo, quando o procedimento de rebalanceamento do EC estiver concluído, todos os cinco nós agora estão apenas 60% cheios e os objetos podem continuar a ser ingeridos no 2 esquema de codificação de apagamento de mais de 1 anos em todos os nós de storage.



Considerações para o reequilíbrio CE

Em geral, só deve executar o procedimento de reequilíbrio CE em casos limitados. Especificamente, você deve realizar o rebalanceamento EC somente se todas as seguintes afirmações forem verdadeiras:

- Você usa codificação de apagamento para seus dados de objeto.
- O alerta **Low Object Storage** foi acionado para um ou mais nós de storage em um local, indicando que os nós estão 80% ou mais cheios.
- Não é possível adicionar o número recomendado de novos nós de storage para o esquema de codificação de apagamento em uso.

  "Adição de capacidade de storage para objetos codificados por apagamento"

- Seus clientes S3 e Swift podem tolerar um desempenho inferior para suas operações de gravação e leitura enquanto o procedimento EC Rebalanceance está sendo executado.

Como o procedimento de reequilíbrio EC interage com outras tarefas de manutenção

Não é possível executar determinados procedimentos de manutenção ao mesmo tempo que está a executar o procedimento EC Rebalanceance.

Procedimento	Permitido durante o procedimento de reequilíbrio CE?
Procedimentos adicionais de reequilíbrio da CE	Não Só é possível executar um procedimento de rebalanceamento EC de cada vez.
Procedimento de desativação Trabalho de reparação de dados EC	Não • É impedido de iniciar um procedimento de desativação ou uma reparação de dados EC enquanto o procedimento de reequilíbrio EC está em execução. • É impedido de iniciar o procedimento de rebalanceamento EC enquanto um procedimento de desativação do nó de storage ou um reparo de dados EC estiver em execução.
Procedimento de expansão	Não Se você precisar adicionar novos nós de storage em uma expansão, aguarde para executar o procedimento de rebalanceamento do EC até que você tenha adicionado todos os novos nós. Se um procedimento de rebalanceamento do EC estiver em andamento quando você adicionar novos nós de storage, os dados não serão movidos para esses nós.
Procedimento de atualização	Não Se você precisar atualizar o software StorageGRID, execute o procedimento de atualização antes ou depois de executar o procedimento de rebalanceamento EC. Conforme necessário, você pode encerrar o procedimento EC Rebalanceance para realizar uma atualização de software.
Procedimento de clone de nó do dispositivo	Não Se você precisar clonar um nó de storage de dispositivo, aguarde para executar o procedimento de rebalanceamento do EC até que você tenha adicionado o novo nó. Se um procedimento de rebalanceamento do EC estiver em andamento quando você adicionar novos nós de storage, os dados não serão movidos para esses nós.
Procedimento de correção	Sim. Você pode aplicar um hotfix do StorageGRID enquanto o procedimento EC Rebalanceance estiver sendo executado.
Outros procedimentos de manutenção	Não Você deve terminar o procedimento EC Rebalanceance antes de executar outros procedimentos de manutenção.

Como o procedimento de reequilíbrio EC interage com o ILM

Enquanto o procedimento de rebalanceamento EC estiver em execução, evite fazer alterações no ILM que possam alterar o local dos objetos codificados por apagamento existentes. Por exemplo, não comece a usar uma regra ILM que tenha um perfil de codificação de apagamento diferente. Se você precisar fazer essas alterações no ILM, você deve abortar o procedimento EC Rebalancance.

Informações relacionadas

"Rebalanceamento de dados codificados por apagamento após a adição de nós de storage"

Adição de 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. Consulte as instruções para monitoramento e solução de problemas do StorageGRID para obter detalhes.

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.

Diretrizes para aumentar a capacidade dos metadados

Antes de adicionar nós de storage para aumentar a capacidade dos metadados, leia as diretrizes e limitações a seguir:

- Supondo que haja capacidade suficiente de storage de objetos disponível, ter mais espaço disponível para metadados de objetos aumenta o número de objetos que você pode armazenar no sistema StorageGRID.
- Você pode aumentar a capacidade de metadados de uma grade adicionando um ou mais nós de storage a cada local.
- O espaço real reservado para metadados de objetos em qualquer nó de armazenamento depende da opção de armazenamento de espaço reservado de metadados (configuração de todo o sistema), da quantidade de RAM alocada ao nó e do tamanho do volume do nó 0. Consulte as instruções para administrar o StorageGRID para obter mais informações.
- Você não pode aumentar a capacidade dos metadados adicionando volumes de storage aos nós de storage existentes, porque os metadados são armazenados apenas no volume 0.
- Você não pode aumentar a capacidade dos metadados adicionando um novo local.
- O StorageGRID mantém três cópias de todos os metadados de objetos em todos os locais. Por esse motivo, a capacidade de metadados do sistema é limitada pela capacidade de metadados do seu menor local.

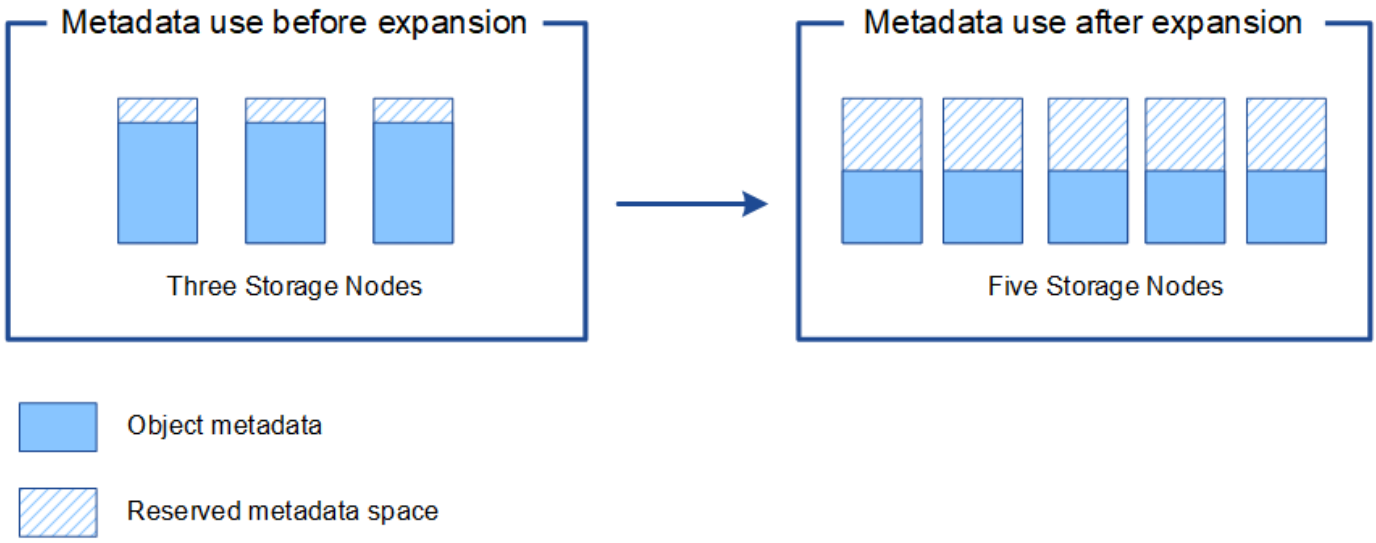
- Ao adicionar capacidade de metadados, você deve adicionar o mesmo número de nós de storage a cada local.

Como os metadados são redistribuídos quando você adiciona nós de storage

Quando você adiciona nós de storage a uma expansão, o StorageGRID redistribui os metadados de objetos existentes aos novos nós em cada local, o que aumenta a capacidade geral dos metadados da grade. Nenhuma ação do usuário é necessária.

A figura a seguir mostra como o StorageGRID redistribui os metadados de objetos quando você adiciona nós de storage em uma expansão. O lado esquerdo da figura representa o volume 0 de três nós de storage antes de uma expansão. Os metadados estão consumindo uma parte relativamente grande do espaço de metadados disponível de cada nó, e o alerta **armazenamento de metadados baixo** foi acionado.

O lado direito da figura mostra como os metadados existentes são redistribuídos depois que dois nós de storage são adicionados ao local. A quantidade de metadados em cada nó diminuiu, o alerta **armazenamento de metadados baixo** não é mais acionado e o espaço disponível para metadados aumentou.



Informações relacionadas

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

Adição de nós de grade para adicionar recursos ao seu sistema

Você pode adicionar redundância ou recursos adicionais a um sistema StorageGRID adicionando novos nós de grade a sites existentes.

Por exemplo, você pode optar por adicionar nós de Gateway adicionais para suportar a criação de grupos de alta disponibilidade de nós de Gateway, ou você pode adicionar um nó de administrador em um site remoto para permitir o monitoramento usando um nó local.

Você pode adicionar um ou mais dos seguintes tipos de nós a um ou mais locais existentes em uma única operação de expansão:

- Nós de administração não primários

- Nós de storage
- Nós de gateway
- Nós de arquivamento

Ao se preparar para adicionar nós de grade, esteja ciente das seguintes limitações:

- O nó de administração principal é implantado durante a instalação inicial. Não é possível adicionar um nó de administração principal durante uma expansão.
- Você pode adicionar nós de storage e outros tipos de nós na mesma expansão.
- Ao adicionar nós de storage, você deve Planejar cuidadosamente o número e o local dos novos nós.

  "Adição de capacidade de storage"

- Se você estiver adicionando nós de Arquivo, observe que cada nó de Arquivo só suporta fita por meio do middleware Tivoli Storage Manager (TSM).
- Se a opção **New Node Client Network Default** estiver definida como **unTrusted** na página redes de clientes não confiáveis, os aplicativos clientes que se conetam a nós de expansão usando a rede de cliente devem se conetar usando uma porta de endpoint do balanceador de carga (**Configuration** > **Network Settings** > **UnTrusted Client Network**). Consulte as instruções de administração do StorageGRID para alterar a configuração do novo nó e para configurar pontos de extremidade do balanceador de carga.

Informações relacionadas

"Administrar o StorageGRID"

Adicionar 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 informações sobre o monitoramento da capacidade de metadados de objetos, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

- Você deve considerar a largura de banda de rede disponível entre sites e o nível de latência de rede. As atualizações de metadados são continuamente replicadas entre sites, mesmo que todos os objetos sejam

armazenados apenas no local onde são ingeridos.

- Como o sistema StorageGRID permanece operacional durante a expansão, você deve revisar as regras do ILM antes de iniciar o procedimento de expansão. Você deve garantir que as cópias de objeto não sejam armazenadas no novo local até que o procedimento de expansão seja concluído.

  Por exemplo, antes de iniciar a expansão, determine se alguma regra usa o pool de storage padrão (todos os nós de storage). Se isso acontecer, você deverá criar um novo pool de storage que contenha os nós de storage existentes e atualizar suas regras de ILM para usar o novo pool de storage. Caso contrário, os objetos serão copiados para o novo site assim que o primeiro nó nesse site se tornar ativo.

  Para obter mais informações sobre como alterar o ILM ao adicionar um novo site, consulte o exemplo para alterar uma política ILM nas instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Informações relacionadas

"Gerenciar objetos com ILM"

Preparando-se para uma expansão

Você deve se preparar para a expansão do StorageGRID obtendo os materiais necessários e instalando e configurando qualquer novo hardware e redes.

Recolha de materiais necessários

Antes de executar uma operação de expansão, você deve reunir os materiais listados na tabela a seguir.

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 baixar e extrair os arquivos de instalação do StorageGRID. **Observação:** você não precisará 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 de cumprir os seguintes requisitos: • Porta de rede • Cliente SSH (por exemplo, PuTTY) • Navegador suportado
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.

Item	Notas
Documentação do StorageGRID	• *Administrando StorageGRID* • *Notas de versão do StorageGRID* • Instruções de instalação para a sua plataforma
Documentação atual para a sua plataforma	Para versões suportadas, consulte a Matriz de interoperabilidade.

Informações relacionadas

"Administrar o StorageGRID"

"Notas de lançamento"

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Transferir e extrair os ficheiros de instalação do StorageGRID

Antes de poder adicionar novos nós de grade ou um novo site, você deve baixar o arquivo de instalação apropriado do StorageGRID e extrair os arquivos.

Sobre esta tarefa

Você deve executar operações de expansão usando a versão do StorageGRID que está atualmente em

execução na grade.

Passos

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

   "NetApp Downloads: StorageGRID"

2. Selecione a versão do StorageGRID que está atualmente em execução na grade.
3. Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.
4. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.
5. Na coluna **Instalar StorageGRID** da página de download, selecione o `.tgz` arquivo ou `.zip` para sua plataforma.

   A versão apresentada no ficheiro de arquivo de instalação tem de corresponder à versão do software atualmente instalado.

   Use o `.zip` arquivo se você estiver executando o Windows no laptop de serviço.

Plataforma	Arquivo de instalação
VMware	StorageGRID-Webscale-*version*-VMware-*uniqueID*.zip StorageGRID-Webscale-*version*-VMware-*uniqueid*.tgz
Red Hat Enterprise Linux ou CentOS	StorageGRID-Webscale-*version*-RPM-*uniqueID*.zip StorageGRID-Webscale-*version*-RPM-*uniqueid*.tgz
Ubuntu ou Debian e appliance	StorageGRID-Webscale-*version*-DEB-*uniqueID*.zip StorageGRID-Webscale-*version*-DEB-*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 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.

Caminho e nome do arquivo	Descrição
	Uma licença gratuita que não fornece qualquer direito de suporte para o produto.
	O arquivo de disco da máquina virtual que é usado como um modelo para criar máquinas virtuais de nó de grade.
	O arquivo de modelo Open Virtualization Format (`.ovf`) e o arquivo de manifesto (`.mf`) para implantar o nó de administração principal.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de administração não primários.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de arquivamento.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós do Gateway.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de storage baseados em máquina virtual.
Ferramenta de script de implantação	Descrição
	Um script de shell Bash usado para automatizar a implantação de nós de grade virtual.
	Um arquivo de configuração de exemplo 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 fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.

Caminho e nome do arquivo	Descrição
	Um arquivo de configuração de exemplo para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.

9. Se estiver expandindo um sistema Red Hat Enterprise Linux ou CentOS, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.
	Uma licença gratuita que não fornece qualquer direito de suporte para o produto.
	Pacote RPM para instalar as imagens do nó StorageGRID em seus hosts RHEL ou CentOS.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL ou CentOS.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.
	Um arquivo de configuração de exemplo 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.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.

Caminho e nome do arquivo	Descrição
	Exemplo de função do Ansible e manual de estratégia para configurar hosts RHEL ou CentOS para implantação de contêineres do StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.

10. 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.
	Um arquivo de configuração de exemplo para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.

Caminho e nome do arquivo	Descrição
	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.

11. Se você estiver expandindo um sistema baseado no StorageGRID Appliance, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	DEB pacote para instalar as imagens do nó StorageGRID em seus dispositivos.
	Soma de verificação do pacote de instalação DEB usado pelo instalador do dispositivo StorageGRID para validar se o pacote está intacto após o upload.

> Para a instalação do dispositivo, esses arquivos só são necessários se você precisar evitar o tráfego de rede. O dispositivo pode baixar os arquivos necessários do nó de administração principal.

Verificação de hardware e rede

Antes de iniciar a expansão do sistema StorageGRID, você deve garantir que instalou e configurou o hardware necessário para oferecer suporte aos novos nós de grade ou ao novo site.

Para obter informações sobre versões suportadas, consulte a Matriz de interoperabilidade.

Você também deve verificar a conetividade de rede entre servidores no site e confirmar se o nó de administração principal pode se comunicar com todos os servidores de expansão destinados a hospedar o sistema StorageGRID.

Se você estiver executando uma atividade de expansão que inclua a adição de uma nova sub-rede, será necessário adicionar a nova sub-rede da grade antes de iniciar o procedimento de expansão.

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.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Atualizando sub-redes para a rede de Grade"

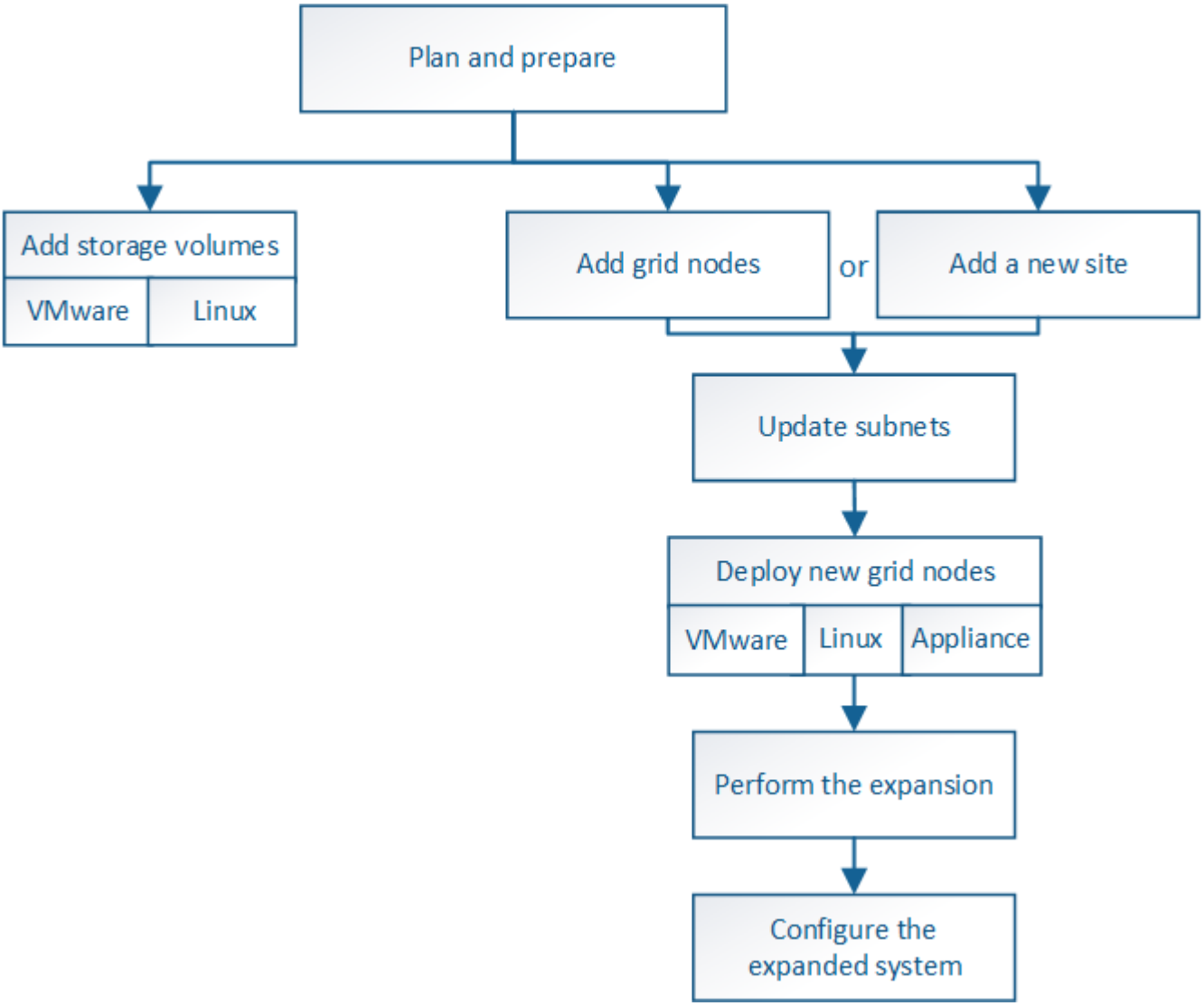
Visão geral do procedimento de expansão

As etapas básicas para executar uma expansão do StorageGRID variam para os diferentes tipos de expansão: Adicionar volumes de storage a um nó de storage, adicionar novos nós a um site existente ou adicionar um novo local. Em todos os casos, você pode realizar expansões sem interromper a operação do seu sistema atual.

O tipo de nó que você está adicionando à grade ou o motivo pelo qual você está adicionando nós não afeta o procedimento básico de expansão. Mas, como mostrado no diagrama de fluxo de trabalho abaixo, as etapas para adicionar nós variam ligeiramente dependendo se você está adicionando dispositivos StorageGRID ou hosts executando VMware ou Linux.

Arquivos de disco de máquina virtual fornecidos pela NetApp e scripts para novas instalações ou expansões do StorageGRID no OpenStack não são mais compatíveis. Para expandir uma implantação existente no OpenStack, consulte as etapas para sua distribuição Linux.

"Linux" refere-se a uma implantação Red Hat Enterprise Linux, Ubuntu, CentOS ou Debian. Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.



Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Planejando uma expansão do StorageGRID"

"Preparando-se para uma expansão"

"Adição de volumes de storage aos nós de storage"

"Adicionar nós de grade a um site existente ou adicionar um novo site"

Adição de volumes de storage aos nós de storage

Você pode expandir a capacidade de storage dos nós de storage que têm 16 ou menos volumes de storage adicionando volumes de storage adicionais. Talvez você precise adicionar volumes de storage a mais de um nó de storage para atender aos requisitos de ILM para cópias replicadas ou codificadas por apagamento.

O que você vai precisar

Antes de adicionar volumes de armazenamento, consulte as diretrizes para adicionar capacidade de armazenamento para garantir que você saiba onde adicionar volumes para atender aos requisitos da política de ILM.

"Adição de capacidade de storage"

> Estas instruções se aplicam somente a nós de storage baseados em software. Consulte as instruções de instalação e manutenção do dispositivo SG6060 para saber como adicionar volumes de armazenamento ao SG6060 instalando prateleiras de expansão. Não é possível expandir os nós de storage de outros dispositivos.
>
> "SG6000 dispositivos de armazenamento"

Sobre esta tarefa

O storage subjacente de um nó de storage é dividido em vários volumes de storage. Os volumes de armazenamento são dispositivos de armazenamento baseados em blocos que são formatados pelo sistema StorageGRID e montados para armazenar objetos. Cada nó de armazenamento pode suportar até 16 volumes de armazenamento, que são chamados *armazenamentos de objetos* no Gerenciador de Grade.

> Os metadados de objetos são sempre armazenados no armazenamento de objetos 0.

Cada armazenamento de objetos é montado em um volume que corresponde ao seu ID. Ou seja, o armazenamento de objetos com uma ID de 0000 corresponde ao `/var/local/rangedb/0` ponto de montagem.

Antes de adicionar novos volumes de armazenamento, use o Gerenciador de Grade para exibir os armazenamentos de objetos atuais para cada nó de armazenamento, bem como os pontos de montagem correspondentes. Você pode usar essas informações ao adicionar volumes de armazenamento.

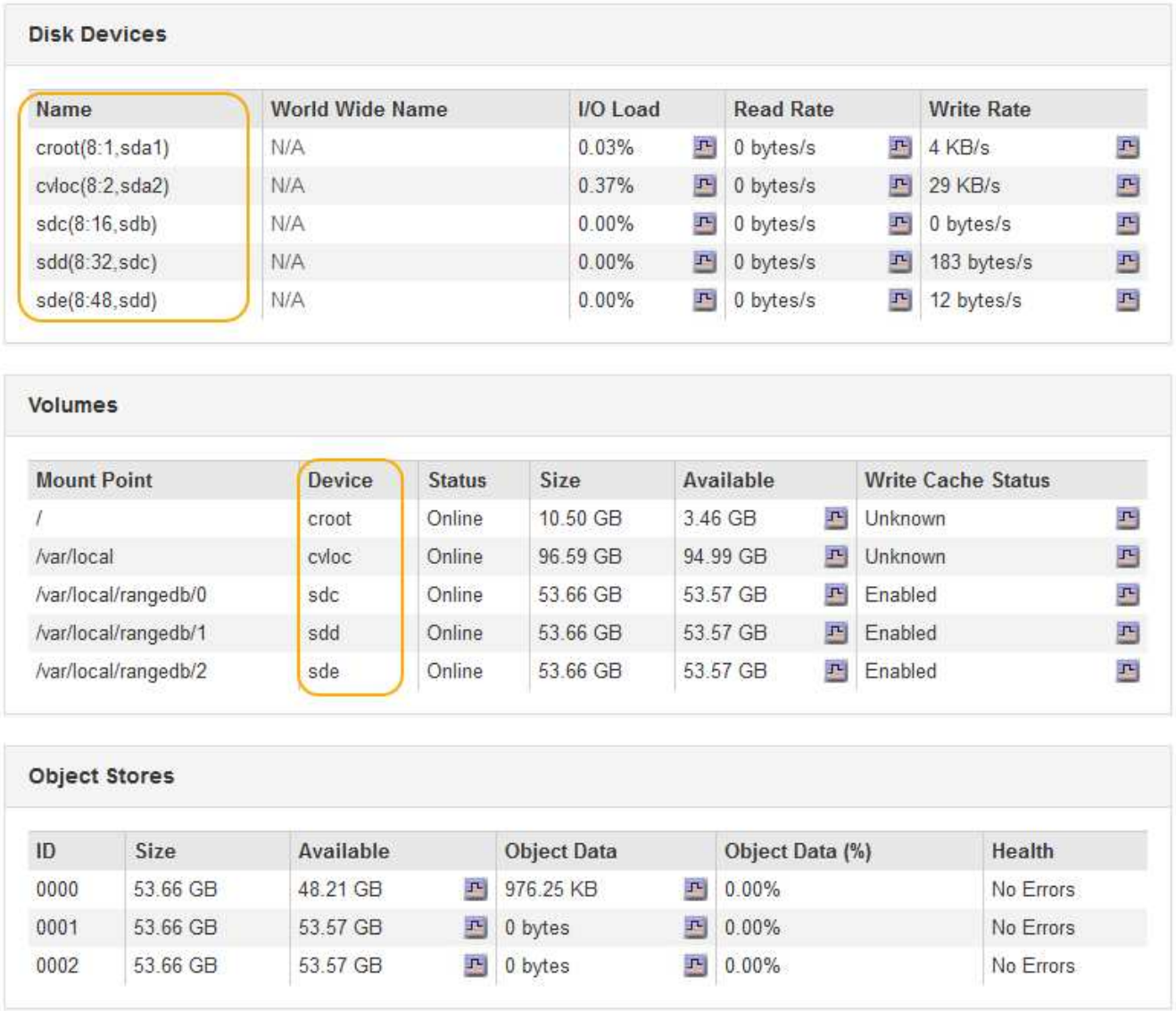
Passos

1. Selecione **nós** > ***site*** > ***Storage Node*** > **Storage**.

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

   Para nós de storage de dispositivo, o Nome Mundial para cada disco corresponde ao identificador mundial de volume (WWID) que aparece quando você visualiza as propriedades de volume padrão no software SANtricity (o software de gerenciamento 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
croot(8:1,sda1)	N/A	0.03%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.37%	0 bytes/s	29 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	0 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	183 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	12 bytes/s

Volumes

Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	10.50 GB	3.46 GB	Unknown
/var/local	cvloc	Online	96.59 GB	94.99 GB	Unknown
/var/local/rangedb/0	sdc	Online	53.66 GB	53.57 GB	Enabled
/var/local/rangedb/1	sdd	Online	53.66 GB	53.57 GB	Enabled
/var/local/rangedb/2	sde	Online	53.66 GB	53.57 GB	Enabled

Object Stores

ID	Size	Available	Object Data	Object Data (%)	Health
0000	53.66 GB	48.21 GB	976.25 KB	0.00%	No Errors
0001	53.66 GB	53.57 GB	0 bytes	0.00%	No Errors
0002	53.66 GB	53.57 GB	0 bytes	0.00%	No Errors

3. Siga as instruções da sua plataforma para adicionar novos volumes de armazenamento ao nó de armazenamento.
   - "VMware: Adicionando volumes de storage a um nó de storage"
   - "Linux: Adicionando volumes de SAN ou de conexão direta a um nó de storage"

VMware: Adicionando volumes de storage a um nó de storage

Se um nó de storage incluir menos de 16 volumes de storage, você poderá aumentar

sua capacidade usando o VMware vSphere para adicionar volumes.

O que você vai precisar

- Você deve ter acesso às instruções para instalar implantações do StorageGRID para VMware.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter permissões de acesso específicas.

> Não tente adicionar volumes de armazenamento a um nó de armazenamento enquanto uma atualização de software, procedimento de recuperação ou outro procedimento de expansão estiver ativo.

Sobre esta tarefa

O nó de armazenamento não está disponível por um breve período de tempo quando você adiciona volumes de armazenamento. Você deve executar este procedimento em um nó de storage de cada vez para evitar afetar os serviços de grade voltados para o cliente.

Passos

1. Se necessário, instale um novo hardware de armazenamento e crie novos armazenamentos de dados VMware.
2. Adicione um ou mais discos rígidos à máquina virtual para uso como armazenamento (armazenamentos de objetos).

   a. Abra o VMware vSphere Client.

   b. Edite as configurações da máquina virtual para adicionar um ou mais discos rígidos adicionais.

   Os discos rígidos são normalmente configurados como discos de máquina virtual (VMDKs). Os VMDKs são mais comumente usados e são mais fáceis de gerenciar, enquanto os RDMs podem fornecer melhor desempenho para cargas de trabalho que usam tamanhos de objetos maiores (por exemplo, maiores que 100 MB). Para obter mais informações sobre como adicionar discos rígidos a máquinas virtuais, consulte a documentação do VMware vSphere.

3. Reinicie a máquina virtual usando a opção **Restart Guest os** no VMware vSphere Client ou inserindo o seguinte comando em uma sessão ssh na máquina virtual:`sudo reboot`

   > Não use **Desligar** ou **Redefinir** para reiniciar a máquina virtual.

4. Configure o novo armazenamento para uso pelo nó de armazenamento:

   a. Faça login no nó da grade:

      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      iii. Digite o seguinte comando para mudar para root: `su -`

      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

   b. Configure os novos volumes de armazenamento:

   ```
   sudo add_rangedbs.rb
   ```

Este script encontra quaisquer novos volumes de armazenamento e solicita que você os formate.

a. Digite **y** para aceitar a formatação.
b. Se algum dos volumes tiver sido formatado anteriormente, decida se deseja reformatá-los.
   - Introduza **y** para reformatar.
   - Digite **n** para ignorar a reformatação. Os volumes de armazenamento são formatados.
c. Quando solicitado, digite **y** para interromper os serviços de armazenamento.

   Os serviços de armazenamento são interrompidos e o `setup_rangedbs.sh` script é executado automaticamente. Depois que os volumes estiverem prontos para uso como rangedbs, os serviços começam novamente.

5. Verifique se os serviços começam corretamente:

   a. Exibir uma lista do status de todos os serviços no servidor:

      ```
      sudo storagegrid-status
      ```

   O estado é atualizado automaticamente.

   a. Aguarde até que todos os serviços estejam em execução ou verificados.
   b. Saia do ecrã de estado:

      ```
      Ctrl+C
      ```

6. Verifique se o nó de storage está on-line:
   a. Faça login no Gerenciador de Grade usando um navegador compatível.
   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**.
7. 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.

Informações relacionadas

"Instale o VMware"

Linux: Adicionando volumes de SAN ou de conexão direta a um nó de storage

Se um nó de armazenamento incluir menos de 16 volumes de armazenamento, você poderá aumentar sua capacidade adicionando novos dispositivos de armazenamento de

bloco, tornando-os visíveis aos hosts Linux e adicionando os novos mapeamentos de dispositivo de bloco ao arquivo de configuração do StorageGRID usado para o nó de armazenamento.

O que você vai precisar

- Você deve ter acesso às instruções para instalar o StorageGRID para sua plataforma Linux.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter permissões de acesso específicas.

> Não tente adicionar volumes de armazenamento a um nó de armazenamento enquanto uma atualização de software, procedimento de recuperação ou outro procedimento de expansão estiver ativo.

Sobre esta tarefa

O nó de armazenamento não está disponível por um breve período de tempo quando você adiciona volumes de armazenamento. Você deve executar este procedimento em um nó de storage de cada vez para evitar afetar os serviços de grade voltados para o cliente.

Passos

1. Instale o novo hardware de armazenamento.

   Para obter mais informações, consulte a documentação fornecida pelo fornecedor de hardware.

2. Crie novos volumes de armazenamento de blocos dos tamanhos desejados.
   - Anexe as novas unidades de disco e atualize a configuração do controlador RAID conforme necessário, ou aloque os novos LUNs SAN nos storages de armazenamento compartilhados e permita que o host Linux os acesse.
   - Use o mesmo esquema de nomenclatura persistente usado para os volumes de storage no nó de storage existente.
   - Se você usar o recurso de migração de nó do StorageGRID, torne os novos volumes visíveis para outros hosts Linux que são destinos de migração para este nó de storage. Para obter mais informações, consulte as instruções para instalar o StorageGRID para sua plataforma Linux.
3. Faça login no host Linux que suporta o nó de storage como raiz ou com uma conta que tenha permissão sudo.
4. Confirme se os novos volumes de armazenamento estão visíveis no host Linux.

   Talvez seja necessário voltar a digitalizar dispositivos.

5. Execute o seguinte comando para desativar temporariamente o nó de armazenamento:

   ```
   sudo storagegrid node stop <node-name>
   ```

6. Usando um editor de texto como vim ou pico, edite o arquivo de configuração do nó para o nó de armazenamento, que pode ser encontrado em `/etc/storagegrid/nodes/<node-name>.conf`.
7. Localize a seção do arquivo de configuração do nó que contém os mapeamentos de dispositivo de bloco de armazenamento de objetos existentes.

   No exemplo, `BLOCK_DEVICE_RANGEDB_00` `BLOCK_DEVICE_RANGEDB_03` para são os mapeamentos de dispositivo de bloco de armazenamento de objetos existentes.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. Adicione novos mapeamentos de dispositivo de bloco de armazenamento de objetos correspondentes aos volumes de armazenamento de bloco adicionados para este nó de armazenamento.

   Certifique-se de começar no `BLOCK_DEVICE_RANGEDB_nn` próximo . Não deixe uma folga.

   - Com base no exemplo acima, comece em `BLOCK_DEVICE_RANGEDB_04`.
   - No exemplo abaixo, quatro novos volumes de armazenamento de bloco foram adicionados ao nó: `BLOCK_DEVICE_RANGEDB_04` Para `BLOCK_DEVICE_RANGEDB_07`.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
<strong>BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-
4</strong>
<strong>BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-
5</strong>
<strong>BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-
6</strong>
<strong>BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-
7</strong>
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. Execute o seguinte comando para validar suas alterações no arquivo de configuração do nó para o nó de armazenamento:

   `sudo storagegrid node validate <node-name>`

   Solucione quaisquer erros ou avisos antes de prosseguir para a próxima etapa.

   Se você observar um erro semelhante ao seguinte, isso significa que o arquivo de configuração do nó está tentando mapear o dispositivo de bloco usado por `<node-name>` para para para `<PURPOSE>` dado `<path-name>` no sistema de arquivos Linux, mas não há um arquivo especial válido de dispositivo de bloco (ou softlink para um arquivo especial de dispositivo de bloco) nesse local.

   ```
   Checking configuration file for node <node-name>…
   ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
   <path-name> is not a valid block device
   ```

   Verifique se você inseriu o `<path-name>` correto .

10. Execute o seguinte comando para reiniciar o nó com os novos mapeamentos de dispositivo de bloco em vigor:

    `sudo storagegrid node start <node-name>`

11. Faça login no nó de armazenamento como administrador usando a senha listada no `Passwords.txt` arquivo.
12. Verifique se os serviços começam corretamente:
    a. Veja uma lista do status de todos os serviços no servidor
       `sudo storagegrid-status`

       O estado é atualizado automaticamente.

    b. Aguarde até que todos os serviços estejam em execução ou verificados.
    c. Saia do ecrã de estado:

       `Ctrl+C`

13. Configure o novo armazenamento para uso pelo nó de armazenamento:
    a. Configure os novos volumes de armazenamento:

       `sudo add_rangedbs.rb`

    Este script encontra quaisquer novos volumes de armazenamento e solicita que você os formate.

    a. Digite **y** para formatar os volumes de armazenamento.
    b. Se algum dos volumes tiver sido formatado anteriormente, decida se deseja reformatá-los.
       - Introduza **y** para reformatar.

- Digite **n** para ignorar a reformatação. Os volumes de armazenamento são formatados.

c. Quando solicitado, digite **y** para interromper os serviços de armazenamento.

Os serviços de armazenamento são interrompidos e o `setup_rangedbs.sh` script é executado automaticamente. Depois que os volumes estiverem prontos para uso como rangedbs, os serviços começam novamente.

14. Verifique se os serviços começam corretamente:

a. Exibir uma lista do status de todos os serviços no servidor:

```
sudo storagegrid-status
```

O estado é atualizado automaticamente.

a. Aguarde até que todos os serviços estejam em execução ou verificados.

b. Saia do ecrã de estado:

```
Ctrl+C
```

15. Verifique se o nó de storage está on-line:

a. Faça login no Gerenciador de Grade usando um navegador compatível.

b. Selecione **Support** > **Tools** > **Grid Topology**.

c. Selecione ***site*** > ***Storage Node*** > **LDR** > **Storage**.

d. Selecione a guia **Configuração** e a guia **Principal**.

e. Se a lista suspensa **Estado de armazenamento - desejado** estiver definida como somente leitura ou Offline, selecione **Online**.

f. Clique em **aplicar alterações**.

16. Para ver os novos armazenamentos de objetos:

a. Selecione **nós** > ***site*** > ***Storage Node*** > **Storage**.

b. Veja os detalhes na tabela **Object Stores**.

Resultado

Agora você pode usar a capacidade expandida dos nós de storage para salvar dados de objetos.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Adicionar nós de grade a um site existente ou adicionar um novo site

Você pode seguir este procedimento para adicionar nós de grade a sites existentes ou adicionar um novo site, mas não pode executar ambos os tipos de expansão ao mesmo tempo.

O que você vai precisar

- Você deve ter permissões de root ou manutenção. Para obter detalhes, consulte informações sobre como

controlar o acesso ao sistema com contas e grupos de usuários de administração.

- Todos os nós existentes na grade devem estar ativos e em execução em todos os locais.
- Quaisquer procedimentos anteriores de expansão, atualização, desativação ou recuperação devem estar 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. "Atualizando sub-redes para a rede de Grade"
2. "Implantando novos nós de grade"
3. "Executando a expansão"

Atualizando sub-redes para a rede de Grade

Quando você adiciona nós de grade ou um novo site em uma expansão, talvez seja necessário atualizar ou adicionar sub-redes à rede de Grade.

O StorageGRID mantém uma lista das sub-redes de rede usadas para se comunicar entre nós de grade na rede de grade (eth0). Essas entradas incluem as sub-redes usadas para a rede de Grade por cada site em seu sistema StorageGRID, bem como quaisquer sub-redes usadas para NTP, DNS, LDAP ou outros servidores externos acessados através do gateway rede de Grade.

O que você vai precisar

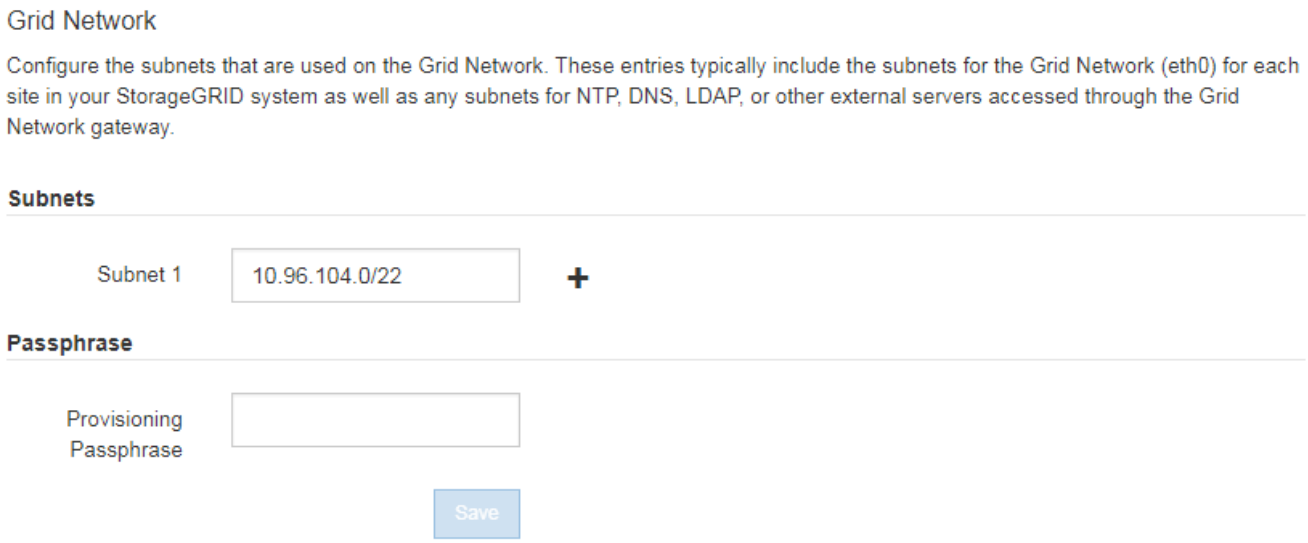
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter os endereços de rede, na notação CIDR, das sub-redes que deseja configurar.

Sobre esta tarefa

Se você estiver executando uma atividade de expansão que inclua a adição de uma nova sub-rede, será necessário adicionar a nova sub-rede da grade antes de iniciar o procedimento de expansão.

Passos

1. Selecione **Manutenção** > **rede** > **rede**.



2. Na lista de sub-redes, clique no sinal de mais para adicionar uma nova sub-rede na notação CIDR.

   Por exemplo, digite 10.96.104.0/22.

3. Digite a senha de provisionamento e clique em **Salvar**.

   As sub-redes especificadas são configuradas automaticamente para o sistema StorageGRID.

Implantando novos nós de grade

As etapas para implantar novos nós de grade em uma expansão são as mesmas que as etapas usadas quando a grade foi instalada pela primeira vez. Você deve implantar todos os novos nós de grade antes de executar a expansão.

Quando você expande a grade, os nós adicionados não precisam corresponder aos tipos de nó existentes. Você pode adicionar nós VMware, nós baseados em contêiner do Linux ou nós de dispositivo.

VMware: Implantando 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 de grade como uma 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.

   "Implantando um nó StorageGRID como uma máquina virtual"

2. Depois de implantar todos os novos nós VMware, retorne a estas instruções para executar o procedimento de expansão.

   "Executando a expansão"

Linux: Implantando nós de grade

Você pode implantar nós de grade em novos hosts Linux ou em hosts Linux existentes. Se você precisar de hosts Linux adicionais para dar suporte aos requisitos de CPU, RAM e storage dos nós StorageGRID que deseja adicionar à sua grade, você os prepara da mesma maneira que preparou os hosts quando os instalou pela primeira vez. Em seguida, você implanta os nós de expansão da mesma maneira que implantou nós de grade durante a instalação.

O que você vai precisar

- Você tem as instruções para instalar o StorageGRID para sua versão do Linux e analisou os requisitos de hardware e armazenamento.
- 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 AFF, 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.

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 executar a expansão.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Executando 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.

O que você vai precisar

- O dispositivo foi instalado em um rack ou gabinete, conetado às redes e ligado.
- Você usou o Instalador de dispositivos StorageGRID para concluir todas as etapas de ""configuração do hardware"" nas instruções de instalação e manutenção do dispositivo.

  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.
- A versão do Instalador de dispositivos StorageGRID no dispositivo de substituição corresponde à versão de software do seu sistema StorageGRID. (Se as versões não corresponderem, tem de atualizar o firmware do instalador do dispositivo StorageGRID.)

  Para obter instruções, consulte as instruções de instalação e manutenção do aparelho.

  - "Aparelhos de serviços SG100 SG1000"
  - "SG5600 dispositivos de armazenamento"
  - "SG5700 dispositivos de armazenamento"
  - "SG6000 dispositivos de armazenamento"
- 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.

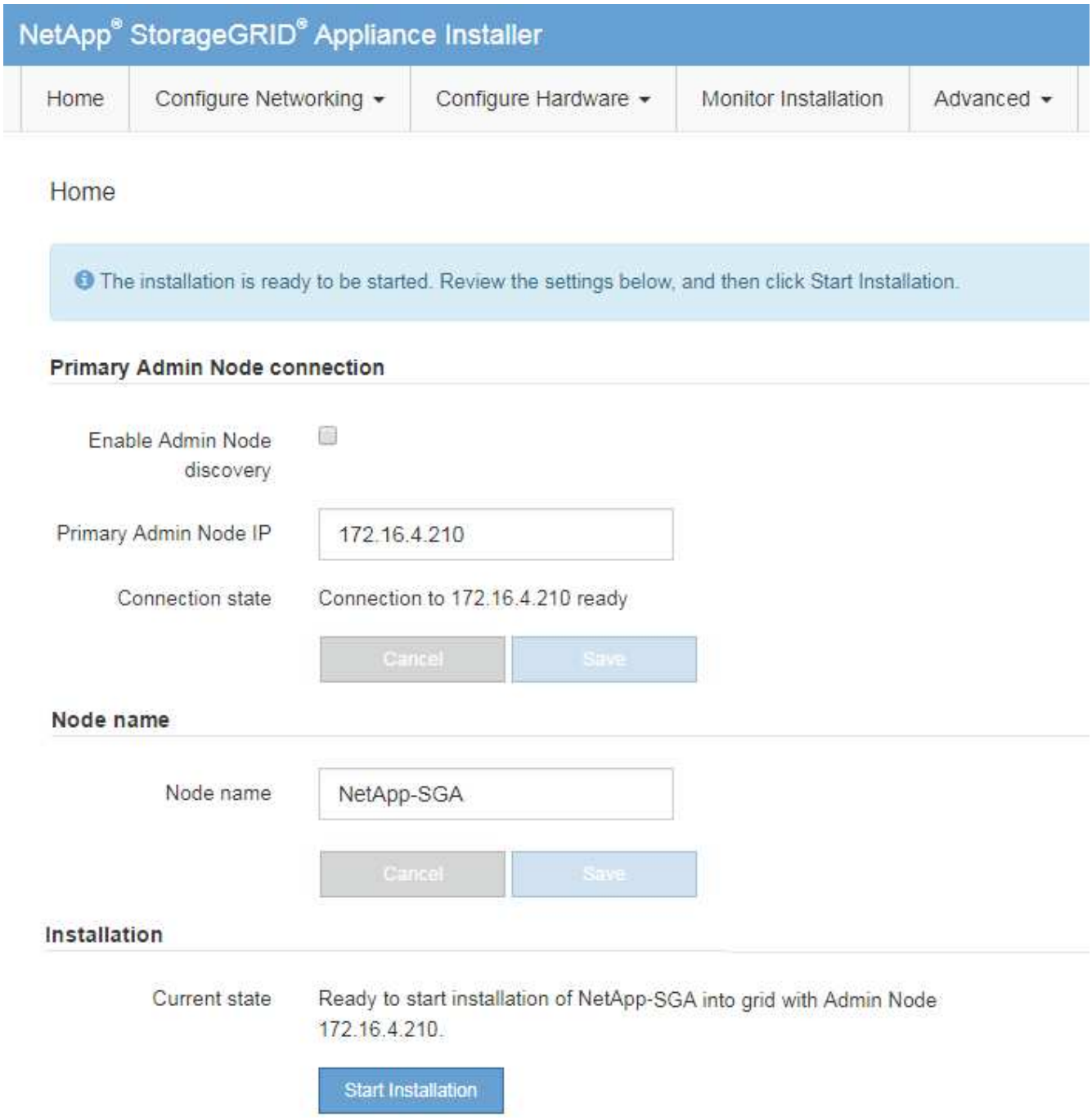
4. No campo **Nome do nó**, insira o nome que deseja usar para este nó de appliance e clique em **Salvar**.

   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 instalação e manutenção do seu aparelho.

6. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.



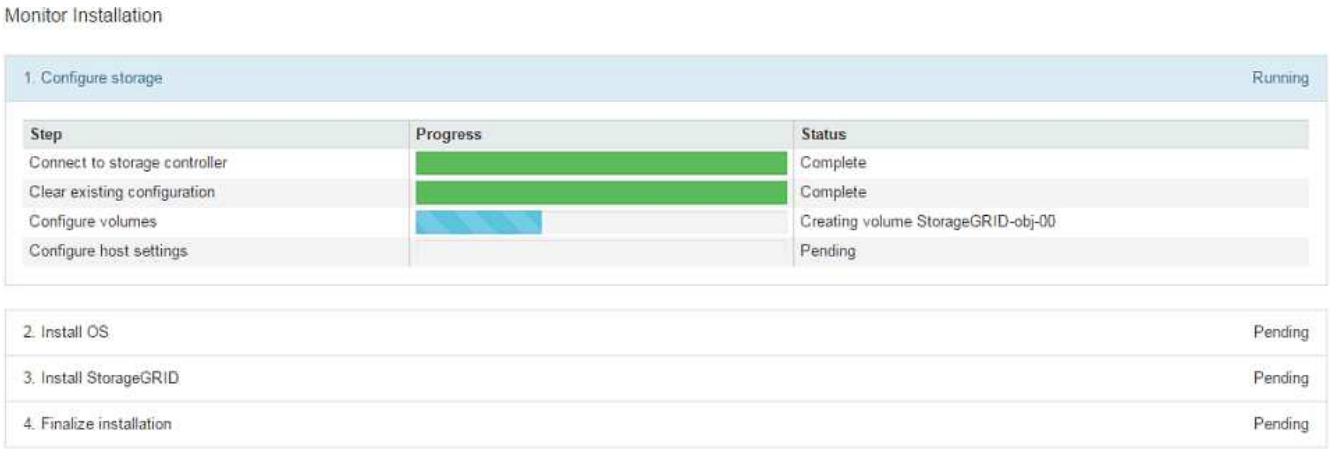
O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

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, clique em **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 serão mostradas com uma barra de status verde e um status de ""pulado"".

9. Reveja o progresso das duas primeiras fases de instalação.

1. Configure o appliance

Durante esta fase, ocorre um dos seguintes processos:

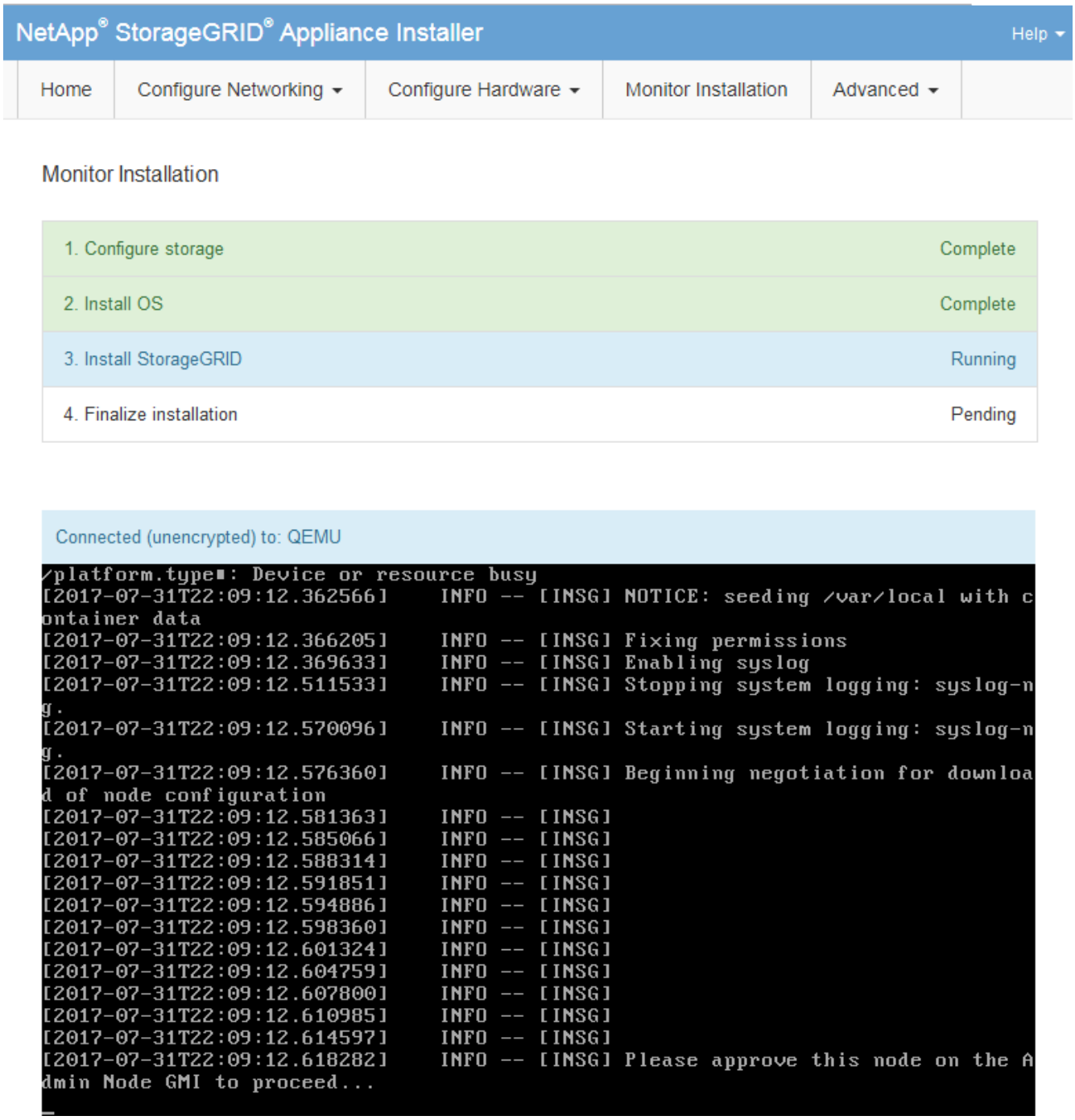
- Para um dispositivo de armazenamento, o instalador se coneta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o software SANtricity para configurar volumes e configura as configurações do host.
- Para um dispositivo de serviços, o instalador limpa qualquer configuração existente das unidades no controlador de computação e configura as configurações do host.

2. Instale o os

Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID para o dispositivo.

10. Continue monitorando o progresso da instalação até que uma mensagem seja exibida na janela do console, solicitando que você use o Gerenciador de Grade para aprovar o nó.

> Aguarde até que todos os nós adicionados nessa expansão estejam prontos para aprovação antes de ir para o Gerenciador de Grade para aprovar os nós.



Informações relacionadas

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"SG6000 dispositivos de armazenamento"

"Aparelhos de serviços SG100 SG1000"

Executando a expansão

Quando você executa a expansão, os novos nós de grade são adicionados à

implantação existente do StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado todos os nós de grade que estão sendo adicionados a essa expansão.
- Se estiver adicionando nós de storage, você deverá confirmar que todas as operações de reparo de dados executadas como parte de uma recuperação estão concluídas. Consulte os passos para verificar os trabalhos de reparação de dados nas instruções de recuperação e manutenção.
- Se você estiver adicionando um novo site, deverá revisar e atualizar as regras do ILM antes de iniciar o procedimento de expansão para garantir que as cópias de objeto não sejam armazenadas no novo site até que a expansão seja concluída. Por exemplo, se uma regra usar o pool de storage padrão (todos os nós de storage), será necessário criar um novo pool de storage que contenha apenas os nós de storage existentes e atualizar a regra ILM para usar o novo pool de storage. Caso contrário, os objetos serão copiados para o novo site assim que o primeiro nó nesse site se tornar ativo. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Sobre esta tarefa

A execução da expansão inclui estas fases:

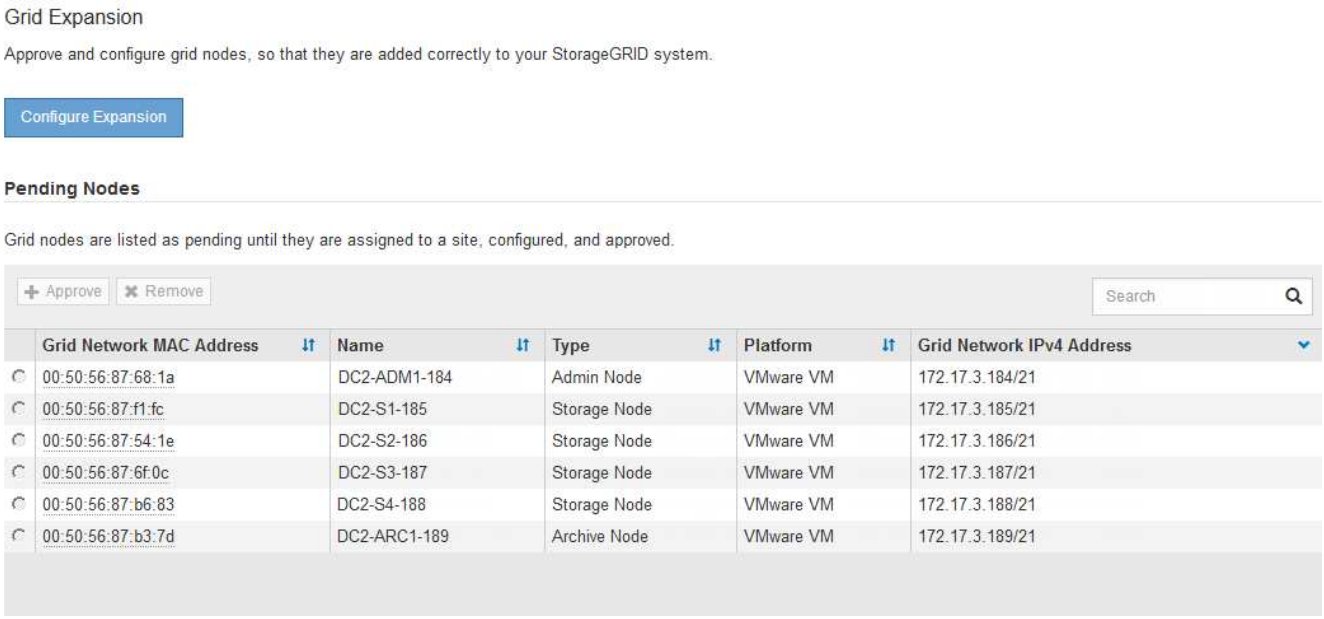
1. Configure a expansão especificando se você está adicionando novos nós de grade ou um novo site e aprovando os nós de grade que deseja adicionar.
2. Você inicia a expansão.
3. Enquanto o processo de expansão estiver em execução, você baixa um novo arquivo do Pacote de recuperação.
4. Você monitora o status das tarefas de configuração de grade, que são executadas automaticamente. O conjunto de tarefas depende de quais tipos de nós de grade estão sendo adicionados e se um novo site está sendo adicionado.

> Algumas tarefas podem levar uma quantidade significativa de tempo para serem executadas 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 relativamente 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. Você pode olhar para a porcentagem de "treamed" mostrada durante o estágio "iniciando Cassandra e streaming de dados" para determinar como é concluída a operação de streaming Cassandra.

Passos

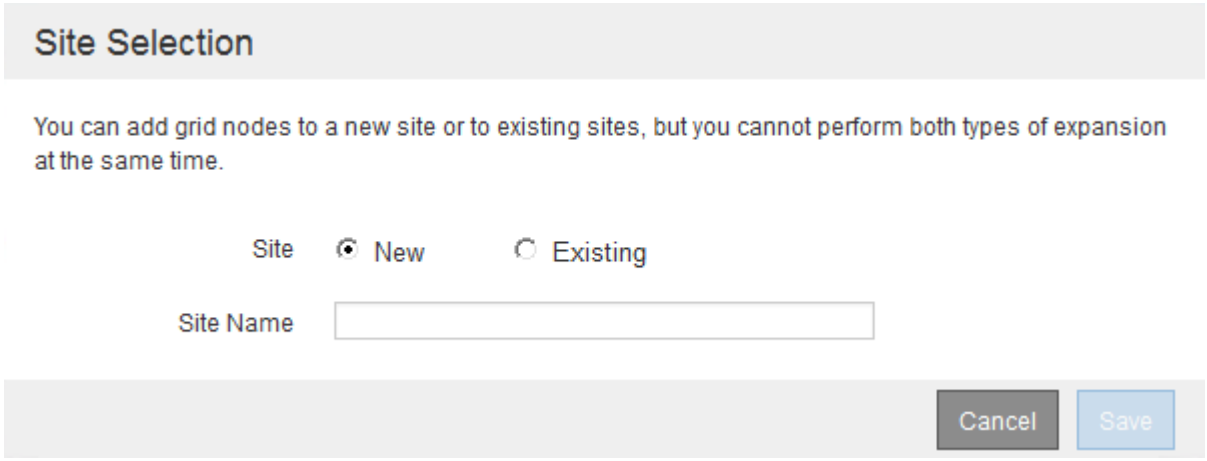
1. Selecione **Manutenção** > **tarefas de manutenção** > **expansão**.

   A página expansão da grade é exibida. A seção Pending Nodes lista todos os nós que estão prontos para serem adicionados.



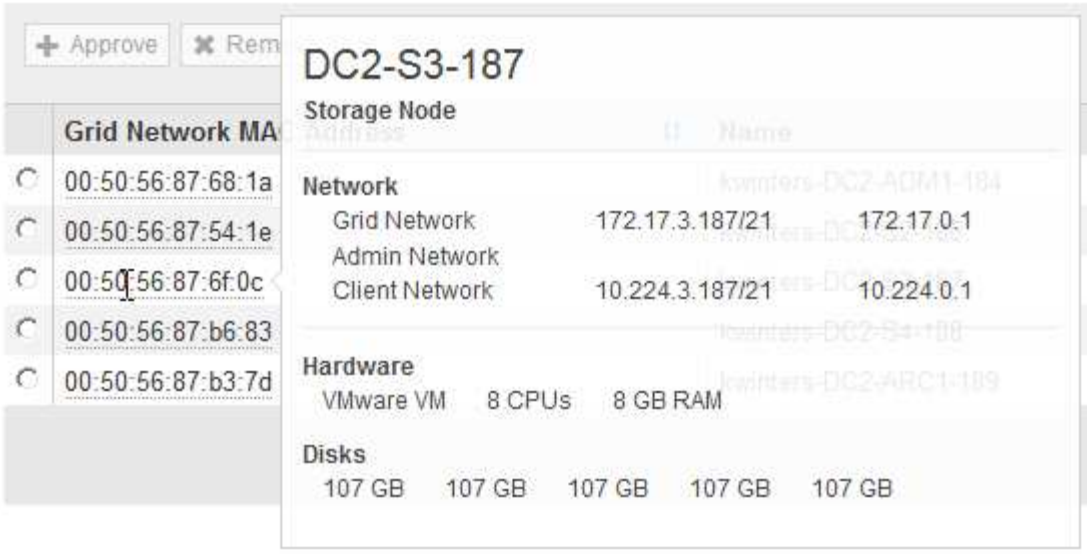
2. Clique em **Configurar expansão**.

   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 nós de grade a um site existente, selecione **existente**.
4. Clique em **Salvar**.
5. Revise a lista **Pending Nodes** e confirme que ela mostra todos os nós de grade implantados.

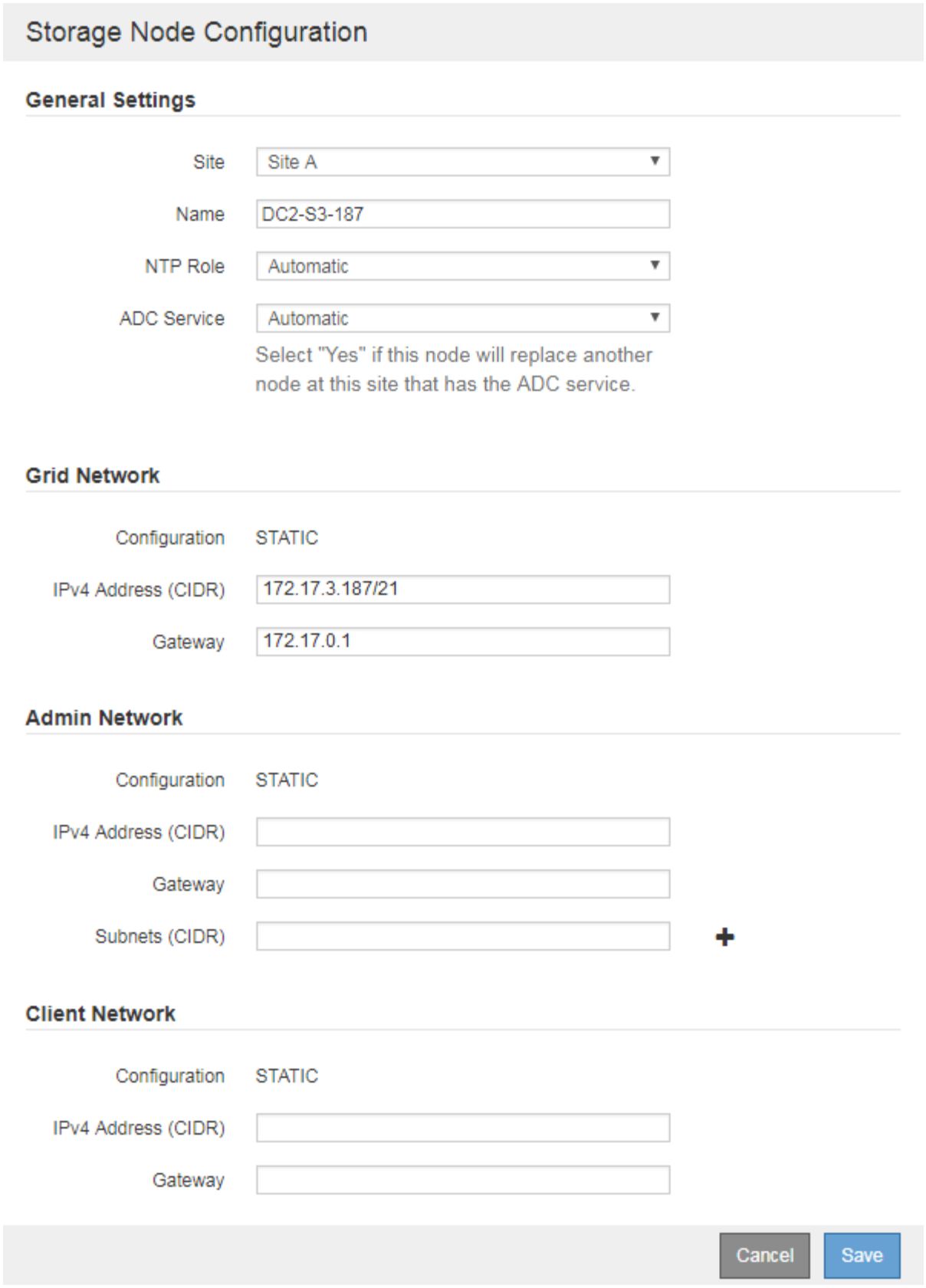
   Conforme necessário, você pode passar o cursor sobre o **Grid Network MAC Address** de um nó para ver detalhes sobre esse nó.



Se um nó de grade estiver ausente, confirme que ele foi implantado com sucesso.

6. Na lista de nós pendentes, aprove os nós de grade para essa expansão.
   a. Selecione o botão de opção ao lado do primeiro nó de grade pendente que você deseja aprovar.
   b. Clique em **Approve**.

      O formulário de configuração do nó de grade é exibido.



c. Conforme necessário, modifique as definições gerais:

- **Site**: O nome do site ao qual o nó da grade será associado. Se você estiver adicionando vários nós, certifique-se de selecionar o local correto para cada nó. Se você estiver adicionando um novo site, todos os nós serão adicionados ao novo site.

- **Nome**: O nome do host que será atribuído ao nó e o nome que será exibido no Gerenciador de Grade.
- **Função NTP**: A função Network Time Protocol (NTP) do nó de grade. As opções são **Automático**, **primário** e **Cliente**. A seleção de **Automático** atribui a função primária a nós de administração, nós de armazenamento com serviços ADC, nós de gateway e quaisquer nós de grade que tenham endereços IP não estáticos. Todos os outros nós de grade recebem a função Cliente.

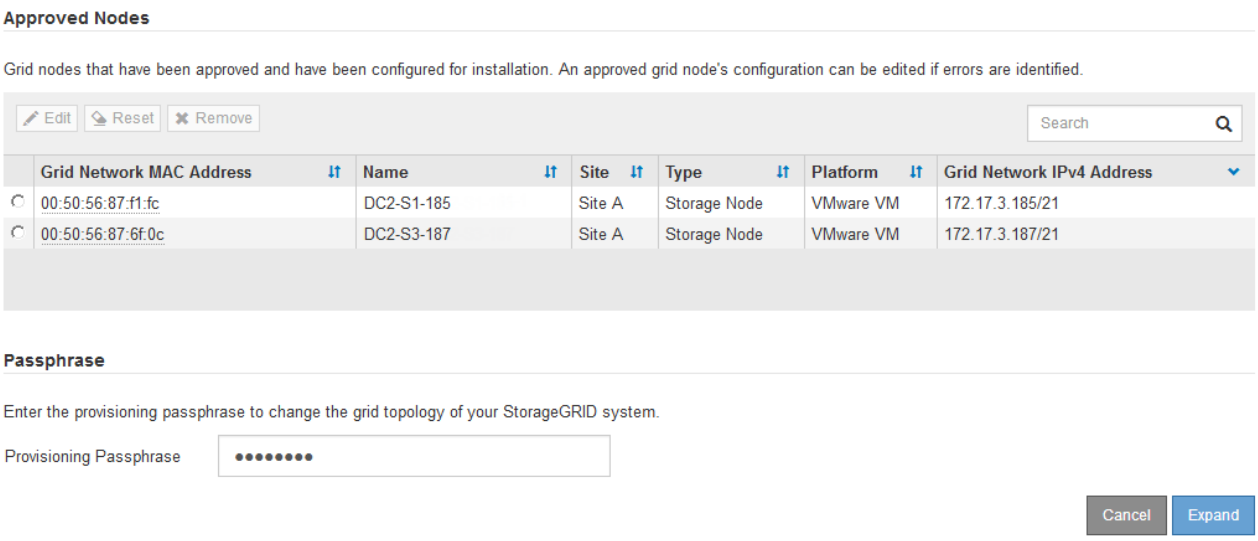
  > Atribua a função NTP primária a pelo menos dois nós em cada local. Isso fornece acesso redundante ao sistema a fontes de temporização externas.

- **ADC Service** (somente nós de armazenamento): Se este nó de armazenamento executará o serviço controlador de domínio administrativo (ADC). O serviço ADC mantém o controle da localização e disponibilidade dos serviços da grade. Pelo menos três nós de storage em cada local devem incluir o serviço ADC. Você não pode adicionar o serviço ADC a um nó depois que ele é implantado.
  - Se você estiver adicionando esse nó para substituir um nó de armazenamento, selecione **Sim** se o nó que você está substituindo incluir o serviço ADC. Como você não pode desativar um nó de armazenamento se houver poucos serviços ADC, isso garante que um novo serviço ADC esteja disponível antes que o serviço antigo seja removido.
  - Caso contrário, selecione **Automático** para permitir que o sistema determine se esse nó requer o serviço ADC. Saiba mais sobre o quórum ADC nas instruções de recuperação e manutenção.

d. Conforme necessário, modifique as configurações para rede de Grade, rede de Admin e rede de cliente.
   - **Endereço IPv4 (CIDR)**: O endereço de rede CIDR para a interface de rede. Por exemplo: 172.16.10.100/24
   - **Gateway**: O gateway padrão do nó de grade. Por exemplo: 172.16.10.1
   - **Sub-redes (CIDR)**: Uma ou mais sub-redes para a rede Admin.

e. Clique em **Salvar**.

   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 clique em **Edit**.

- Para mover um nó de grade aprovado de volta para a lista de nós pendentes, selecione seu botão de opção e clique em **Redefinir**.
- Para remover permanentemente um nó de rede aprovado, desligue o nó. Em seguida, selecione o botão de opção e clique em **Remover**.

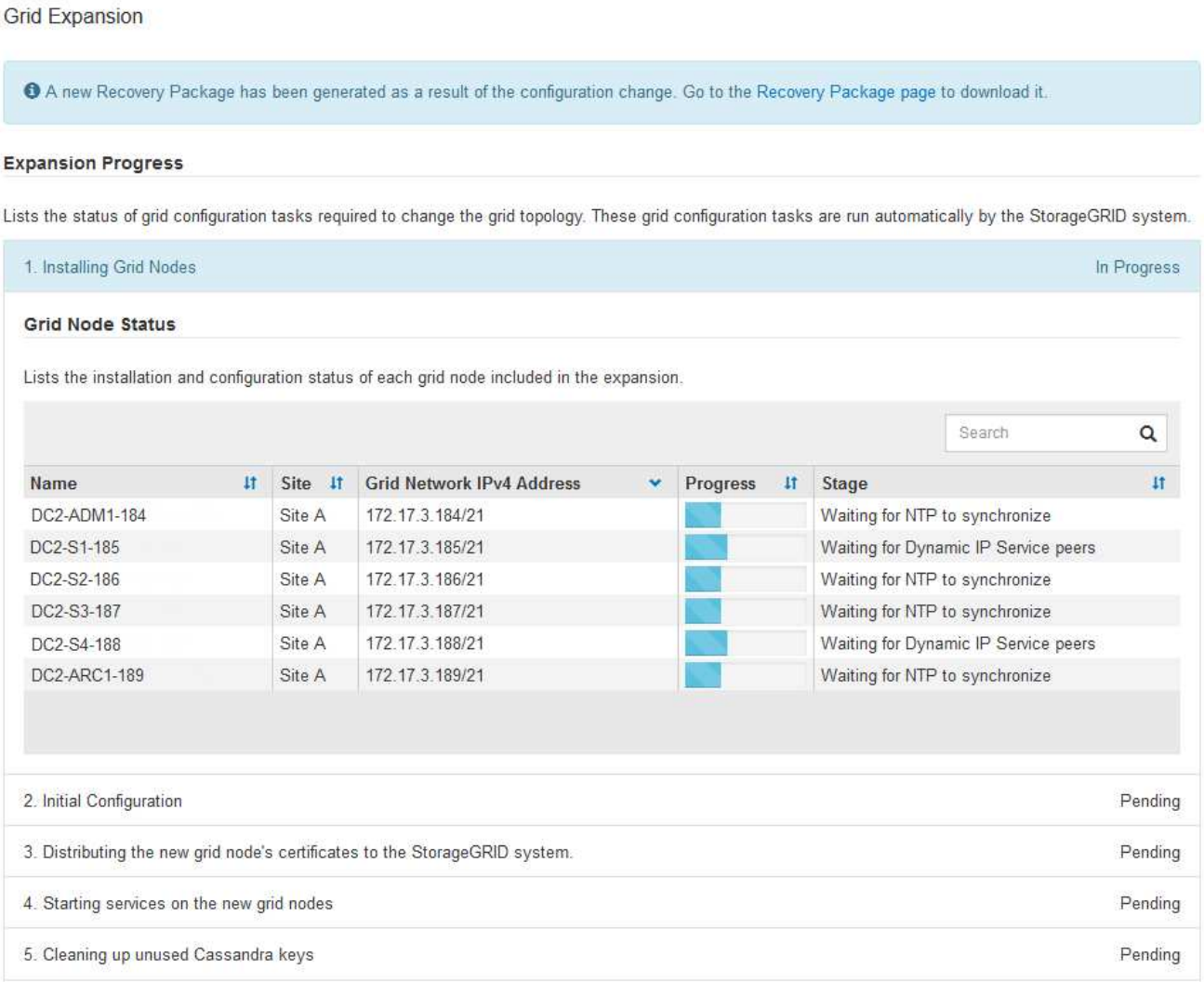
f. Repita estas etapas para cada nó de grade pendente que você deseja aprovar.

> 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 clique em **expandir**.

   Após alguns minutos, esta página é atualizada para exibir o status do procedimento de expansão. Quando as tarefas que afetam o nó de grade individual estão em andamento, a seção Status do nó de grade lista o status atual de cada nó de grade.

> Durante esse processo, para os aparelhos, o Instalador do StorageGRID Appliance mostra a instalação passando do Estágio 3 para o Estágio 4, finalize a Instalação. Quando a fase 4 é concluída, o controlador é reinicializado.



Uma expansão de site inclui uma tarefa adicional para configurar o Cassandra para o novo site.

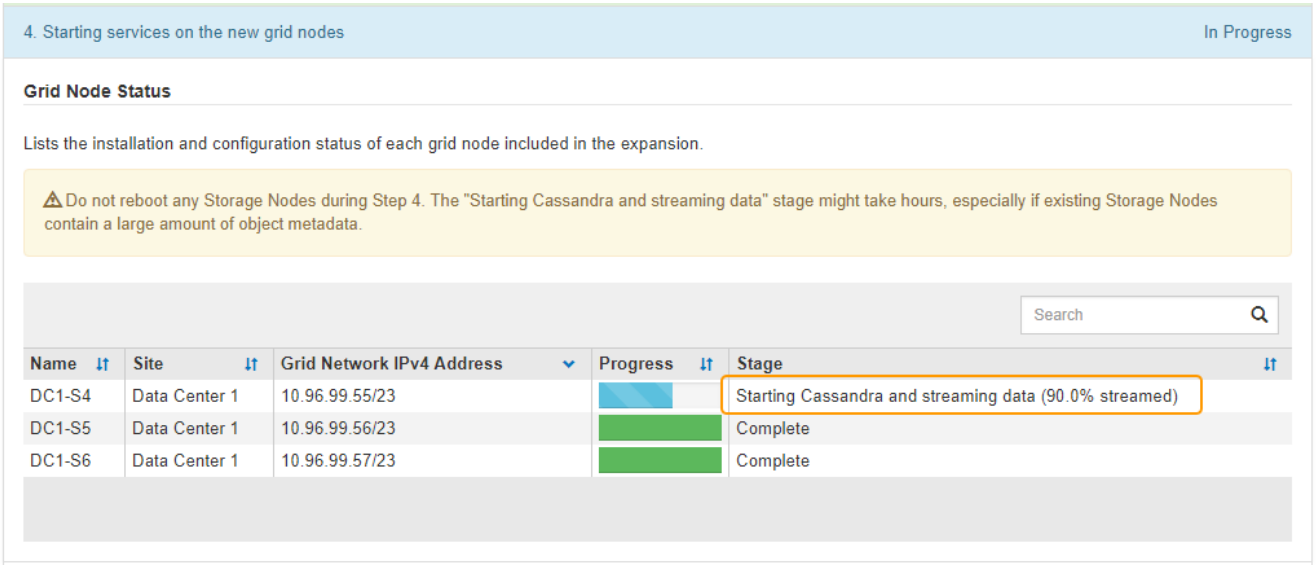
8. Assim que o link **Download Recovery Package** for exibido, baixe o arquivo Recovery Package.

   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. Clique no link de download.
   b. Digite a senha de provisionamento e clique em **Iniciar download**.
   c. Quando o download for concluído, abra o `.zip` arquivo e confirme que ele inclui um `gpt-backup` diretório e um `_SAID.zip` arquivo. Em seguida, extraia o `_SAID.zip` arquivo, vá para `/GID*_REV*` o diretório e confirme que você pode abrir o `passwords.txt` arquivo.
   d. Copie o arquivo do Pacote de recuperação baixado (.zip) para dois locais seguros, seguros e separados.

   O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

9. Se você estiver adicionando um ou mais nós de storage, monitore o progresso da etapa ""iniciando Cassandra e streaming de dados"", revisando a porcentagem mostrada na mensagem de status.



   Essa porcentagem estima o quão completa é a operação de streaming do Cassandra, com base na quantidade total de dados do Cassandra disponíveis e na quantidade que já foi gravada no novo nó.

   Não reinicie nenhum nó de storage durante a Etapa 4 (iniciando serviços nos novos nós de grade). A etapa "'iniciando Cassandra e streaming de dados'" pode levar horas para ser concluída para cada novo nó de storage, especialmente se os nós de storage existentes contiverem uma grande quantidade de metadados de objetos.

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, você deve executar etapas adicionais de integração e configuração.

Informações relacionadas

"Gerenciar objetos com ILM"

"Manter recuperar"

"Configurando seu sistema StorageGRID expandido"

Configurando seu sistema StorageGRID expandido

Depois de concluir uma expansão, você deve executar etapas adicionais de integração e configuração.

Sobre esta tarefa

Você deve concluir as tarefas de configuração listadas abaixo para os nós de grade que você está adicionando em sua expansão. Algumas tarefas podem ser opcionais, dependendo das opções selecionadas durante a instalação e administração do sistema, e como você deseja configurar os nós de grade adicionados durante a expansão.

Passos

1. Se você adicionou um nó de storage, execute as seguintes tarefas de configuração.

Tarefas de configuração do nó de storage	Para obter informações
Revise os pools de armazenamento usados em suas regras de ILM para garantir que o novo armazenamento será usado. • Se você adicionou um site, crie um pool de armazenamento para o site e atualize as regras do ILM para usar o novo pool de armazenamento. • Se você adicionou um nó de armazenamento a um site existente, confirme se o novo nó usa o grau de armazenamento correto. **Observação:** por padrão, um novo nó de armazenamento é atribuído ao nível de armazenamento de todos os nós de armazenamento e adicionado a pools de armazenamento que usam essa classificação para o site. Se você quiser que um novo nó use um grau de armazenamento personalizado, você deve atribuí-lo manualmente ao grau personalizado (**ILM** > **graus de armazenamento**).	"Gerenciar objetos com ILM"
Verifique se o nó de armazenamento está ingerindo objetos.	"Verificando se o nó de storage está ativo"
Rebalancear os dados codificados por apagamento (somente se você não conseguir adicionar o número recomendado de nós de storage).	"Rebalanceamento de dados codificados por apagamento após a adição de nós de storage"

2. Se você adicionou um nó de gateway, execute as seguintes tarefas de configuração.

Tarefas de configuração do Gateway Node	Para obter informações
Se forem utilizados grupos de alta disponibilidade para ligações de clientes, adicione os nós de Gateway a um grupo de HA. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade** para revisar a lista de grupos de HA existentes e adicionar os novos nós.	"Administrar o StorageGRID"

3. Se você adicionou um nó Admin, execute as seguintes tarefas de configuração.

Tarefas de configuração do nó de administração	Para obter informações
Se o logon único estiver ativado para o seu sistema StorageGRID, você deverá criar uma confiança de parte confiável nos Serviços de Federação do ative Directory (AD FS) para o novo nó de administração. Você não pode entrar no nó até criar essa confiança de parte confiável.	"Configurando logon único"
Se você planeja usar o serviço Load Balancer em nós de administração, talvez seja necessário adicionar os nós de administração a grupos de alta disponibilidade. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade** para revisar a lista de grupos de HA existentes e adicionar os novos nós.	"Administrar o StorageGRID"
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.	"Copiando o banco de dados Admin Node"
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.	"Copiando métricas Prometheus"
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"
Opcionalmente, configure o acesso ao sistema para fins de auditoria por meio de um compartilhamento de arquivos NFS ou CIFS. **Observação:** a exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.	"Administrar o StorageGRID"

Tarefas de configuração do nó de administração	Para obter informações
Opcionalmente, altere o remetente preferido para notificações. Você pode tornar o nó de administração de expansão o remetente preferido. Caso contrário, um nó de administração existente configurado como o remetente preferido continua a enviar notificações, incluindo mensagens AutoSupport, notificações SNMP, e-mails de alerta e e-mails de alarme (sistema legado).	"Administrar o StorageGRID"

4. Se tiver adicionado um nó de arquivo, conclua as seguintes tarefas de configuração.

Tarefas de configuração do nó de arquivamento	Para obter informações
Configure a ligação do nó de arquivo ao sistema de armazenamento de arquivo externo de destino. Quando você conclui a expansão, os nós de arquivo estão em um estado de alarme até que você configure as informações de conexão através do componente **ARC** > **Target**.	"Administrar o StorageGRID"
Atualize a política ILM para arquivar dados de objetos através do novo nó de arquivo.	"Gerenciar objetos com ILM"
Configure alarmes personalizados para os atributos usados para monitorar a velocidade e a eficiência da recuperação de dados de objetos a partir de nós de arquivo.	"Administrar o StorageGRID"

5. Para verificar se os nós de expansão foram adicionados a uma rede cliente não confiável ou para alterar se a rede cliente de um nó não é confiável ou confiável, vá para **Configuração** > **Configurações de rede** > **rede cliente não confiável**.

   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. Consulte as instruções para administrar o StorageGRID para obter mais informações.

6. Configure o sistema de nomes de domínio (DNS).

   Se você tiver especificado as configurações de DNS separadamente para cada nó de grade, você deve adicionar configurações de DNS personalizadas por nó para os novos nós. Consulte informações sobre como modificar a configuração DNS para um único nó de grade nas instruções de recuperação e manutenção.

   A melhor prática é que a lista de servidores DNS em toda a grade contenha alguns servidores DNS que são acessíveis localmente a partir de cada site. Se você acabou de adicionar um novo site, adicione novos servidores DNS para o site à configuração DNS em toda a grade.

   > Forneça dois a seis endereços IPv4 para servidores DNS. Você deve selecionar servidores DNS que cada site pode acessar localmente no caso de rede ser aterrissada. Isso é para garantir que um site islanded continua a ter acesso ao serviço DNS. Depois de configurar a lista de servidores DNS em toda a grade, você pode personalizar ainda mais a lista de servidores DNS para cada nó. Para obter detalhes, consulte as informações sobre como modificar a configuração DNS nas instruções de recuperação e manutenção.

7. Se você adicionou um novo site, confirme se os servidores NTP (Network Time Protocol) estão acessíveis a partir desse site.

> 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.

Para obter mais informações, consulte as instruções de recuperação e manutenção.

Informações relacionadas

"Gerenciar objetos com ILM"

"Verificando se o nó de storage está ativo"

"Copiando o banco de dados Admin Node"

"Copiando métricas Prometheus"

"Copiar registos de auditoria"

"Atualizar o software"

"Manter recuperar"

Verificando 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 compatível.
2. Selecione **nós** > ***Expansion Storage Node*** > **Storage**.
3. Passe o cursor sobre o gráfico **Storage Used - Object Data** (armazenamento usado - dados do objeto) para visualizar o valor para **Used**, que é a quantidade total de espaço utilizável que foi usada para dados do objeto.
4. Verifique se o valor de **usado** está aumentando à medida que você move o cursor para a direita no gráfico.

Copiando o banco de dados Admin Node

Ao adicionar nós de administração através de um procedimento de expansão, você pode opcionalmente copiar o banco de dados do nó de administração principal para o novo nó de administração. Copiar o banco de dados permite que você retenha informações históricas sobre atributos, alertas e alertas.

O que você vai precisar

- Você deve ter concluído as etapas de expansão necessárias para adicionar um nó de administrador.

- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter a senha de provisionamento.

Sobre esta tarefa

O processo de ativação do software StorageGRID cria um banco de dados vazio para o serviço NMS no nó de administração de expansão. Quando o serviço NMS é iniciado no nó de administração de expansão, ele Registra informações para servidores e serviços que atualmente fazem parte do sistema ou adicionados mais tarde. Este banco de dados Admin Node inclui as seguintes informações:

- Histórico de alertas
- Histórico de alarmes
- Dados de atributos históricos, que são usados nos gráficos e relatórios de texto disponíveis na página **Support** > **Tools** > **Grid Topology**

Para garantir que o banco de dados do nó de administração seja consistente entre nós, você pode copiar o banco de dados do nó de administração principal para o nó de administração de expansão.

> Copiar o banco de dados do nó Admin principal (o nó 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`

Copiando métricas Prometheus

Depois de adicionar um novo nó Admin, você pode opcionalmente copiar as métricas históricas mantidas pelo Prometheus do nó Admin primário para o novo nó Admin. Copiar as métricas garante que as métricas históricas sejam consistentes entre os nós de administração.

O que você vai precisar

- O novo nó de administração deve ser instalado e em execução.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter 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. Você pode copiar logs de auditoria de um nó de administrador instalado anteriormente para o novo nó de administrador de expansão, de modo que ele esteja sincronizado com o resto do sistema StorageGRID.

O que você vai precisar

- Você deve ter concluído as etapas de expansão necessárias para adicionar um nó de administrador.
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Para disponibilizar as mensagens de auditoria histórica de outros nós de administração no nó de administração de expansão, você deve copiar os arquivos de log de auditoria manualmente do nó de administração principal ou de outro nó de administração existente para o nó de administração de expansão.

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. Renomeie `audit.log` o arquivo para garantir que ele não substitua o arquivo no nó de administração de expansão para o qual você está copiando:

   ```
   cd /var/local/audit/export
   ls -l E
   mv audit.log new_name.txt
   ```
4. Copiar todos os arquivos de log de auditoria para o nó de administração de expansão:

   ```
   scp -p * IP_address:/var/local/audit/export
   ```
5. Se for solicitada a senha para `/root/.ssh/id_rsa`, digite a senha de acesso SSH para o nó de administração principal listado no `Passwords.txt` arquivo.
6. Restaure o arquivo original `audit.log`:

   ```
   mv new_name.txt audit.log
   ```
7. Inicie o serviço AMS:

   ```
   service ams start
   ```
8. Terminar sessão a partir do servidor:

   ```
   exit
   ```
9. Faça login no nó de administração de expansão:
   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 `#`.
10. Atualize as configurações de usuário e grupo para os arquivos de log de auditoria:

    ```
    cd /var/local/audit/export E
    chown ams-user:bycast *
    ```

11. Terminar sessão a partir do servidor:

```
exit
```

Rebalanceamento de dados codificados por apagamento após a adição de nós de storage

Em alguns casos, talvez você precise rebalancear os dados codificados por apagamento após adicionar novos nós de storage.

O que você vai precisar

- Você deve ter concluído as etapas de expansão para adicionar os novos nós de storage.
- Você precisa ter revisado as considerações para reequilibrar os dados codificados por apagamento.

  "Considerações para rebalanceamento de dados codificados por apagamento"

> Execute este procedimento somente se o alerta **armazenamento de objetos baixos** tiver sido acionado para um ou mais nós de armazenamento em um local e você não conseguir adicionar o número recomendado de novos nós de armazenamento.

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

Sobre esta tarefa

Quando o procedimento de reequilíbrio EC está em execução, o desempenho das operações ILM e das operações dos clientes S3 e Swift provavelmente serão impactados. Por esse motivo, você só deve executar esse procedimento em casos limitados.

> O procedimento de reequilíbrio CE reserva temporariamente uma grande quantidade de armazenamento. Os alertas de storage podem ser acionados, mas serão resolvidos quando o rebalancear for concluído. Se não houver armazenamento suficiente para a reserva, o procedimento de reequilíbrio CE falhará. As reservas de armazenamento são liberadas quando o procedimento de reequilíbrio CE for concluído, independentemente de o procedimento ter falhado ou ter êxito.

> As operações S3 e Swift API para carregar objetos (ou partes de objetos) podem falhar durante o procedimento de rebalanceamento EC se precisarem de mais de 24 horas para serem concluídas. As OPERAÇÕES PUT de longa duração falharão se a regra ILM aplicável usar um posicionamento rigoroso ou equilibrado na ingestão. Será comunicado o seguinte erro:
>
> `500 Internal Server Error`

Passos

1. Revise os detalhes de armazenamento de objetos atuais para o site que você planeja reequilibrar.
   a. Selecione **nós**.
   b. Selecione o primeiro nó de storage no local.
   c. Selecione a guia **armazenamento**.
   d. Passe o cursor sobre o gráfico Storage Used - Object Data (armazenamento usado - dados de objetos) para ver a quantidade atual de dados replicados e dados codificados por apagamento no Storage Node.

e. Repita estas etapas para exibir os outros nós de storage no local.

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

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

3. Introduza o seguinte comando:

   ```
   rebalance-data start --site "site-name"
   ```

   Para "*site-name*", especifique o primeiro local em que você adicionou novos nós ou nós de storage. Inclua `site-name` em citações.

   O procedimento de reequilíbrio EC é iniciado e um ID de tarefa é retornado.

4. Copie a ID do trabalho.
5. Acompanhar o estado do procedimento de reequilíbrio CE.
   - Para visualizar o estado de um procedimento único de reequilíbrio CE:

     ```
     rebalance-data status --job-id job-id
     ```

     Para *job-id*, especifique o ID que foi retornado quando você iniciou o procedimento.
   - Para visualizar o estado do atual procedimento de reequilíbrio CE e de quaisquer procedimentos concluídos anteriormente:

     ```
     rebalance-data status
     ```

   > Para obter ajuda sobre o comando rebalanceamento-data:
   >
   > ```
   > rebalance-data --help
   > ```

6. Execute etapas adicionais, com base no status retornado:
   - Se o estado indicar `In progress`, a operação de reequilíbrio CE continua a funcionar. Você deve monitorar periodicamente o procedimento até que ele seja concluído.
   - Se o estado indicar `Failure`, efetuar o passos de falha.
   - Se o estado indicar `Success`, efetuar o etapa de sucesso.
7. Se o procedimento de reequilíbrio EC estiver gerando muita carga (por exemplo, as operações de ingestão são afetadas), interrompa o procedimento.

   ```
   rebalance-data pause --job-id job-id
   ```

8. Se você precisar encerrar o procedimento de rebalanceamento EC (por exemplo, para que você possa executar uma atualização de software StorageGRID), digite o seguinte:

`rebalance-data abort --job-id job-id`

> Quando você encerrar um procedimento de rebalanceamento do EC, todos os fragmentos de dados que já foram movidos permanecem no novo local. Os dados não são movidos de volta para o local original.

9. se o status do procedimento EC Rebalanceance for `Failure`, siga estas etapas:
   a. Confirme se todos os nós de storage no local estão conetados à grade.
   b. Verifique e resolva quaisquer alertas que possam estar afetando esses nós de storage.

      Para obter informações sobre alertas específicos, consulte as instruções de monitoramento e solução de problemas.

   c. Reinicie o procedimento de reequilíbrio CE
      `rebalance-data start --job-id job-id`
   d. Se o estado do procedimento de reequilíbrio CE persistir `Failure`, contactar o suporte técnico.
10. se o status do procedimento de rebalanceamento EC for `Success`, opcionalmente revise o armazenamento de objetos para ver os detalhes atualizados do local.

    Agora, os dados codificados por apagamento devem ser mais equilibrados entre os nós de storage no local.

    > Os dados de objeto replicados não são movidos pelo procedimento de rebalanceamento EC.

11. Se você estiver usando codificação de apagamento em mais de um site, execute este procedimento para todos os outros sites afetados.

Informações relacionadas

"Considerações para rebalanceamento de dados codificados por apagamento"

"Monitorizar Resolução de problemas"

Contactar o suporte técnico

Se você encontrar erros durante o processo de expansão da grade que você não consegue resolver ou se uma tarefa de grade falhar, entre em Contato com o suporte técnico.

Sobre esta tarefa

Ao entrar em Contato com o suporte técnico, você deve fornecer os arquivos de log necessários para ajudar a solucionar os erros que você está encontrando.

Passos

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 contentor Docker 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 iniciar sessão como root, o aviso muda de `$` para `#`.

2. Dependendo do estágio em que a instalação chegou, recupere qualquer um dos seguintes logs que estão disponíveis no nó da grade:

Plataforma	Registos
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
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 a recuperação

Saiba como aplicar um hotfix; recuperar um nó de grade com falha; desativar nós de grade e sites; e recuperar objetos em caso de falha do sistema.

- "Introdução à recuperação e manutenção do StorageGRID"
- "Procedimento de correção do StorageGRID"
- "Procedimentos de recuperação do nó de grade"
- "Como a recuperação do local é realizada pelo suporte técnico"
- "Procedimento de desativação"
- "Procedimentos de manutenção da rede"
- "Procedimentos de nível de host e middleware"
- "Procedimentos do nó de grade"
- "Clonagem do nó do dispositivo"

Introdução à recuperação e manutenção do StorageGRID

Os procedimentos de recuperação e manutenção do StorageGRID incluem a aplicação de um hotfix de software, a recuperação de nós de grade, a recuperação de um site com

falha, a desativação de nós de grade ou um site inteiro, a execução de manutenção de rede, a execução de procedimentos de manutenção de middleware e nível de host e a execução de procedimentos de nó de grade.

Todas as atividades de recuperação e manutenção exigem uma ampla compreensão do sistema StorageGRID. Você deve revisar a topologia do sistema StorageGRID para garantir que você entenda a configuração da grade.

Você deve seguir todas as instruções exatamente e atender a todos os avisos.

Os procedimentos de manutenção não descritos não são suportados nem requerem um envolvimento dos serviços.

Para obter os procedimentos de hardware, consulte as instruções de instalação e manutenção do seu dispositivo StorageGRID.

> "Linux" refere-se a uma implantação Red Hat Enterprise Linux, Ubuntu, CentOS ou Debian. Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

Informações relacionadas

"Primário de grelha"

"Diretrizes de rede"

"Administrar o StorageGRID"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Transferir o pacote de recuperação

O arquivo do pacote de recuperação permite restaurar o sistema StorageGRID se ocorrer uma falha.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a senha de provisionamento.
- Você deve ter permissões de acesso específicas.

Faça o download do arquivo atual do Pacote de recuperação antes de fazer alterações na topologia da grade no sistema StorageGRID ou antes de atualizar o software. Em seguida, faça o download de uma nova cópia do Pacote de recuperação após fazer alterações na topologia da grade ou após atualizar o software.

Passos

1. Selecione **Manutenção** > **sistema** > **Pacote de recuperação**.
2. Digite a senha de provisionamento e selecione **Iniciar download**.

   O download começa imediatamente.

3. Quando o download for concluído:
   a. Abra o `.zip` ficheiro.
   b. Confirme que inclui um diretório gpt-backup e um arquivo interno `.zip`.
   c. Extraia o arquivo interno `.zip`.
   d. Confirme que você pode abrir o `Passwords.txt` arquivo.
4. Copie o arquivo do pacote de recuperação baixado (`.zip`) para dois locais seguros, seguros e separados.

> O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Procedimento de correção do StorageGRID

Talvez seja necessário aplicar um hotfix ao seu sistema StorageGRID se problemas com o software forem detetados e resolvidos entre versões de recursos.

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

hotfix contém um roll-up de todos os hotfixes anteriores dentro da versão de recurso ou patch.

- "Considerações para aplicar um hotfix"
- "Como seu sistema é afetado quando você aplica um hotfix"
- "Obter os materiais necessários para um hotfix"
- "Transferir o ficheiro de correção"
- "Verificar a condição do sistema antes de aplicar um hotfix"
- "Aplicando o hotfix"

Considerações para aplicar um hotfix

Quando você aplica um hotfix, uma série cumulativa de atualizações de software é aplicada aos nós do seu sistema StorageGRID.

Não é possível aplicar um hotfix do StorageGRID quando outro procedimento de manutenção estiver sendo executado. Por exemplo, você não pode aplicar um hotfix enquanto um procedimento de desativação, expansão ou recuperação está sendo executado.

> Se um procedimento de desativação de nó ou site estiver pausado, você pode aplicar um hotfix com segurança. Além disso, você pode ser capaz de aplicar um hotfix durante os estágios finais de um procedimento de atualização do StorageGRID. Consulte as instruções para atualizar o software StorageGRID para obter detalhes.

Depois de carregar o hotfix no Gerenciador de Grade, o hotfix é aplicado automaticamente ao nó de administrador principal. Em seguida, você pode aprovar o aplicativo do hotfix para o resto dos nós no seu sistema StorageGRID.

Se um hotfix não for aplicado a um ou mais nós, o motivo da falha será exibido na coluna Detalhes da tabela de progresso do hotfix. Você deve resolver quaisquer problemas que causaram as falhas e, em seguida, tentar novamente todo o processo. Os nós com uma aplicação anteriormente bem-sucedida do hotfix serão ignorados nos aplicativos subsequentes. Você pode tentar novamente o processo de hotfix com segurança quantas vezes for necessário até que todos os nós tenham sido atualizados. O hotfix deve ser instalado com sucesso em todos os nós de grade para que o aplicativo seja concluído.

Embora os nós de grade sejam atualizados com a nova versão de hotfix, as alterações reais em um hotfix podem afetar apenas serviços específicos em tipos específicos de nós. Por exemplo, um hotfix pode afetar apenas o serviço LDR em nós de armazenamento.

Como os hotfixes são aplicados para recuperação e expansão

Depois que um hotfix foi aplicado à sua grade, o nó de administrador principal instala automaticamente a mesma versão de hotfix para todos os nós restaurados por operações de recuperação ou adicionados em uma expansão.

No entanto, se você precisar recuperar o nó de administração principal, você deve instalar manualmente a versão correta do StorageGRID e, em seguida, aplicar o hotfix. A versão final do StorageGRID do nó de administração principal deve corresponder à versão dos outros nós na grade.

O exemplo a seguir ilustra como aplicar um hotfix ao recuperar o nó de administrador principal:

1. Suponha que a grade esteja executando uma versão do StorageGRID 11.*A.B* com o hotfix mais recente. A "versão em grade" é 11.*A.B.y*.

2. O nó de administração principal falha.
3. Reimplante o nó de administração principal usando o StorageGRID 11.*A.B* e execute o procedimento de recuperação.

> Conforme necessário para corresponder à versão da grade, você pode usar uma versão menor ao implantar o nó; você não precisa implantar a versão principal primeiro.

4. Em seguida, aplique o hotfix 11.*A.B.y* ao nó de administração principal.

Informações relacionadas

"Configurar o nó de administração principal de substituição"

Como seu sistema é afetado quando você aplica um hotfix

Você deve entender como seu sistema StorageGRID será afetado quando você aplicar um hotfix.

As aplicações do cliente podem sofrer interrupções de curto prazo

O sistema StorageGRID pode obter e recuperar dados de aplicativos clientes durante todo o processo de hotfix; no entanto, as conexões de clientes com nós de gateway individuais ou nós de armazenamento podem ser interrompidas temporariamente se o hotfix precisar reiniciar os serviços nesses nós. A 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. Para configurar grupos de alta disponibilidade, consulte as instruções para administrar o StorageGRID.

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.

Obter os materiais necessários para um 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)	Consulte "requisitos do navegador da Web".
Pacote de recuperação (`.zip`) arquivo	Antes de aplicar um hotfix, baixe o arquivo mais recente do pacote de recuperação no caso de qualquer problema ocorrer durante o hotfix.então, após a aplicação do hotfix, baixe uma nova cópia do arquivo do pacote de recuperação e salve-o em um local seguro. O arquivo atualizado do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.
Ficheiro Passwords.txt	Opcional e usado somente se você estiver aplicando um hotfix manualmente usando o cliente SSH. O `Passwords.txt` arquivo está incluído no REFERIDO pacote, que faz parte do arquivo Recovery Package `.zip`.
Frase-passe do 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.

Informações relacionadas

"Transferir o ficheiro de correção"

"Transferir o pacote de recuperação"

Transferir o ficheiro de correção

Tem de transferir o ficheiro de correção para poder aplicar a correção.

Passos

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

   "NetApp Downloads: StorageGRID"

2. Selecione a seta para baixo em **Software disponível** para ver uma lista de hotfixes disponíveis para download.

   As versões do arquivo de hotfix têm o formulário: 11,4.*x.y*.

3. Reveja as alterações incluídas na atualização.

   > Se você acabou de recuperar o nó de administrador principal e precisa aplicar um hotfix, selecione a mesma versão de hotfix que está instalada nos outros nós de grade.

   a. Selecione a versão do hotfix que deseja baixar e selecione **Go**.
   b. Inicie sessão utilizando o nome de utilizador e a palavra-passe da sua conta NetApp.
   c. Leia e aceite o Contrato de Licença de Usuário final.

      É apresentada a página de transferência da versão selecionada.

   d. Transfira o ficheiro de correção `readme.txt` para ver um resumo das alterações incluídas na correção.
4. Selecione o botão de download do hotfix e salve o arquivo.

   > Não altere o nome deste ficheiro.

   > Se você estiver usando um dispositivo macOS, o arquivo de hotfix pode ser salvo automaticamente como um `.txt` arquivo. Se estiver, você deve renomear o arquivo sem a `.txt` extensão.

5. Selecione um local para o download e selecione **Salvar**.

Informações relacionadas

"Configurar o nó de administração principal de substituição"

Verificar a condição do sistema antes de aplicar um hotfix

Você deve verificar se o sistema está pronto para acomodar o hotfix.

1. Faça login no Gerenciador de Grade usando um navegador compatível.
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.

   Para obter informações sobre alertas específicos, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

4. Certifique-se de que não existem outros procedimentos de manutenção em curso, como um procedimento de atualização, recuperação, expansão ou desativação.

   Você deve esperar que todos os procedimentos de manutenção ativos sejam concluídos antes de aplicar um hotfix.

   Não é possível aplicar um hotfix do StorageGRID quando outro procedimento de manutenção estiver sendo executado. Por exemplo, você não pode aplicar um hotfix enquanto um procedimento de desativação, expansão ou recuperação está sendo executado.

Se um procedimento de desativação de nó ou site estiver pausado, você pode aplicar um hotfix com segurança. Além disso, você pode ser capaz de aplicar um hotfix durante os estágios finais de um procedimento de atualização do StorageGRID. Consulte as instruções para atualizar o software StorageGRID para obter detalhes.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Pausar e retomar o processo de desativação dos nós de storage"

Aplicando o hotfix

A correção é aplicada automaticamente primeiro ao nó de administração principal. Em seguida, você deve aprovar o aplicativo do hotfix para outros nós de grade até que todos os nós estejam executando a mesma versão de software. Você pode personalizar a sequência de aprovação selecionando para aprovar nós de grade individuais, grupos de nós de grade ou todos os nós de grade.

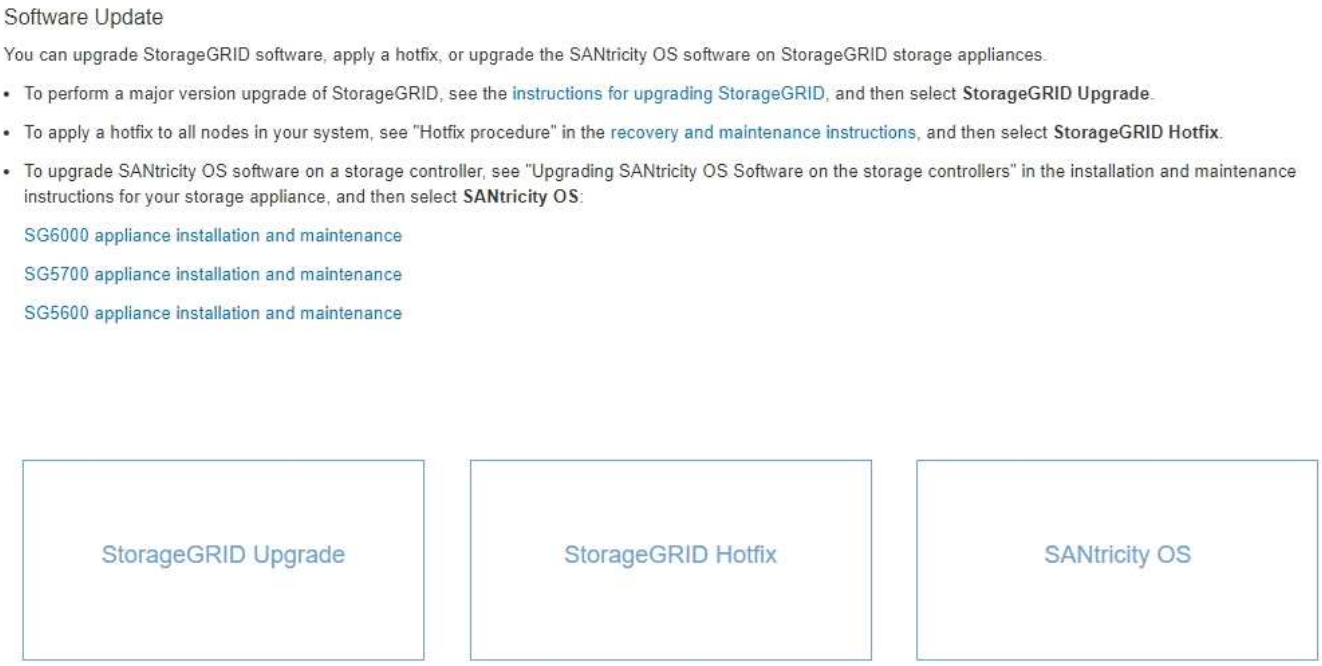
O que você vai precisar

- Você revisou todas as considerações e concluiu todas as etapas em "Planejamento e preparação de Hotfix".
- Você deve ter a senha de provisionamento.
- Você deve ter acesso root ou a permissão Manutenção.
- Pode atrasar a aplicação de uma correção a um nó, mas o processo de correção não está concluído até aplicar a correção a todos os nós.
- Não é possível executar uma atualização do software StorageGRID ou uma atualização do SANtricity os até que tenha concluído o processo de correção.

Passos

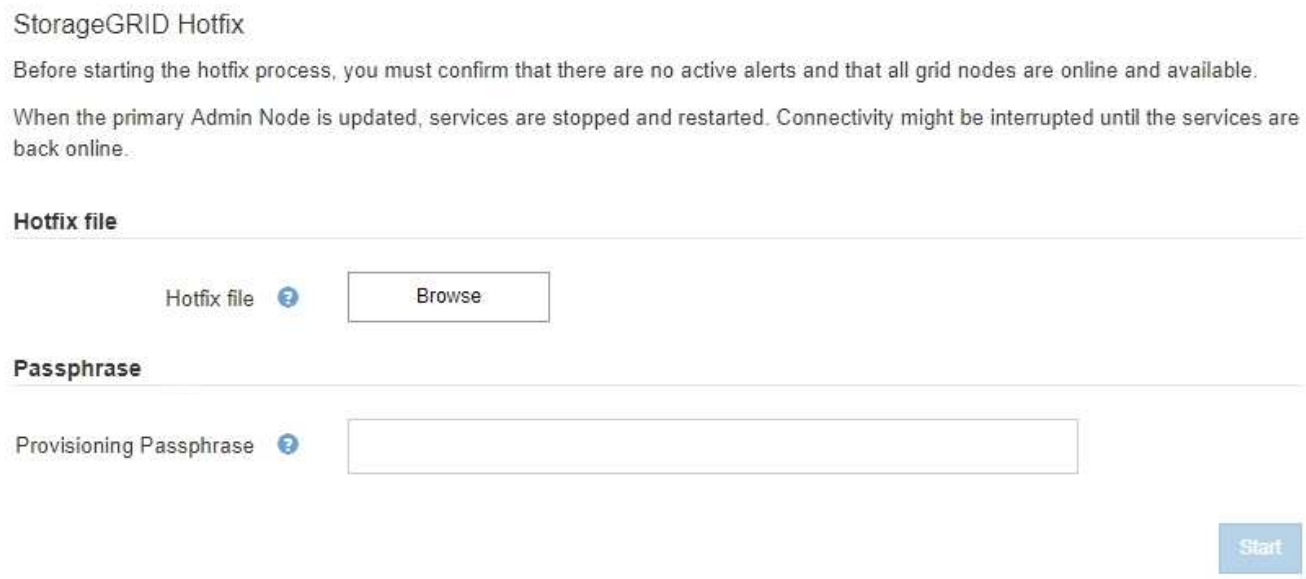
1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. Selecione **Manutenção** > **sistema** > **Atualização de Software**.

   A página Atualização de software é exibida.



3. Selecione **Hotfix StorageGRID**.

   A página de correção do StorageGRID é exibida.



4. Selecione o ficheiro de correção transferido a partir do site de suporte da NetApp.

   a. Selecione **Procurar**.

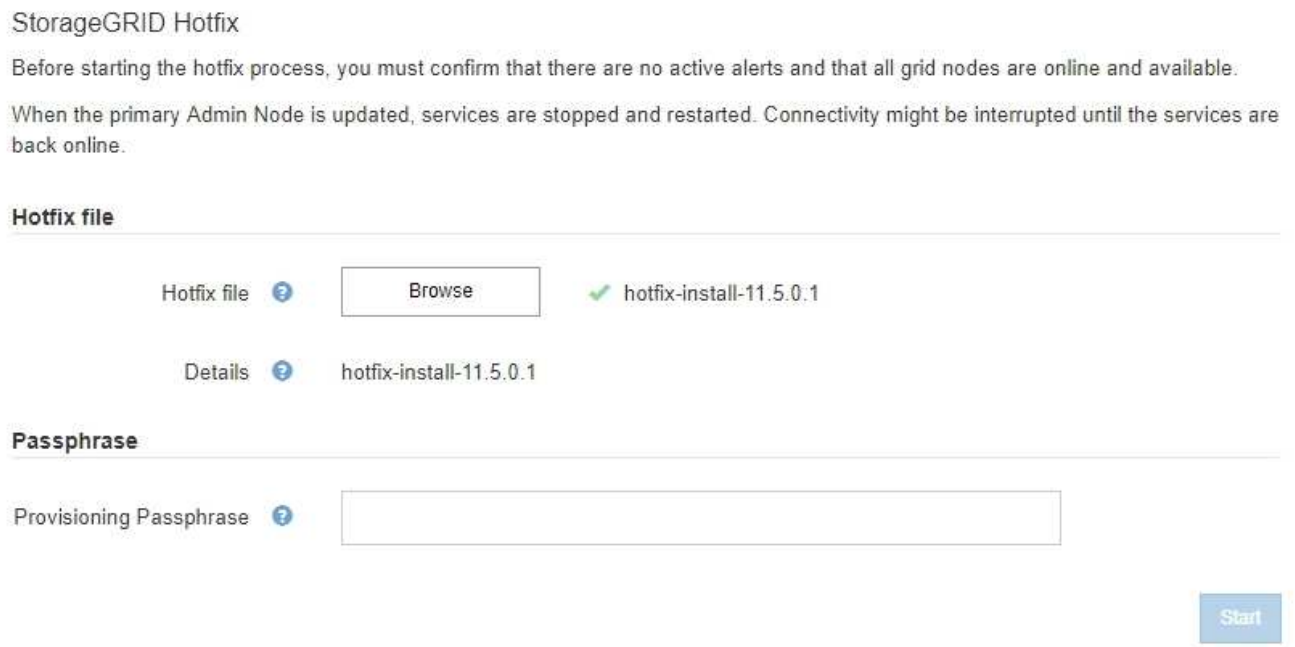
   b. Localize e selecione o ficheiro.

      `hotfix-install-version`

   c. Selecione **Open**.

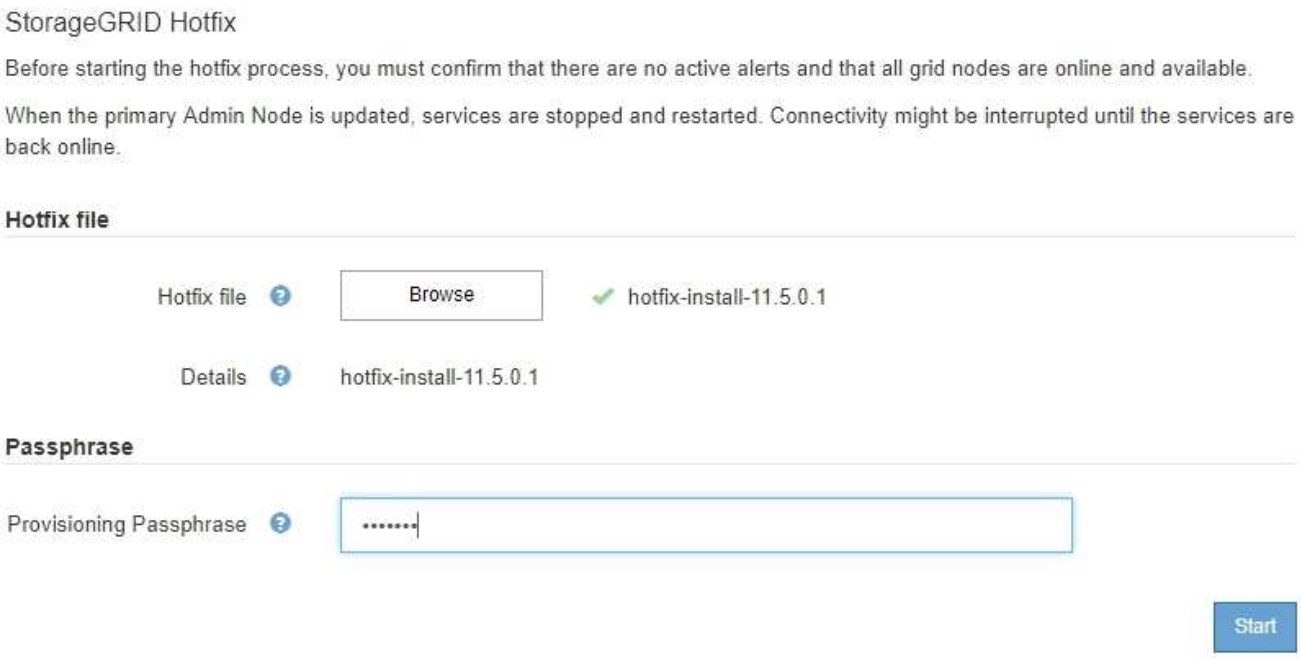
      O ficheiro é carregado. Quando o upload estiver concluído, o nome do arquivo é mostrado no campo Detalhes.

Não altere o nome do arquivo, pois ele faz parte do processo de verificação.



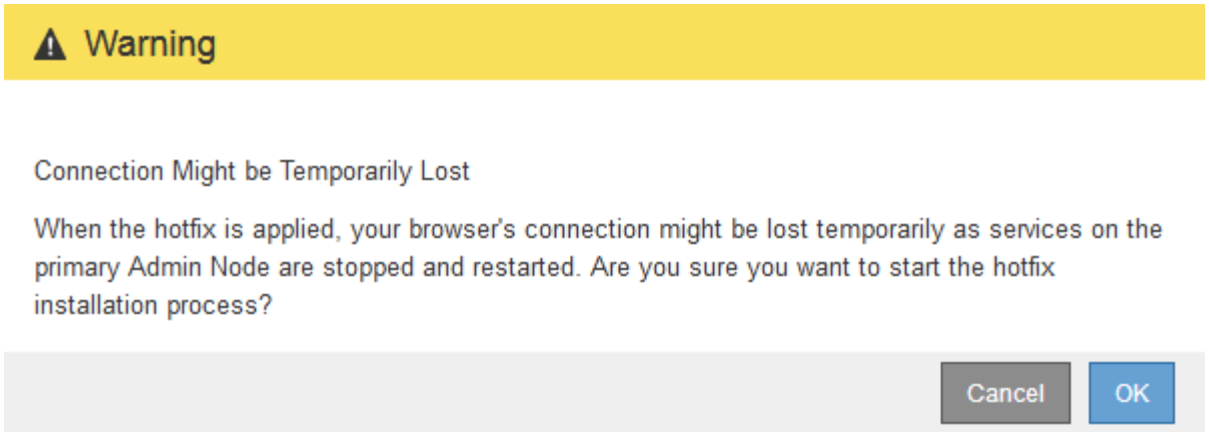
5. Insira a senha de provisionamento na caixa de texto.

   O botão **Start** (Iniciar) fica ativado.



6. Selecione **Iniciar**.

   É apresentado um aviso informando que a ligação do seu browser pode ser perdida temporariamente à medida que os serviços no nó de administração principal são reiniciados.



7. Selecione **OK** para começar a aplicar o hotfix ao nó de administração principal.

   Quando o hotfix é iniciado:

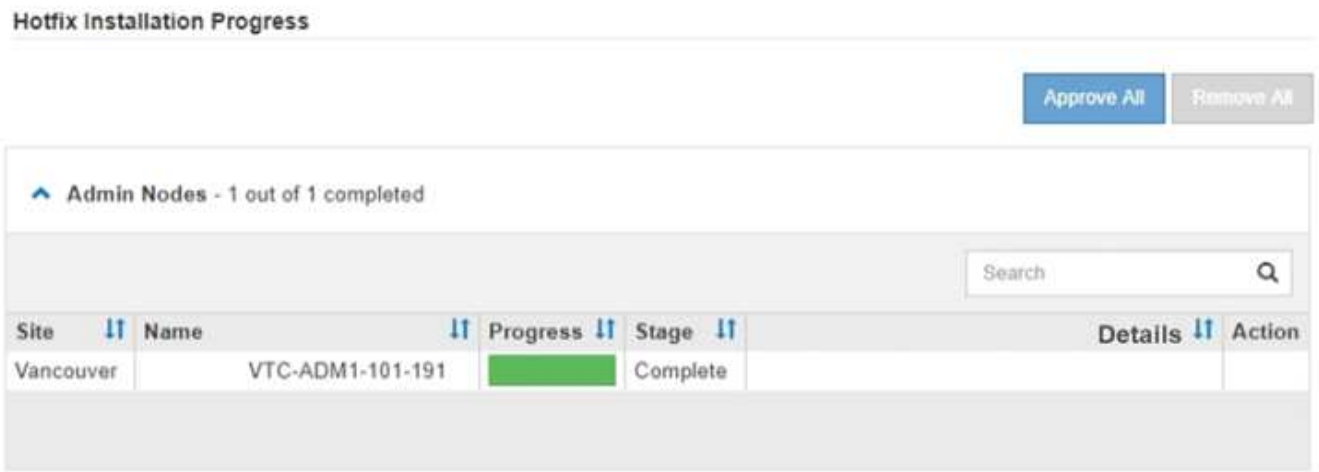
   a. As validações de hotfix são executadas.

      Se algum erro for relatado, resolva-os, faça o upload novamente do arquivo de hotfix e selecione **Iniciar** novamente.

   b. A tabela de progresso da instalação do hotfix é exibida. Esta tabela mostra todos os nós na grade e o estágio atual da instalação do hotfix para cada nó. Os nós da tabela são agrupados por tipo:

      - Nós de administração
      - Nós de gateway
      - Nós de storage
      - Nós de arquivamento

      A barra de progresso atinge a conclusão e, em seguida, o nó de administração principal é mostrado primeiro com o estágio "'concluído".



8. Opcionalmente, classifique as listas de nós em cada agrupamento em ordem crescente ou decrescente por **Site**, **Nome**, **progresso**, **Estágio** ou **Detalhes**. Ou insira um termo na caixa **pesquisar** para pesquisar nós específicos.

9. Aprove os nós de grade que estão prontos para ser atualizados. Nós aprovados do mesmo tipo são atualizados um de cada vez.

> Não aprove o hotfix para um nó, a menos que você tenha certeza de que o nó está pronto para ser atualizado.quando o hotfix for aplicado a um nó de grade, alguns serviços nesse nó podem ser reiniciados. Essas operações podem causar interrupções de serviço para clientes que estão se comunicando com o nó.

   - Selecione um ou mais botões **Approve** para adicionar um ou mais nós individuais à fila de correções.
   - Selecione o botão **Approve All** em cada agrupamento para adicionar todos os nós do mesmo tipo à fila de correções. Se você inseriu critérios de pesquisa na caixa **pesquisar**, o botão **aprovar tudo** se aplica a todos os nós selecionados pelos critérios de pesquisa.

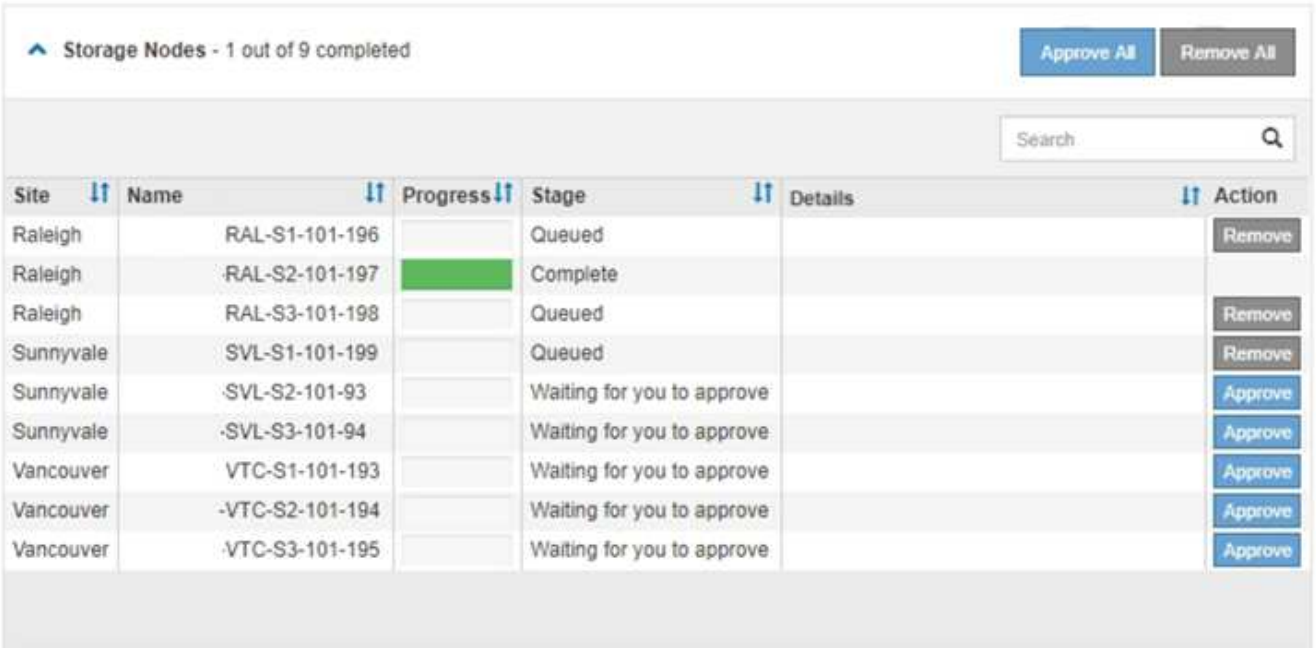
> O botão **Approve All** na parte superior da página aprova todos os nós listados na página, enquanto o botão **Approve All** na parte superior de um agrupamento de tabelas só aprova todos os nós nesse grupo. Se a ordem em que os nós são atualizados for importante, aprove nós ou grupos de nós um de cada vez e aguarde até que a atualização seja concluída em cada nó antes de aprovar o(s) próximo(s) nó(s).

   - Selecione o botão de nível superior **Approve All** na parte superior da página para adicionar todos os nós na grade à fila de hotfix.

> Tem de concluir a correção do StorageGRID antes de poder iniciar uma atualização de software diferente. Se não conseguir concluir a correção, contacte o suporte técnico.

10. Se precisar remover um nó ou todos os nós da fila de correções, selecione **Remover** ou **Remover tudo**.

    Como mostrado no exemplo, quando o estágio progride além de ""enfileirado"", o botão **Remover** fica oculto e você não pode mais remover o nó do processo de hotfix.



11. 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.

12. Se o hotfix não puder ser aplicado a nenhum nó, revise o erro de cada nó, resolva o problema e repita essas etapas.

    O procedimento não está concluído até que o hotfix seja aplicado com êxito a todos os nós. Você pode tentar novamente o processo de hotfix com segurança quantas vezes for necessário até que ele seja concluído.

Informações relacionadas

"Planejamento e preparação de hotfix"

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

Procedimentos de recuperação do nó de grade

Se um nó de grade falhar, você poderá recuperá-lo substituindo o servidor físico ou virtual com falha, reinstalando o software StorageGRID e restaurando dados recuperáveis.

Os nós de grade podem falhar se uma falha de hardware, virtualização, sistema operacional ou software tornar o nó inoperável ou não confiável. Há muitos tipos de falha que podem desencadear a necessidade de recuperar um nó de grade.

As etapas para recuperar um nó de grade variam, dependendo da plataforma onde o nó de grade está hospedado e do tipo de nó de grade. Cada tipo de nó de grade tem um procedimento de recuperação específico, que você deve seguir exatamente.

Geralmente, você tenta preservar os dados do nó de grade com falha quando possível, reparar ou substituir o nó com falha, usar o Gerenciador de Grade para configurar o nó de substituição e restaurar os dados do nó.

> Se um site StorageGRID inteiro falhar, entre em Contato com o suporte técnico. O suporte técnico trabalhará com você para desenvolver e executar um plano de recuperação de local que maximiza a quantidade de dados recuperados e atende aos seus objetivos de negócios.

Informações relacionadas

"Como a recuperação do local é realizada pelo suporte técnico"

Avisos e considerações para a recuperação do nó da grade

Se um nó de grade falhar, você deve recuperá-lo o mais rápido possível. Você deve rever todos os avisos e considerações sobre a recuperação do nó antes de começar.

> O StorageGRID é um sistema distribuído composto por vários nós que trabalham uns com os outros. Não use snapshots de disco para restaurar nós de grade. Em vez disso, consulte os procedimentos de recuperação e manutenção para cada tipo de nó.

Alguns dos motivos para recuperar um nó de grade com falha o mais rápido possível incluem o seguinte:

- Um nó de grade com falha pode reduzir a redundância de dados do sistema e do objeto, deixando você

vulnerável ao risco de perda permanente de dados se outro nó falhar.

- Um nó de grade com falha pode afetar a eficiência das operações diárias.
- Um nó de grade com falha pode reduzir sua capacidade de monitorar as operações do sistema.
- Um nó de grade com falha pode causar um erro de servidor interno do 500 se regras rígidas de ILM estiverem em vigor.
- Se um nó de grade não for recuperado prontamente, os tempos de recuperação podem aumentar. Por exemplo, podem ocorrer filas que precisam ser limpas antes da conclusão da recuperação.

Siga sempre o procedimento de recuperação para o tipo específico de nó de grade que você está recuperando. Os procedimentos de recuperação variam para nós de administração primários ou não primários, nós de gateway, nós de arquivamento, nós de dispositivo e nós de storage.

Pré-condições para a recuperação de nós de grade

Todas as condições a seguir são assumidas ao recuperar nós de grade:

- O hardware físico ou virtual com falha foi substituído e configurado.
- A versão do Instalador de dispositivos StorageGRID no dispositivo de substituição corresponde à versão de software do seu sistema StorageGRID, conforme descrito em instalação e manutenção de hardware para verificar e atualizar a versão do Instalador de dispositivos StorageGRID.
  - "Aparelhos de serviços SG100 SG1000"
  - "SG5600 dispositivos de armazenamento"
  - "SG5700 dispositivos de armazenamento"
  - "SG6000 dispositivos de armazenamento"
- Se você estiver recuperando um nó de grade diferente do nó Admin principal, há conetividade entre o nó de grade sendo recuperado e o nó Admin principal.

Ordem de recuperação de nó se um servidor que hospeda mais de um nó de grade falhar

Se um servidor que hospeda mais de um nó de grade falhar, você poderá recuperar os nós em qualquer ordem. No entanto, se o servidor com falha estiver hospedando o nó Admin principal, você deve recuperar esse nó primeiro. A recuperação do nó de administração principal primeiro impede que outras recuperações de nós parem à medida que esperam para entrar em Contato com o nó de administração principal.

Endereços IP para nós recuperados

Não tente recuperar um nó usando um endereço IP que está atualmente atribuído a qualquer outro nó. Quando você implantar o novo nó, use o endereço IP atual do nó com falha ou um endereço IP não utilizado.

Recolha de materiais necessários para a recuperação do nó da grelha

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 precisar recuperar um nó de grade, precisará do arquivo de instalação do StorageGRID para sua plataforma. **Observação:** você não precisa baixar arquivos se estiver recuperando volumes de armazenamento com falha em um nó de armazenamento.
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 **Manutenção sistema Pacote de recuperação**. 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	Para obter as versões suportadas atuais da sua plataforma, consulte a ferramenta de Matriz de interoperabilidade. "Ferramenta de Matriz de interoperabilidade do NetApp" Vá para o site do fornecedor da plataforma para obter documentação.

Informações relacionadas

"Transferir e extrair os ficheiros de instalação do StorageGRID"

"Requisitos do navegador da Web"

Transferir e extrair os ficheiros de instalação do StorageGRID

Antes de recuperar os nós de grade do StorageGRID, você deve baixar o software e

extrair os arquivos.

Você deve usar a versão do StorageGRID que está atualmente em execução na grade.

Passos

1. Determine qual versão do software está instalada atualmente. No Gerenciador de Grade, vá para **Ajuda sobre**.
2. Vá para a página de downloads do NetApp para StorageGRID.

   "NetApp Downloads: StorageGRID"

3. Selecione a versão do StorageGRID que está atualmente em execução na grade.

   As versões do software StorageGRID têm este formato: 11.x.y.

4. Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.
5. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.
6. Na coluna **Instalar StorageGRID** da página de download, selecione o `.tgz` arquivo ou `.zip` para sua plataforma.

   A versão apresentada no ficheiro de arquivo de instalação tem de corresponder à versão do software atualmente instalado.

   Use o `.zip` arquivo se estiver executando o Windows.

Plataforma	Arquivo de instalação
VMware	StorageGRID-Webscale-*version*-VMware-*uniqueID*.zip StorageGRID-Webscale-*version*-VMware-*uniqueid*.tgz
Red Hat Enterprise Linux ou CentOS	StorageGRID-Webscale-*version*-RPM-*uniqueID*.zip StorageGRID-Webscale-*version*-RPM-*uniqueid*.tgz
Ubuntu ou Debian Ou aparelhos	StorageGRID-Webscale-*version*-DEB-*uniqueID*.zip StorageGRID-Webscale-*version*-DEB-*uniqueid*.tgz
OpenStack ou outro hipervisor	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

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 você estiver recuperando um sistema VMware, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.
	Uma licença gratuita que não fornece qualquer direito de suporte para o produto.
	O arquivo de disco da máquina virtual que é usado como um modelo para criar máquinas virtuais de nó de grade.
	O arquivo de modelo Open Virtualization Format (`.ovf`) e o arquivo de manifesto (`.mf`) para implantar o nó de administração principal.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de administração não primários.
/vsphere/vsphere-archive.ovf ./vsphere/vsphere-archive.mf	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de arquivamento.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós do Gateway.
	O arquivo de (`.ovf`modelo) e o arquivo de manifesto (.mf`) para implantar nós de storage baseados em máquina virtual.
Ferramenta de script de implantação	Descrição
	Um script de shell Bash usado para automatizar a implantação de nós de grade virtual.
	Um arquivo de configuração de exemplo 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.

Caminho e nome do arquivo	Descrição
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.
	Um arquivo de configuração de exemplo para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.

10. Se você estiver recuperando um sistema Red Hat Enterprise Linux ou CentOS, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.
	Uma licença gratuita que não fornece qualquer direito de suporte para o produto.
	Pacote RPM para instalar as imagens do nó StorageGRID em seus hosts RHEL ou CentOS.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL ou CentOS.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.
	Um arquivo de configuração de exemplo 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.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.

Caminho e nome do arquivo	Descrição
	Exemplo de função do Ansible e manual de estratégia para configurar hosts RHEL ou CentOS para implantação de contêineres do StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.

11. Se você estiver recuperando 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.
	Soma de verificação MD5 para o ficheiro `/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.
	Um arquivo de configuração de exemplo para uso com o `configure-storagegrid.py` script.
	Um arquivo de configuração em branco para uso com o `configure-storagegrid.py` script.

Caminho e nome do arquivo	Descrição
	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.

12. Se estiver a recuperar um sistema baseado no StorageGRID Appliance, selecione os ficheiros apropriados.

Caminho e nome do arquivo	Descrição
	DEB pacote para instalar as imagens do nó StorageGRID em seus dispositivos.
	Soma de verificação do pacote de instalação DEB usado pelo instalador do dispositivo StorageGRID para validar se o pacote está intacto após o upload.

Nota: para a instalação do appliance, 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.

Informações relacionadas

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Selecionando um procedimento de recuperação de nó

Você deve selecionar o procedimento de recuperação correto para o tipo de nó que falhou.

Nó de grade	Procedimento de recuperação
Mais de um nó de storage	Entre em Contato com o suporte técnico. Se mais de um nó de storage falhar, o suporte técnico deve ajudar na recuperação para evitar inconsistências no banco de dados que podem levar à perda de dados. Um procedimento de recuperação de local pode ser necessário. "Como a recuperação do local é realizada pelo suporte técnico"
Um único nó de storage	O procedimento de recuperação do nó de armazenamento depende do tipo e duração da falha. "Recuperando-se de falhas no nó de storage"

Nó de grade	Procedimento de recuperação
Nó de administração	O procedimento Admin Node depende se você precisa recuperar o nó Admin primário ou um nó Admin não primário. "Recuperando-se de falhas do nó de administrador"
Nó de gateway	"Recuperando-se de falhas do Gateway Node".
Nó de arquivo	"Recuperando-se de falhas do nó de arquivamento".

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.

Recuperando-se 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.	Você deve entrar em Contato com o suporte técnico.	Se todos os nós de storage com falha estiverem no mesmo local, talvez seja necessário executar um procedimento de recuperação de local. O suporte técnico avaliará sua situação e desenvolverá um plano de recuperação. "Como a recuperação do local é realizada pelo 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.
Um nó de armazenamento está offline há mais de 15 dias.	"Recuperando um nó de storage inativo mais de 15 dias"	Este procedimento é necessário para garantir a integridade do banco de dados Cassandra.
Um nó de storage de dispositivo falhou.	"Recuperando um nó de storage de dispositivo StorageGRID"	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	"Recuperando-se de uma falha do volume de storage em que a unidade do sistema está intacta"	Este procedimento é usado para nós de storage baseados em software.
A unidade do sistema falhou.	"Recuperando-se da falha da 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 você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

Recuperando um nó de storage inativo mais de 15 dias

Se um nó de storage único estiver offline e não estiver conetado a outros nós de storage por mais de 15 dias, você deverá reconstruir o Cassandra no nó.

O que você vai precisar

- Você verificou que a desativação de um nó de storage não está em andamento ou interrompeu o procedimento de desativação do nó. (No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção Decommission**.)
- Você verificou que uma expansão não está em andamento. (No Gerenciador de Grade, selecione **Manutenção tarefas de manutenção expansão**.)

Sobre esta tarefa

Os nós de storage têm um banco de dados Cassandra que inclui metadados de objetos. Se um nó de storage não conseguir se comunicar com outros nós de storage por mais de 15 dias, o StorageGRID presume que o banco de dados Cassandra do nó está obsoleto. O nó de storage não pode reingressar na grade até que o Cassandra tenha sido reconstruído usando informações de outros nós de storage.

Use este procedimento para reconstruir o Cassandra somente se um nó de armazenamento único estiver inativo. Entre em Contato com o suporte técnico se nós de armazenamento adicionais estiverem offline ou se o Cassandra tiver sido reconstruído em outro nó de armazenamento nos últimos 15 dias; por exemplo, o Cassandra pode ter sido reconstruído como parte dos procedimentos para recuperar volumes de armazenamento com falha ou para recuperar um nó de armazenamento com falha.

Se mais de um nó de armazenamento tiver falhado (ou estiver offline), contacte o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.

Se esta for a segunda falha do nó de storage em menos de 15 dias após uma falha ou recuperação do nó de storage, entre em Contato com o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.

Se mais de um nó de armazenamento em um local tiver falhado, um procedimento de recuperação do local pode ser necessário. Entre em Contato com o suporte técnico.

"Como a recuperação do local é realizada pelo suporte técnico"

Passos

1. Se necessário, ligue o nó de armazenamento que precisa ser recuperado.
2. Faça login no nó da grade:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver logado como root, o prompt muda de `$` para `#`

> Se você não conseguir fazer login no nó da grade, o disco do sistema pode não estar intacto. Vá para o procedimento de recuperação da falha da unidade do sistema. "Recuperando-se da falha da unidade do sistema"

1. Execute as seguintes verificações no nó de storage:

   a. Emita este comando: `nodetool status`

      A saída deve ser de `Connection refused`

   b. No Gerenciador de Grade, selecione **suporte Ferramentas topologia de Grade**.

   c. Selecione *site* **nó de armazenamento SSM Serviços**. Verifique se o serviço Cassandra exibe `Not Running`.

   d. Selecione **nó de armazenamento SSM recursos**. Verifique se não há status de erro na seção volumes.

   e. Emita este comando: `grep -i Cassandra /var/local/log/servermanager.log`

      Você deve ver a seguinte mensagem na saída:

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

2. Emita este comando e monitore a saída do script: `check-cassandra-rebuild`

   - Se os serviços de armazenamento estiverem em execução, ser-lhe-á pedido que os pare. Digite: **Y**
   - Reveja os avisos no script. Se nenhum deles se aplicar, confirme que você deseja reconstruir o Cassandra. Digite: **Y**

> Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. As reparações ocorrem automaticamente assim que os serviços relacionados ou necessários tiverem sido iniciados. Você pode notar saída de script que menciona "reaper" ou "Cassandra repair." se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

3. Após a conclusão da reconstrução, execute as seguintes verificações:

   a. No Gerenciador de Grade, selecione **suporte Ferramentas topologia de Grade**.

   b. Selecione *site* **nó de armazenamento recuperado SSM Serviços**.

   c. Confirme se todos os serviços estão em execução.

   d. Selecione **DDS Data Store**.

   e. Confirme que o **Status do armazenamento de dados** é "'Up'" e que o **Data Store State** é "'normal.'"

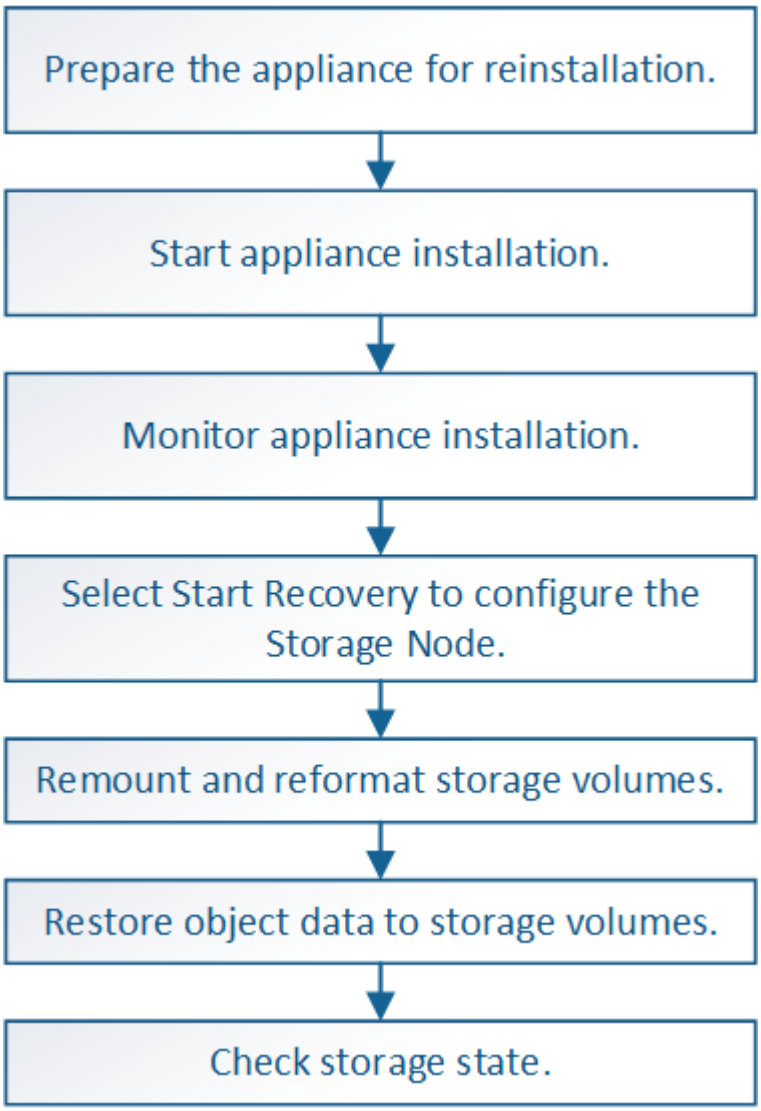
Informações relacionadas

"Recuperando-se da falha da unidade do sistema"

O procedimento para recuperar um nó de storage de dispositivo StorageGRID com falha é o mesmo se você está se recuperando da perda da unidade do sistema ou da perda de volumes de storage somente.

Sobre esta tarefa

Você deve preparar o dispositivo e reinstalar o software, configurar o nó para reingressar na grade, reformatar o armazenamento e restaurar os dados do objeto.



Se mais de um nó de armazenamento tiver falhado (ou estiver offline), contacte o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.

Se esta for a segunda falha do nó de storage em menos de 15 dias após uma falha ou recuperação do nó de storage, entre em Contato com o suporte técnico. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias pode resultar na perda de dados.

Se mais de um nó de armazenamento em um local tiver falhado, um procedimento de recuperação do local pode ser necessário. Entre em Contato com o suporte técnico.

"Como a recuperação do local é realizada pelo suporte técnico"

Se as regras ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir num volume de armazenamento que falhou, não será possível recuperar o objeto.

Se você encontrar um alarme Serviços: Status - Cassandra (SVST) durante a recuperação, consulte as instruções de monitoramento e solução de problemas para recuperar do alarme reconstruindo o Cassandra. Após a reconstrução do Cassandra, os alarmes devem ser apagados. Se os alarmes não forem apagados, contacte o suporte técnico.

Para procedimentos de manutenção de hardware, como instruções para substituir um controlador ou reinstalar o SANtricity os, consulte as instruções de instalação e manutenção do seu dispositivo de armazenamento.

Informações relacionadas

"Monitorizar Resolução de problemas"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

Passos

- "Preparando um nó de armazenamento de dispositivo para reinstalação"
- "Iniciar a instalação do dispositivo StorageGRID"
- "Monitoramento da instalação do dispositivo StorageGRID"
- "Selecione Iniciar recuperação para configurar um nó de armazenamento de dispositivo"
- "Remontar e reformatar os volumes de armazenamento do dispositivo (""passos manuais"")"
- "Restaurar dados de objetos para um volume de armazenamento de um dispositivo"
- "Verificar o estado de armazenamento após recuperar um nó de armazenamento de dispositivo"

Preparando um nó de armazenamento de dispositivo para reinstalação

Ao recuperar um nó de storage do dispositivo, primeiro você deve preparar o dispositivo para a reinstalação do software StorageGRID.

1. Faça login no nó de storage com falha:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Prepare o nó de storage do dispositivo para a instalação do software StorageGRID. `sgareinstall`

3. Quando solicitado a continuar, digite: `y`

   O aparelho reinicializa e sua sessão SSH termina. Normalmente, demora cerca de 5 minutos para que o Instalador de dispositivos StorageGRID fique disponível, embora em alguns casos você possa precisar esperar até 30 minutos.

   O nó de armazenamento do dispositivo StorageGRID é redefinido e os dados no nó de armazenamento não estão mais acessíveis. Os endereços IP configurados durante o processo de instalação original devem permanecer intactos; no entanto, é recomendável que você confirme isso quando o procedimento for concluído.

   Depois de executar o `sgareinstall` comando, todas as contas, senhas e chaves SSH provisionadas pelo StorageGRID são removidas e novas chaves de host são geradas.

Iniciar a instalação do dispositivo StorageGRID

Para instalar o StorageGRID em um nó de armazenamento de dispositivos, use o Instalador de dispositivos StorageGRID, que está incluído no dispositivo.

O que você vai precisar

- O dispositivo foi instalado em um rack, 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 e manutenção do seu dispositivo de armazenamento:
  - "SG5600 dispositivos de armazenamento"
  - "SG5700 dispositivos de armazenamento"
  - "SG6000 dispositivos de armazenamento"
- Você está usando um navegador da Web compatível.
- Você conhece um dos endereços IP atribuídos ao controlador de computação no dispositivo. Você pode usar o endereço IP da rede Admin (porta de gerenciamento 1 no controlador), da rede de Grade ou da rede do cliente.

Sobre esta tarefa

Para instalar o StorageGRID em um nó de storage do dispositivo:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do nó.
- Inicie a instalação e aguarde à medida que os volumes estão configurados e o software está instalado.
- No decorrer do processo, a instalação é interrompida. Para retomar a instalação, você deve entrar no Gerenciador de Grade e configurar o nó de armazenamento pendente como um substituto para o nó com falha.
- Depois de configurar o nó, o processo de instalação do appliance é concluído e o appliance é reinicializado.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação no dispositivo.

   `https://Controller_IP:8443`

   A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Na seção conexão nó de administrador principal, determine se você precisa especificar o endereço IP do nó de administrador principal.

   O Instalador do StorageGRID Appliance pode descobrir esse endereço IP automaticamente, assumindo que o nó de administrador principal, ou pelo menos um outro nó de grade com ADMIN_IP configurado, está presente na mesma sub-rede.

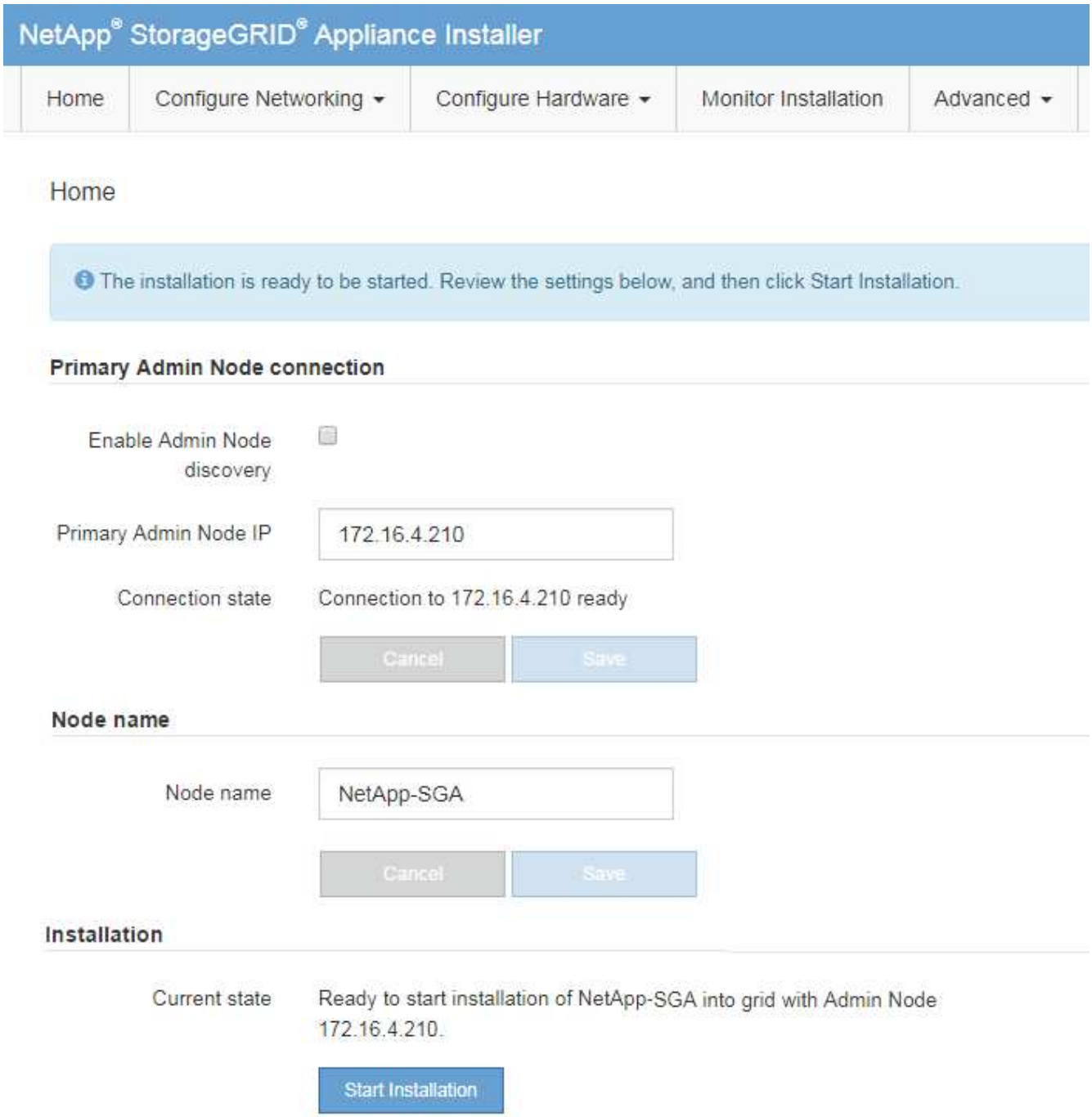
3. Se este endereço IP não for exibido ou você precisar alterá-lo, especifique o endereço:

Opção	Passos
Entrada de IP manual	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 que foi usado para o nó que você está recuperando e clique em **Salvar**.
5. Na seção Instalação, confirme se o estado atual é ""Pronto para iniciar a instalação do nome do nó na grade com Admin Node admin_ip principal"" e que o botão **Start Installation** está ativado.

   Se o botão **Start Installation** (Iniciar instalação) não estiver ativado, poderá ser necessário alterar a configuração da rede ou as definições da porta. Para obter instruções, consulte as instruções de instalação e manutenção do seu aparelho.

6. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.



O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor** na barra de menus.

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

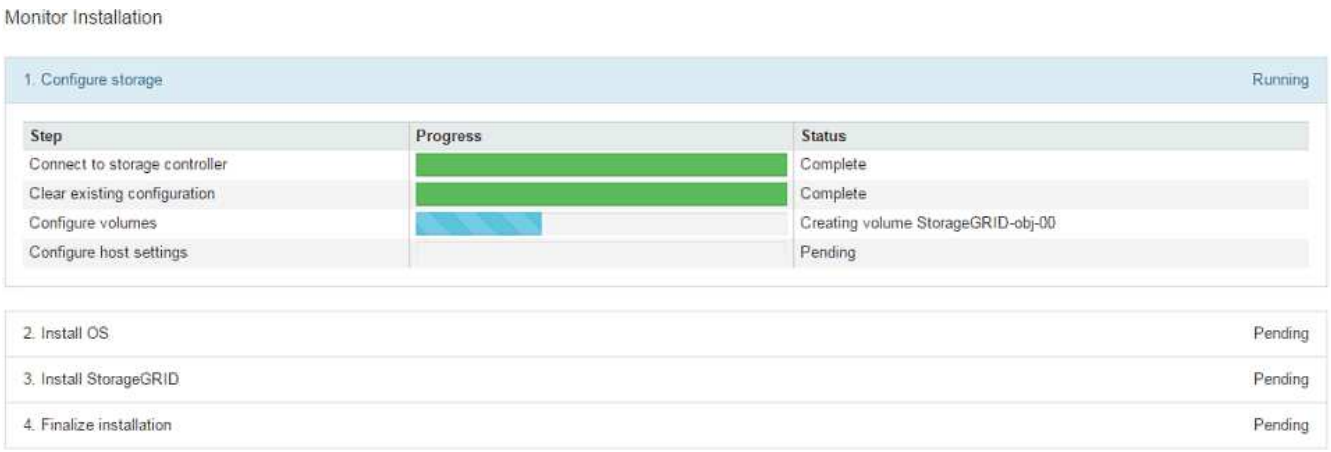
"SG5600 dispositivos de armazenamento"

Monitoramento da instalação do dispositivo StorageGRID

O Instalador de dispositivos StorageGRID fornece o status até que a instalação esteja concluída. Quando a instalação do software estiver concluída, o dispositivo é reinicializado.

1. Para monitorar o progresso da instalação, clique em **Monitor Installation** na barra de menus.

   A página Instalação do monitor mostra o progresso da instalação.



   A barra de status azul indica qual tarefa está atualmente em andamento. As barras de estado verdes indicam tarefas concluídas com êxito.

   > O instalador garante que as tarefas concluídas em uma instalação anterior não sejam executadas novamente. Se você estiver reexecutando uma instalação, todas as tarefas que não precisam ser executadas novamente serão mostradas com uma barra de status verde e um status de ""pulado"".

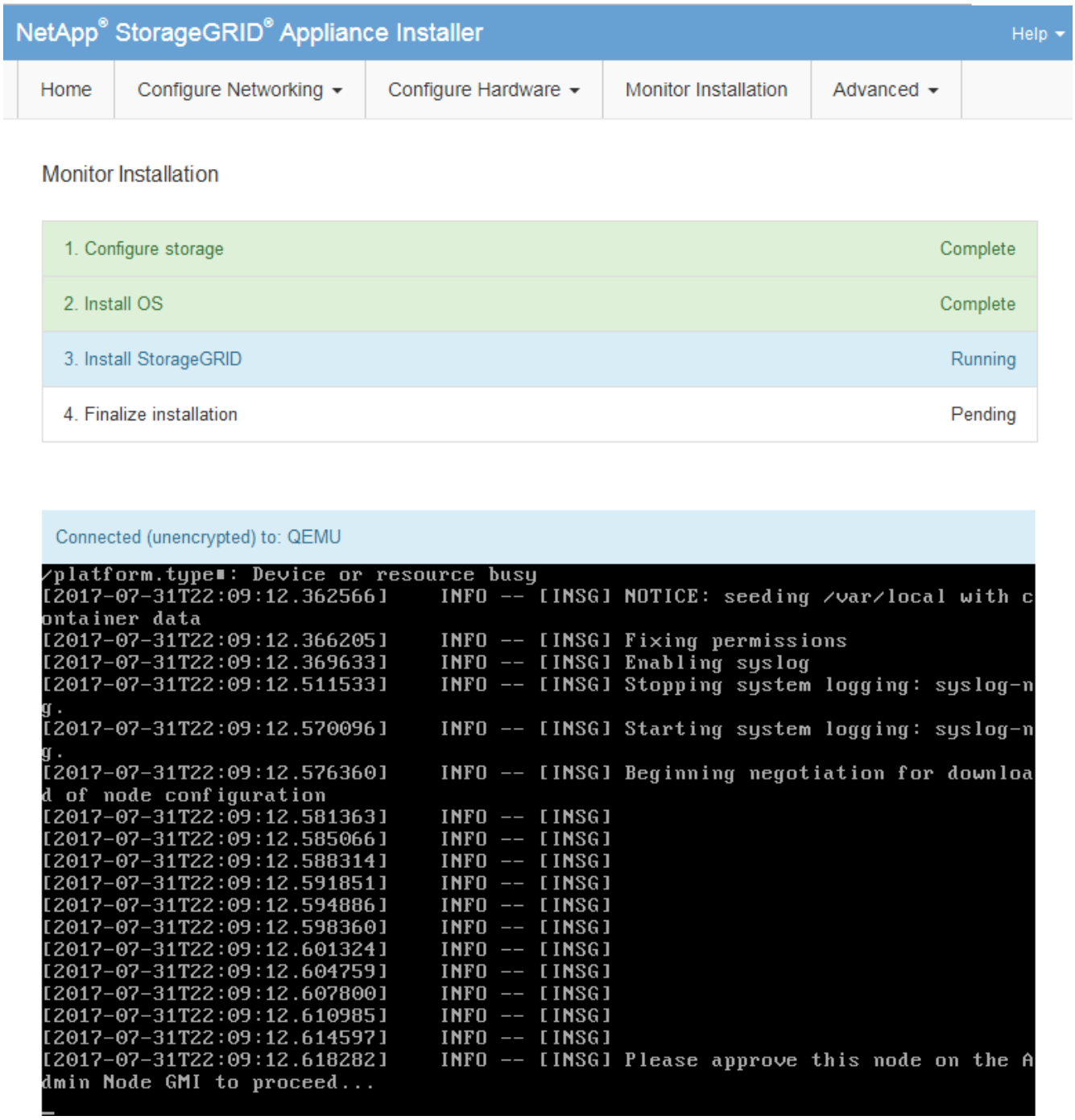
2. Reveja o progresso das duas primeiras fases de instalação.
   - **1. Configurar armazenamento**

     Durante essa etapa, o instalador se coneta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o software SANtricity para configurar volumes e configura as configurações do host.

   - **2. Instale o os**

     Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID para o dispositivo.

3. Continue monitorando o progresso da instalação até que o estágio **Install StorageGRID** pare e uma mensagem seja exibida no console incorporado solicitando que você aprove esse nó no nó Admin usando o Gerenciador de Grade.



4. Vá para o procedimento para configurar o nó de armazenamento do dispositivo.

Selecione Iniciar recuperação para configurar um nó de armazenamento de dispositivo

Você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar um nó de armazenamento de appliance como um substituto para o nó com falha.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.

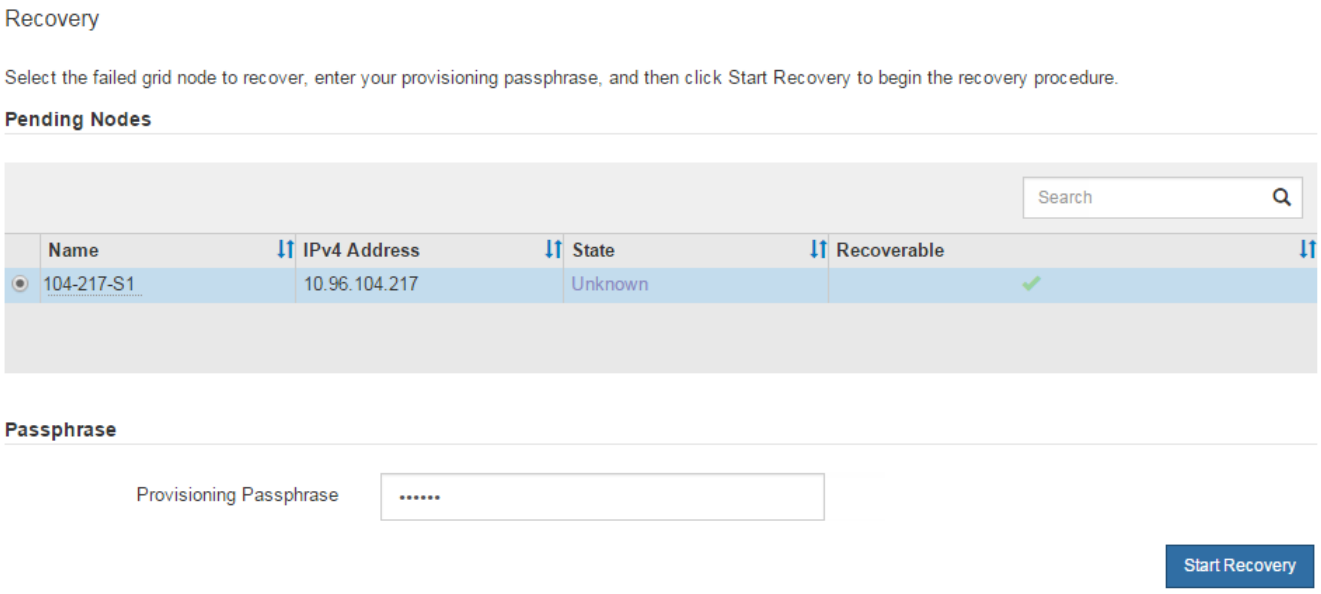
- Você precisa ter implantado um nó de storage do dispositivo de recuperação.
- Você deve saber a data de início de quaisquer trabalhos de reparo para dados codificados por apagamento.
- Você deve ter verificado se o nó de storage não foi reconstruído nos últimos 15 dias.

Passos

1. No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção recuperação**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

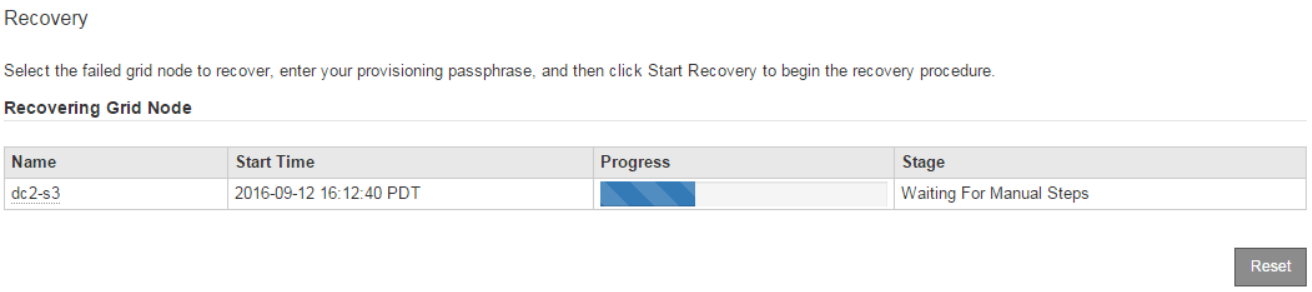
   Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de aprovisionamento**.
4. Clique em **Iniciar recuperação**.

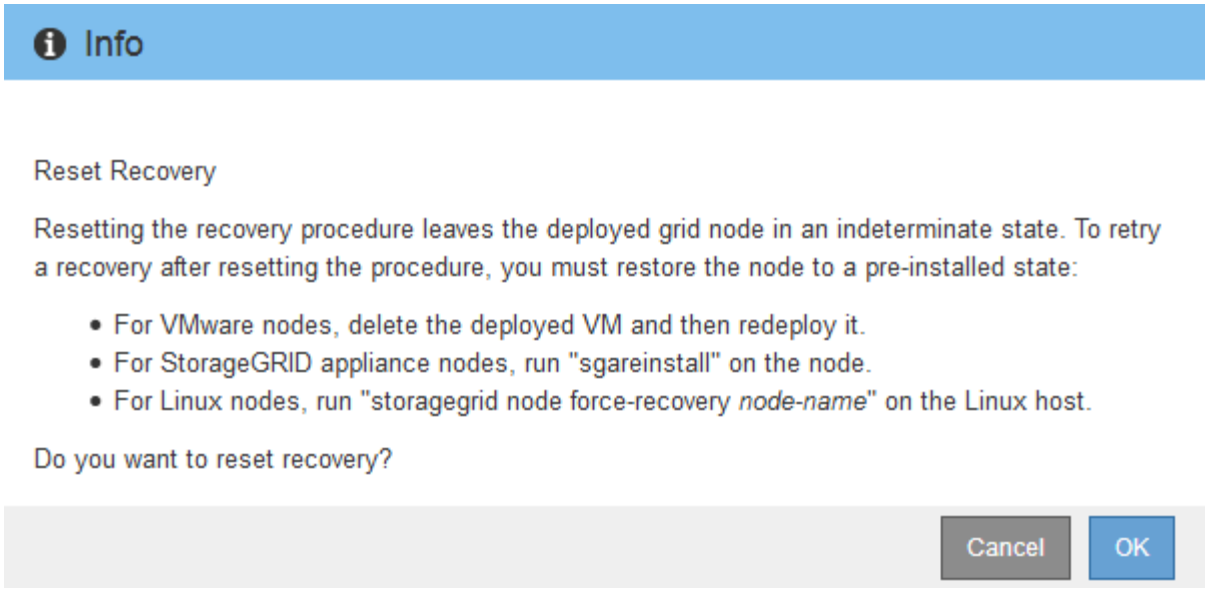


5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).

   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 armazenamento do dispositivo.



A qualquer momento durante a recuperação, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo Info (informações) é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.



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.

Remontar e reformatar os volumes de armazenamento do dispositivo ("etapas manuais")

É necessário executar manualmente dois scripts para remontar volumes de storage preservados e reformatar os volumes de storage com falha. O primeiro script remonta volumes que são formatados corretamente como volumes de armazenamento StorageGRID. O segundo script reformata quaisquer volumes não montados, reconstrói o banco de dados Cassandra, se necessário, e inicia os serviços.

O que você vai precisar

- Você já substituiu o hardware para quaisquer volumes de armazenamento com falha que você sabe que precisam ser substituídos.

  A execução `sn-remount-volumes` do script pode ajudá-lo a identificar volumes de armazenamento com falha adicionais.

- Você verificou que a desativação de um nó de storage não está em andamento ou interrompeu o procedimento de desativação do nó. (No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção Decommission**.)
- Você verificou que uma expansão não está em andamento. (No Gerenciador de Grade, selecione **Manutenção tarefas de manutenção expansão**.)

> Contacte o suporte técnico se mais de um nó de armazenamento estiver offline ou se um nó de armazenamento nesta grelha tiver sido reconstruído nos últimos 15 dias. Não execute o `sn-recovery-postinstall.sh` script. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias um do outro pode resultar na perda de dados.

Sobre esta tarefa

Para concluir este procedimento, execute estas tarefas de alto nível:

- Faça login no nó de armazenamento recuperado.

- Execute `sn-remount-volumes` o script para remontar volumes de armazenamento devidamente formatados. Quando este script é executado, ele faz o seguinte:
  - Monta e desmonta cada volume de armazenamento para reproduzir o diário XFS.
  - Executa uma verificação de consistência de arquivo XFS.
  - Se o sistema de arquivos for consistente, determina se o volume de armazenamento é um volume de armazenamento StorageGRID formatado corretamente.
  - Se o volume de armazenamento estiver formatado corretamente, remonta o volume de armazenamento. Todos os dados existentes no volume permanecem intactos.
- Revise a saída do script e resolva quaisquer problemas.
- Execute `sn-recovery-postinstall.sh` o script. Quando este script é executado, ele faz o seguinte.

> Não reinicie um nó de armazenamento durante a recuperação antes de ser executado `sn-recovery-postinstall.sh` (etapa 4) para reformatar os volumes de armazenamento com falha e restaurar os metadados de objetos. A reinicialização do nó de armazenamento antes `sn-recovery-postinstall.sh` da conclusão causa erros para serviços que tentam iniciar e faz com que os nós do dispositivo StorageGRID saiam do modo de manutenção.

  - Reformata todos os volumes de armazenamento que o `sn-remount-volumes` script não pôde montar ou que foram encontrados para serem formatados incorretamente.

> Se um volume de armazenamento for reformatado, todos os dados nesse volume serão perdidos. Você deve executar um procedimento adicional para restaurar dados de objetos de outros locais na grade, assumindo que as regras ILM foram configuradas para armazenar mais de uma cópia de objeto.

  - Reconstrói o banco de dados Cassandra no nó, se necessário.
  - Inicia os serviços no nó de storage.

Passos

1. Faça login no nó de storage recuperado:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Execute o primeiro script para remontar quaisquer volumes de armazenamento devidamente formatados.

> Se todos os volumes de armazenamento forem novos e precisarem ser formatados, ou se todos os volumes de armazenamento tiverem falhado, você poderá pular esta etapa e executar o segundo script para reformatar todos os volumes de armazenamento não montados.

   a. Execute o script: `sn-remount-volumes`

Esse script pode levar horas para ser executado em volumes de armazenamento que contêm dados.

b. À medida que o script é executado, revise a saída e responda a quaisquer prompts.

> Conforme necessário, você pode usar o `tail -f` comando para monitorar o conteúdo do arquivo de log do script (`/var/local/log/sn-remount-volumes.log`) . O arquivo de log contém informações mais detalhadas do que a saída da linha de comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
```

```
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Na saída de exemplo, um volume de armazenamento foi remontado com sucesso e três volumes de armazenamento tiveram erros.

- `/dev/sdb` Passou a verificação de consistência do sistema de arquivos XFS e teve uma estrutura de volume válida, então foi 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:

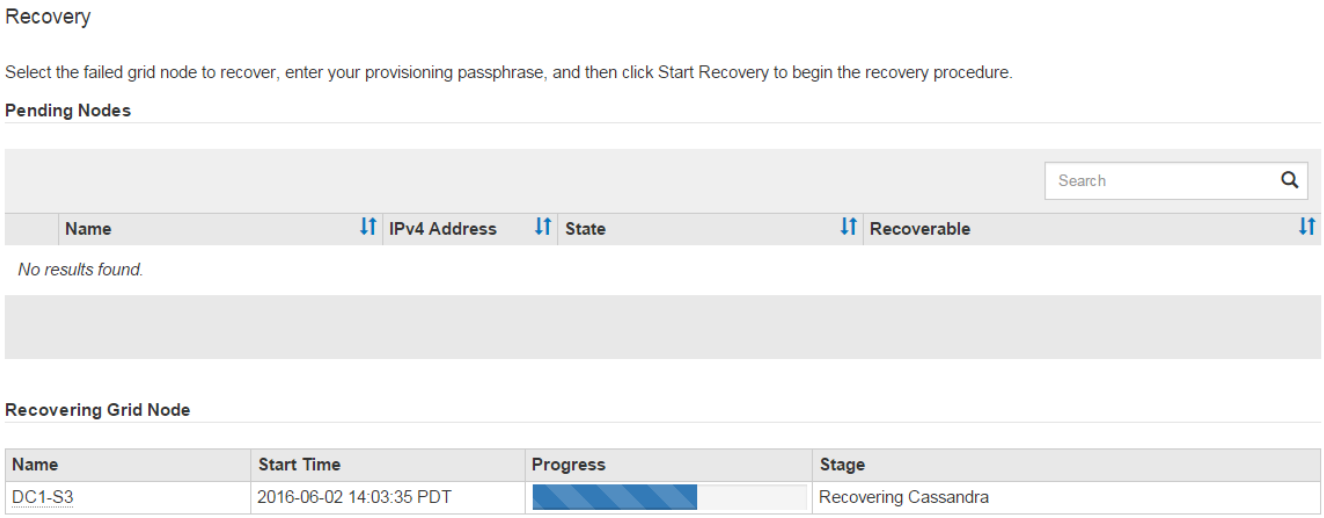
   - O script pode levar horas para ser executado.
   - Em geral, você deve deixar a sessão SSH sozinha enquanto o script estiver sendo executado.
   - Não pressione **Ctrl C** enquanto a sessão SSH estiver ativa.
   - O script será executado em segundo plano se ocorrer uma interrupção da rede e terminar 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 você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

5. À medida que o `sn-recovery-postinstall.sh` script é executado, monitore a página recuperação no Gerenciador de Grade.

   A barra de progresso e a coluna Estágio na página recuperação fornecem um status de alto nível `sn-recovery-postinstall.sh` do script.



6. Retorne à página Instalação do Monitor do Instalador do StorageGRID Appliance inserindo `http://Controller_IP:8080`, usando o endereço IP do controlador de computação.

   A página Instalação do Monitor mostra o progresso da instalação enquanto o script está em execução.

Depois que o `sn-recovery-postinstall.sh` script iniciar os serviços no nó, você pode restaurar os dados do objeto para quaisquer volumes de armazenamento que foram formatados pelo script, conforme descrito no procedimento seguinte.

Informações relacionadas

"Rever avisos para recuperação da unidade do sistema Storage Node"

"Restaurar dados de objetos para um volume de armazenamento de um dispositivo"

Restaurar dados de objetos para um volume de armazenamento de um dispositivo

Depois de recuperar volumes de armazenamento para o nó de armazenamento do dispositivo, você pode restaurar os dados do objeto que foram perdidos quando o nó de armazenamento falhou.

O que você vai precisar

- Você deve ter confirmado que o nó de armazenamento recuperado tem um estado de conexão de **Connected*** na guia *Nodes Overview** no Gerenciador de Grade.

Sobre esta tarefa

Os dados de objetos podem ser restaurados de outros nós de storage, um nó de arquivamento ou um pool de storage de nuvem, supondo que as regras de ILM da grade tenham sido configuradas de modo que as cópias de objetos estejam disponíveis.

> Se uma regra ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.

Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID deverá emitir várias solicitações ao endpoint do pool de armazenamento em nuvem para restaurar os dados do objeto. Antes de executar esse procedimento, entre em Contato com o suporte técnico para obter ajuda na estimativa do período de tempo de recuperação e dos custos associados.

Se a única cópia restante de um objeto estiver em um nó de arquivo, os dados do objeto serão recuperados do nó de arquivo. Devido à latência associada a recuperações de sistemas de storage de arquivamento externo, a restauração de dados de objetos para um nó de storage a partir de um nó de arquivamento demora mais do que a restauração de cópias de outros nós de storage.

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. Você usa opções diferentes com o `repair-data` script, com base se você está restaurando dados replicados ou apagando dados codificados, como segue:

- **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
```

- **Dados codificados de apagamento (EC)**: Dois comandos estão disponíveis para restaurar dados codificados de apagamento, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

  As reparações de dados codificados de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis. Você pode rastrear reparos de dados codificados de apagamento com este comando:

```
repair-data show-ec-repair-status
```

O trabalho de reparação EC reserva temporariamente uma grande quantidade de armazenamento. Os alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparação EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparação EC é concluído, quer o trabalho tenha falhado ou sido bem-sucedido.

Para obter mais informações sobre como usar o `repair-data` script, digite `repair-data --help` a partir da linha de comando do nó Admin 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. 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`
3. Se todos os volumes de armazenamento tiverem falhado, repare o nó inteiro. (Se apenas alguns volumes tiverem falhado, avance para o passo seguinte.)

   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.

   - Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

     Este comando repara os dados replicados em um nó de storage chamado SG-DC-SN3:

     ```
     repair-data start-replicated-node-repair --nodes SG-DC-SN3
     ```

     À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

   - Se sua grade contiver dados codificados de apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

     Este comando repara os dados codificados de 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 de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

- Se a grade tiver dados replicados e codificados para apagamento, execute os dois comandos.

4. Se apenas alguns dos volumes tiverem falhado, repare os volumes afetados.

   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.

   - Se a grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

     - Volume único*: Este comando restaura dados replicados para o volume `0002` em um nó de armazenamento chamado SG-DC-SN3:

       ```
       repair-data start-replicated-volume-repair --nodes SG-DC-SN3
       --volumes 0002
       ```

       Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo `0003` para `0009` um nó de armazenamento chamado SG-DC-SN3:

       ```
       repair-data start-replicated-volume-repair --nodes SG-DC-SN3
       --volume-range 0003-0009
       ```

       Vários volumes não em uma sequência: Este comando restaura dados replicados para volumes `0001`, `0005` e `0008` em um nó de armazenamento chamado SG-DC-SN3:

   ```
   repair-data start-replicated-volume-repair --nodes SG-DC-SN3
   --volumes 0001,0005,0008
   ```

   +

   > À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

   - Se sua grade contiver dados codificados de apagamento, use o `start-ec-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

- Volume único*: Este comando restaura os dados codificados de apagamento para o volume `0007` em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes
0007
```

Intervalo de volumes: Este comando restaura os dados codificados de 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 de 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 de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

◦ Se a grade tiver dados replicados e codificados para apagamento, execute os dois comandos.

5. Monitore o reparo de dados replicados.
   a. Selecione **nós nó de armazenamento a ser reparado ILM**.
   b. Utilize os atributos na secção avaliação para determinar se as reparações estão concluídas.

      Quando os reparos estiverem concluídos, o atributo aguardando - todos indica objetos 0D.

   c. Para monitorar o reparo com mais detalhes, selecione **suporte Ferramentas topologia de grade**.
   d. Selecione **Grid Storage Node a ser reparado LDR Data Store**.
   e. 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.

6. Monitore o reparo de dados codificados de apagamento e tente novamente quaisquer solicitações que possam ter falhado.

   a. Determinar o status dos reparos de dados codificados de apagamento:

      - 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.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time  End Time  State  Est Bytes
Affected/Repaired Retry Repair
================================================================================
================
 949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
 949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0     Yes
 949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0     Yes
 949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0     Yes
```

b. 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 `83930030303133434` :

   ```
   repair-data start-ec-node-repair --repair-id 83930030303133434
   ```

   Este comando tenta novamente uma reparação de volume com falha, utilizando a ID de reparação `83930030303133434` :

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

Informações relacionadas

"Monitorizar Resolução de problemas"

Verificar o estado de armazenamento após recuperar um nó de armazenamento de dispositivo

Depois de recuperar um nó de armazenamento de dispositivo, você deve verificar se o estado desejado do nó de armazenamento de dispositivo está definido como on-line e garantir que o estado estará on-line por padrão sempre que o servidor nó de armazenamento for reiniciado.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- 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.

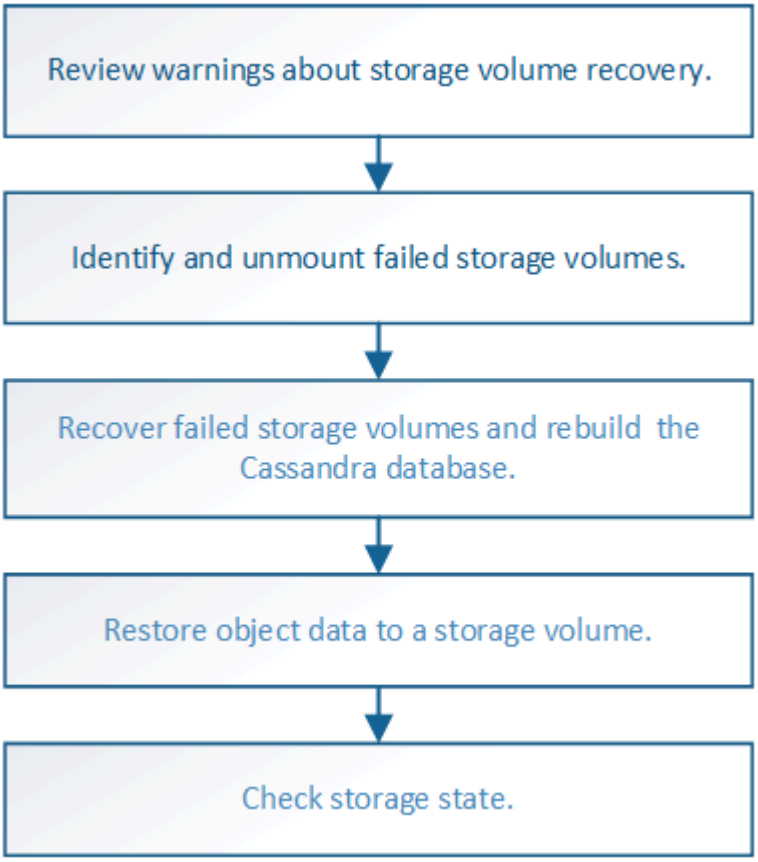
Recuperando-se de uma falha do volume de storage em que a unidade do sistema está intacta

Você deve concluir uma série de tarefas para recuperar um nó de storage baseado em software em que um ou mais volumes de armazenamento no nó de armazenamento

falharam, mas a unidade do sistema está intacta. Se apenas os volumes de armazenamento tiverem falhado, o nó de armazenamento ainda estará disponível para o sistema StorageGRID.

Sobre esta tarefa

Este procedimento de recuperação aplica-se apenas a nós de storage baseados em software. Se os volumes de storage tiverem falhado em um nó de storage de dispositivo, use o procedimento para "'recuperar um nó de storage de dispositivos StorageGRID".



Informações relacionadas

"Recuperando um nó de storage de dispositivo StorageGRID"

Passos

- "Rever avisos sobre a recuperação do volume de armazenamento"
- "Identificação e desinstalação de volumes de armazenamento com falha"
- "Recuperação de volumes de armazenamento com falha e reconstrução do banco de dados Cassandra"
- "Restaurar dados de objetos para um volume de armazenamento em que a unidade do sistema está intacta"
- "Verificando o estado de armazenamento após recuperar volumes de armazenamento"

Rever avisos sobre a recuperação do volume de armazenamento

Antes de recuperar volumes de armazenamento com falha para um nó de armazenamento, deve rever os seguintes avisos.

Os volumes de armazenamento (ou rangedbs) em um nó de armazenamento são identificados por um número hexadecimal, que é conhecido como ID de volume. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. O primeiro armazenamento de objetos (volume 0) em cada nó de armazenamento usa até 4 TB de espaço para metadados de objetos e operações de banco de dados Cassandra; qualquer espaço restante nesse volume é usado para dados de objeto. Todos os outros volumes de storage são usados exclusivamente para dados de objetos.

Se o volume 0 falhar e precisar ser recuperado, o banco de dados Cassandra pode ser reconstruído como parte do procedimento de recuperação de volume. Cassandra também pode ser reconstruída nas seguintes circunstâncias:

- Um nó de armazenamento é colocado de volta online depois de estar offline por mais de 15 dias.
- A unidade do sistema e um ou mais volumes de armazenamento falham e são recuperados.

Quando o Cassandra é reconstruído, o sistema usa informações de outros nós de storage. Se muitos nós de storage estiverem offline, alguns dados do Cassandra podem não estar disponíveis. Se o Cassandra foi reconstruído recentemente, os dados do Cassandra podem ainda não ser consistentes em toda a grade. A perda de dados pode ocorrer se o Cassandra for reconstruído quando muitos nós de storage estiverem off-line ou se dois ou mais nós de storage forem reconstruídos em até 15 dias um do outro.

Se mais de um nó de armazenamento tiver falhado (ou estiver offline), contacte o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.

Se esta for a segunda falha do nó de storage em menos de 15 dias após uma falha ou recuperação do nó de storage, entre em Contato com o suporte técnico. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias pode resultar na perda de dados.

Se mais de um nó de armazenamento em um local tiver falhado, um procedimento de recuperação do local pode ser necessário. Entre em Contato com o suporte técnico.

"Como a recuperação do local é realizada pelo suporte técnico"

Se as regras ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir num volume de armazenamento que falhou, não será possível recuperar o objeto.

Se você encontrar um alarme Serviços: Status - Cassandra (SVST) durante a recuperação, consulte as instruções de monitoramento e solução de problemas para recuperar do alarme reconstruindo o Cassandra. Após a reconstrução do Cassandra, os alarmes devem ser apagados. Se os alarmes não forem apagados, contacte o suporte técnico.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Avisos e considerações para a recuperação do nó da grade"

Identificação e desinstalação de volumes de armazenamento com falha

Ao recuperar um nó de storage com volumes de storage com falha, você deve identificar e desmontar os volumes com falha. Você deve verificar se apenas os volumes de armazenamento com falha são reformatados como parte do procedimento de recuperação.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

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. Uma vez que um volume tenha sido reformatado, os dados no volume não podem ser recuperados.

Para recuperar corretamente volumes de armazenamento com falha, você precisa saber os nomes dos dispositivos dos volumes de armazenamento com falha e suas IDs de volume.

Na instalação, cada dispositivo de armazenamento recebe um identificador exclusivo universal (UUID) do sistema de arquivos e é montado em um diretório rangedb no nó de armazenamento usando esse UUID do sistema de arquivos atribuído. O sistema de arquivos 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 `#`.

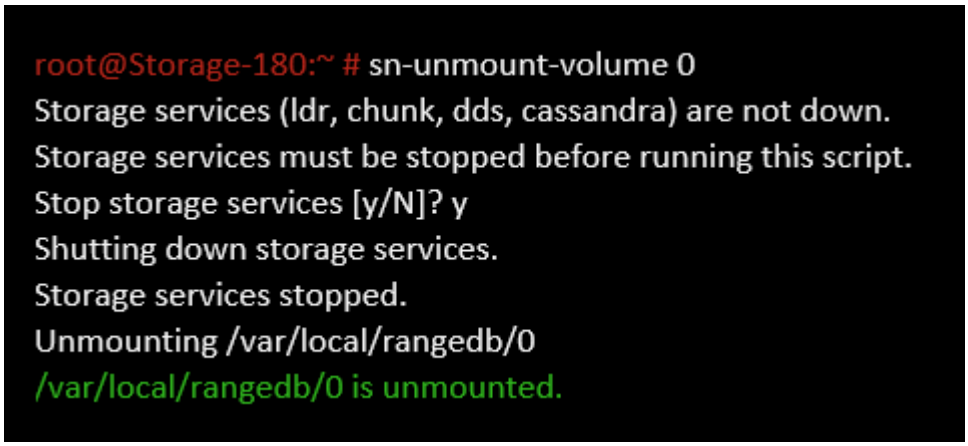
3. Execute o script a seguir para interromper os serviços de storage e desmontar um volume de storage com falha:

   ```
   sn-unmount-volume object_store_ID
   ```

   O `object_store_ID` é a ID do volume de armazenamento com falha. Por exemplo, especifique `0` no comando para um armazenamento de objetos com ID 0000.

4. Se solicitado, pressione **y** para interromper os serviços de armazenamento no nó de armazenamento.

Se os serviços de armazenamento já estiverem parados, você não será solicitado. O serviço Cassandra é interrompido apenas para o volume 0.



Em alguns segundos, os serviços de armazenamento são interrompidos e o volume é desmontado. As mensagens são exibidas indicando cada etapa do processo. A mensagem final indica que o volume está desmontado.

Recuperação de volumes de armazenamento com falha e reconstrução do banco de dados Cassandra

Você deve executar um script que reformata e remonta o armazenamento em volumes de armazenamento com falha e reconstrói o banco de dados Cassandra no nó de armazenamento se o sistema determinar que é necessário.

- Tem de ter o `Passwords.txt` ficheiro.
- As unidades de sistema no servidor devem estar intactas.
- A causa da falha deve ter sido identificada e, se necessário, o hardware de armazenamento de substituição já deve ter sido adquirido.
- O tamanho total do armazenamento de substituição deve ser o mesmo que o original.
- Você verificou que a desativação de um nó de storage não está em andamento ou interrompeu o procedimento de desativação do nó. (No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção Decommission**.)
- Você verificou que uma expansão não está em andamento. (No Gerenciador de Grade, selecione **Manutenção tarefas de manutenção expansão**.)
- Analisou os avisos sobre a recuperação do volume de armazenamento.

  "Rever avisos sobre a recuperação do volume de armazenamento"

  a. Conforme necessário, substitua o armazenamento físico ou virtual com falha associado aos volumes de armazenamento com falha identificados e desmontados anteriormente.

     Depois de substituir o storage, verifique novamente ou reinicialize para ter certeza de que ele é reconhecido pelo sistema operacional, mas não remonte os volumes. O armazenamento é remontado e adicionado em `/etc/fstab` um passo posterior.

  b. Faça login no nó de storage com falha:

     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 `#`.

c. Use um editor de texto (vi ou vim) para excluir volumes com falha do `/etc/fstab` arquivo e, em seguida, salve o arquivo.

> Comentar um volume com falha `/etc/fstab` no arquivo é insuficiente. O volume deve ser excluído `fstab`, pois o processo de recuperação verifica se todas as linhas no `fstab` arquivo correspondem aos sistemas de arquivos montados.

d. Reformate quaisquer volumes de armazenamento com falha e reconstrua o banco de dados Cassandra, se necessário. Introduza: `reformat_storage_block_devices.rb`

- Se os serviços de armazenamento estiverem em execução, ser-lhe-á pedido que os pare. Digite: **Y**
- Você será solicitado a reconstruir o banco de dados do Cassandra, se necessário.
  - Reveja os avisos. Se nenhum deles se aplicar, reconstrua o banco de dados Cassandra. Digite: **Y**
  - Se mais de um nó de armazenamento estiver offline ou se outro nó de armazenamento tiver sido reconstruído nos últimos 15 dias. Digite: **N**

    O script sairá sem reconstruir o Cassandra. Entre em Contato com o suporte técnico.
- Para cada unidade rangedb no nó de armazenamento, quando for solicitado: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, Insira uma das seguintes respostas:
  - **y** para reformatar uma unidade com erros. Isso reformata o volume de armazenamento e adiciona o volume de armazenamento reformatado ao `/etc/fstab` arquivo.
  - **n** se a unidade não contiver erros e você não quiser reformatá-la.

> Selecionar **n** sai do script. Monte a unidade (se você acha que os dados na unidade devem ser retidos e a unidade foi desmontada por erro) ou remova a unidade. Em seguida, execute o `reformat_storage_block_devices.rb` comando novamente.

> Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. As reparações ocorrem automaticamente assim que os serviços relacionados ou necessários tiverem sido iniciados. Você pode notar saída de script que menciona "reaper" ou "Cassandra repair." se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

Na saída de exemplo a seguir, a unidade `/dev/sdf` deve ser reformatada e o Cassandra não precisa ser reconstruído:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? **y**
Successfully formatted /dev/sdf with UUID c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done.  Now do manual steps to
restore copies of data.
```

Informações relacionadas

"Rever avisos sobre a recuperação do volume de armazenamento"

Restaurar dados de objetos para um volume de armazenamento em que a unidade do sistema está intacta

Depois de recuperar um volume de armazenamento em um nó de armazenamento em que a unidade do sistema está intacta, você pode restaurar os dados do objeto que foram perdidos quando o volume de armazenamento falhou.

O que você vai precisar

- Você deve ter confirmado que o nó de armazenamento recuperado tem um estado de conexão de **Connected*** ✔ **na guia *Nodes Overview** no Gerenciador de Grade.

Sobre esta tarefa

Os dados de objetos podem ser restaurados de outros nós de storage, um nó de arquivamento ou um pool de storage de nuvem, supondo que as regras de ILM da grade tenham sido configuradas de modo que as cópias de objetos estejam disponíveis.

> ⓘ Se uma regra ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.

Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID deverá emitir várias solicitações ao endpoint do pool de armazenamento em nuvem para restaurar os dados do objeto. Antes de executar esse procedimento, entre em Contato com o suporte técnico para obter ajuda na estimativa do período de tempo de recuperação e dos custos associados.

Se a única cópia restante de um objeto estiver em um nó de arquivo, os dados do objeto serão recuperados do nó de arquivo. Devido à latência associada a recuperações de sistemas de storage de arquivamento externo, a restauração de dados de objetos para um nó de storage a partir de um nó de arquivamento demora mais do que a restauração de cópias de outros nós de storage.

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. Você usa opções diferentes com o `repair-data` script, com base se você está restaurando dados replicados ou apagando dados codificados, como segue:

- **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
```

- **Dados codificados de apagamento (EC)**: Dois comandos estão disponíveis para restaurar dados codificados de apagamento, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

As reparações de dados codificados de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis. Você pode rastrear reparos de dados codificados de apagamento com este comando:

```
repair-data show-ec-repair-status
```

O trabalho de reparação EC reserva temporariamente uma grande quantidade de armazenamento. Os alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparação EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparação EC é concluído, quer o trabalho tenha falhado ou sido bem-sucedido.

Para obter mais informações sobre como usar o `repair-data` script, digite `repair-data --help` a partir da linha de comando do nó Admin 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. 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`
3. Se todos os volumes de armazenamento tiverem falhado, repare o nó inteiro. (Se apenas alguns volumes tiverem falhado, avance para o passo seguinte.)

   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.

   - Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

     Este comando repara os dados replicados em um nó de storage chamado SG-DC-SN3:

     ```
     repair-data start-replicated-node-repair --nodes SG-DC-SN3
     ```

     À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

   - Se sua grade contiver dados codificados de apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

     Este comando repara os dados codificados de 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 de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

- Se a grade tiver dados replicados e codificados para apagamento, execute os dois comandos.

4. Se apenas alguns dos volumes tiverem falhado, repare os volumes afetados.

   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.

   - Se a grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

     - Volume único*: Este comando restaura dados replicados para o volume `0002` em um nó de armazenamento chamado SG-DC-SN3:

       ```
       repair-data start-replicated-volume-repair --nodes SG-DC-SN3
       --volumes 0002
       ```

       Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo `0003` para `0009` um nó de armazenamento chamado SG-DC-SN3:

       ```
       repair-data start-replicated-volume-repair --nodes SG-DC-SN3
       --volume-range 0003-0009
       ```

       Vários volumes não em uma sequência: Este comando restaura dados replicados para volumes `0001`, `0005` e `0008` em um nó de armazenamento chamado SG-DC-SN3:

   ```
   repair-data start-replicated-volume-repair --nodes SG-DC-SN3
   --volumes 0001,0005,0008
   ```

   +

   > À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

   - Se sua grade contiver dados codificados de apagamento, use o `start-ec-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

- Volume único*: Este comando restaura os dados codificados de apagamento para o volume `0007` em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes
0007
```

Intervalo de volumes: Este comando restaura os dados codificados de 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 de 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 de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

◦ Se a grade tiver dados replicados e codificados para apagamento, execute os dois comandos.

5. Monitore o reparo de dados replicados.
   a. Selecione **nós nó de armazenamento a ser reparado ILM**.
   b. Utilize os atributos na secção avaliação para determinar se as reparações estão concluídas.

      Quando os reparos estiverem concluídos, o atributo aguardando - todos indica objetos 0D.

   c. Para monitorar o reparo com mais detalhes, selecione **suporte Ferramentas topologia de grade**.
   d. Selecione **Grid Storage Node a ser reparado LDR Data Store**.
   e. 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.

6. Monitore o reparo de dados codificados de apagamento e tente novamente quaisquer solicitações que possam ter falhado.

   a. Determinar o status dos reparos de dados codificados de apagamento:

      - 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.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

 Repair ID Scope  Start Time  End Time  State  Est Bytes
Affected/Repaired Retry Repair
=============================================================================
====================
 949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
 949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0     Yes
 949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0     Yes
 949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0     Yes
```

b. 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 83930030303133434:

   ```
   repair-data start-ec-node-repair --repair-id 83930030303133434
   ```

   Este comando tenta novamente uma reparação de volume com falha, utilizando a ID de reparação 83930030303133434:

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

Informações relacionadas

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

Verificando o estado de armazenamento após recuperar volumes de armazenamento

Depois de recuperar volumes de armazenamento, você deve verificar se o estado desejado do nó de armazenamento está definido como on-line e garantir que o estado estará on-line por padrão sempre que o servidor nó de armazenamento for reiniciado.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- 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.

Recuperando-se da falha da unidade do sistema

Se a unidade do sistema em um nó de storage baseado em software tiver falhado, o nó

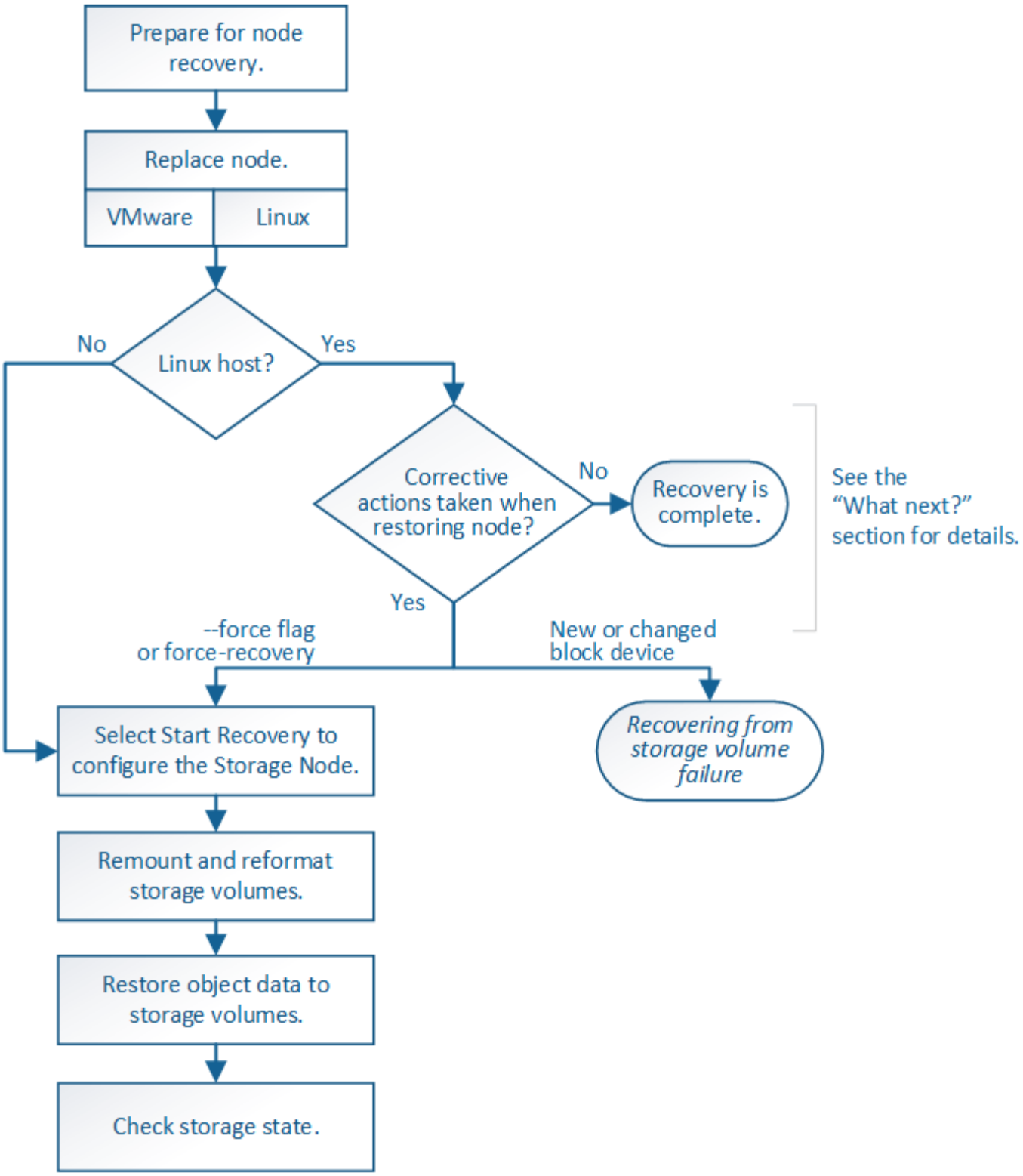
de storage não estará disponível para o sistema StorageGRID. Você deve concluir um conjunto específico de tarefas para recuperar de uma falha na unidade do sistema.

Sobre esta tarefa

Use este procedimento para recuperar de uma falha na unidade do sistema em um nó de armazenamento baseado em software. Este procedimento inclui os passos a seguir se quaisquer volumes de armazenamento também falharem ou não puderem ser remontados.

> Este procedimento aplica-se apenas a nós de storage baseados em software. Você deve seguir um procedimento diferente para recuperar um nó de storage do dispositivo.

"Recuperando um nó de storage de dispositivo StorageGRID"



Passos

- "Rever avisos para recuperação da unidade do sistema Storage Node"
- "Substituindo o nó de storage"
- "Selecionando Iniciar recuperação para configurar um nó de armazenamento"
- "Remontar e reformatar os volumes de armazenamento (""passos manuais"")"
- "Restaurar dados de objetos para um volume de armazenamento, se necessário"

- "Verificar o estado de armazenamento após recuperar uma unidade de sistema Storage Node"

Rever avisos para recuperação da unidade do sistema Storage Node

Antes de recuperar uma unidade de sistema com falha de um nó de armazenamento, deve rever os seguintes avisos.

Os nós de storage têm um banco de dados Cassandra que inclui metadados de objetos. O banco de dados Cassandra pode ser reconstruído nas seguintes circunstâncias:

- Um nó de armazenamento é colocado de volta online depois de estar offline por mais de 15 dias.
- Um volume de armazenamento falhou e foi recuperado.
- A unidade do sistema e um ou mais volumes de armazenamento falham e são recuperados.

Quando o Cassandra é reconstruído, o sistema usa informações de outros nós de storage. Se muitos nós de storage estiverem offline, alguns dados do Cassandra podem não estar disponíveis. Se o Cassandra foi reconstruído recentemente, os dados do Cassandra podem ainda não ser consistentes em toda a grade. A perda de dados pode ocorrer se o Cassandra for reconstruído quando muitos nós de storage estiverem off-line ou se dois ou mais nós de storage forem reconstruídos em até 15 dias um do outro.

Se mais de um nó de armazenamento tiver falhado (ou estiver offline), contacte o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.

Se esta for a segunda falha do nó de storage em menos de 15 dias após uma falha ou recuperação do nó de storage, entre em Contato com o suporte técnico. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias pode resultar na perda de dados.

Se mais de um nó de armazenamento em um local tiver falhado, um procedimento de recuperação do local pode ser necessário. Entre em Contato com o suporte técnico.

"Como a recuperação do local é realizada pelo suporte técnico"

Se este nó de armazenamento estiver no modo de manutenção somente leitura para permitir a recuperação de objetos por outro nó de armazenamento com volumes de armazenamento com falha, recupere volumes no nó de armazenamento com volumes de armazenamento com falha antes de recuperar este nó de armazenamento com falha. Consulte as instruções para recuperar da perda de volumes de armazenamento em que a unidade do sistema está intacta.

Se as regras ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir num volume de armazenamento que falhou, não será possível recuperar o objeto.

Se você encontrar um alarme Serviços: Status - Cassandra (SVST) durante a recuperação, consulte as instruções de monitoramento e solução de problemas para recuperar do alarme reconstruindo o Cassandra. Após a reconstrução do Cassandra, os alarmes devem ser apagados. Se os alarmes não forem apagados, contacte o suporte técnico.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Avisos e considerações para a recuperação do nó da grade"

"Recuperando-se de uma falha do volume de storage em que a unidade do sistema está intacta"

Substituindo o nó de storage

Se a unidade do sistema tiver falhado, tem de substituir primeiro o nó de armazenamento.

Você deve selecionar o procedimento de substituição do nó para sua plataforma. As etapas para substituir um nó são as mesmas para todos os tipos de nós de grade.

> Este procedimento aplica-se apenas a nós de storage baseados em software. Você deve seguir um procedimento diferente para recuperar um nó de storage do dispositivo.

"Recuperando um nó de storage de dispositivo StorageGRID"

- 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	"Substituindo um nó VMware"
Linux	"Substituindo um nó Linux"
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Selecionando Iniciar recuperação para configurar um nó de armazenamento

Depois de substituir um nó de armazenamento, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado e configurado o nó de substituição.
- Você deve saber a data de início de quaisquer trabalhos de reparo para dados codificados por apagamento.
- Você deve ter verificado se o nó de storage não foi reconstruído nos últimos 15 dias.

Sobre esta tarefa

Se o nó de armazenamento for instalado como um contentor em um host Linux, você deverá executar esta

etapa somente se um deles for verdadeiro:

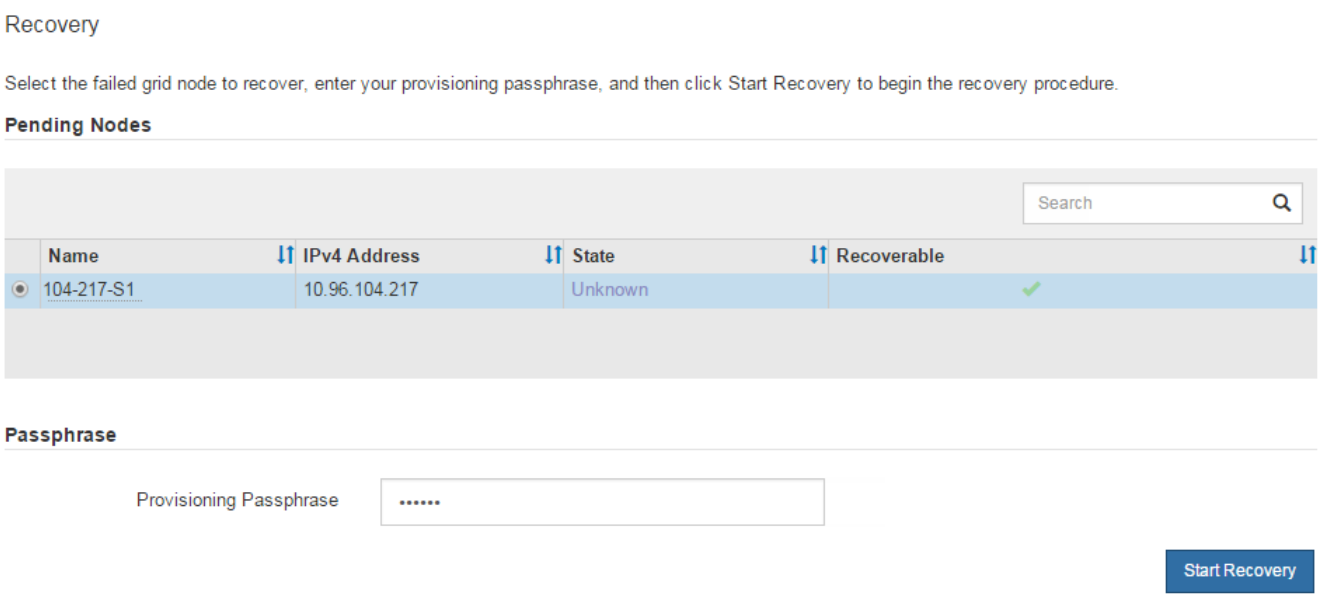
- Você teve que usar o `--force` sinalizador para importar o nó, ou você emitiu `storagegrid node force-recovery` *`node-name`*
- Você teve que fazer uma reinstalação completa do nó, ou você precisava restaurar /var/local.

Passos

1. No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção recuperação**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

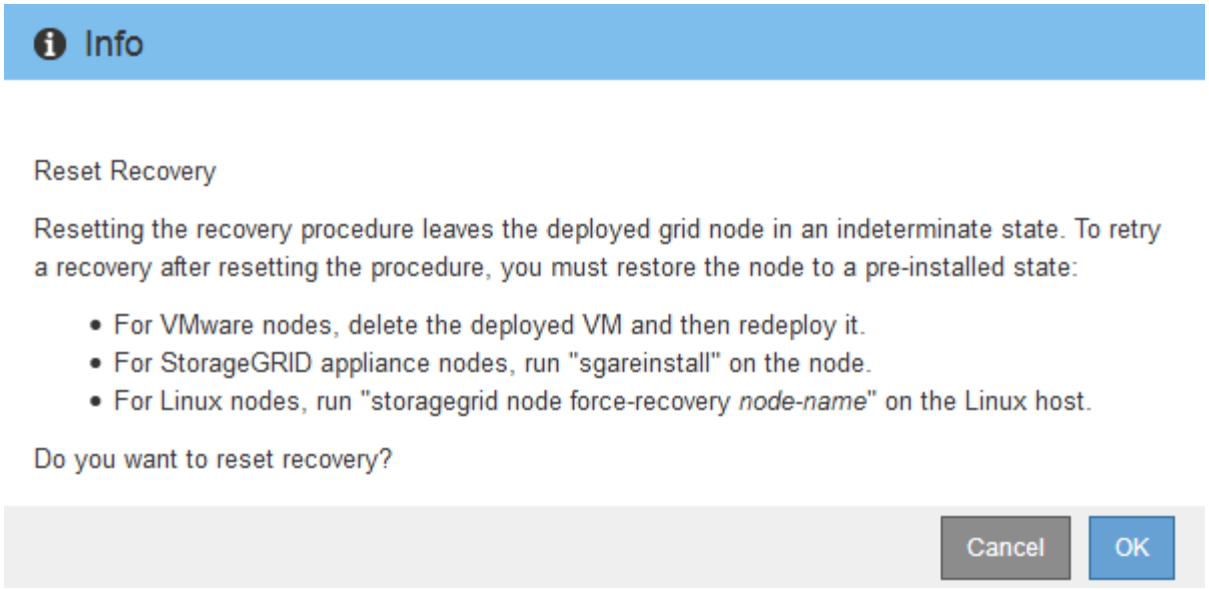
   Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de aprovisionamento**.
4. Clique em **Iniciar recuperação**.



5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).

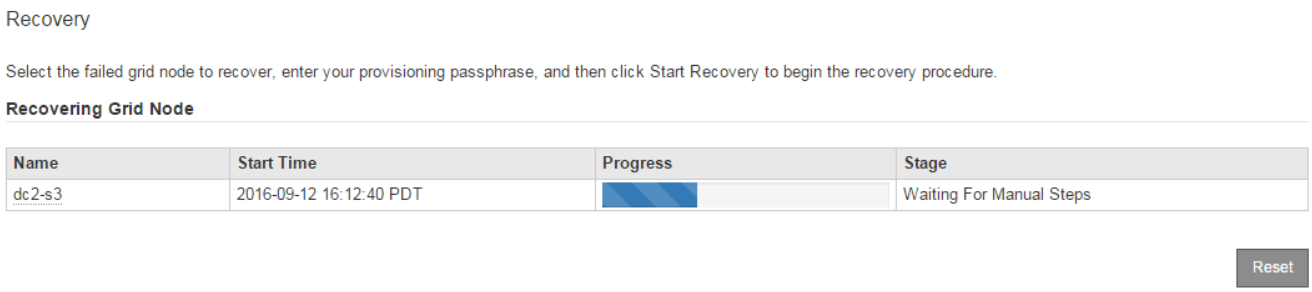
> Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo Info (informações) é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.



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 a próxima tarefa no procedimento de recuperação para remontar e reformatar os volumes de armazenamento.



Informações relacionadas

"Preparação de um aparelho para reinstalação (apenas substituição da plataforma)"

Remontar e reformatar volumes de armazenamento ("etapas manuais")

É necessário executar manualmente dois scripts para remontar volumes de storage preservados e reformatar os volumes de storage com falha. O primeiro script remonta volumes que são formatados corretamente como volumes de armazenamento StorageGRID. O segundo script reformata quaisquer volumes não montados, reconstrói Cassandra, se necessário, e inicia serviços.

O que você vai precisar

- Você já substituiu o hardware para quaisquer volumes de armazenamento com falha que você sabe que precisam ser substituídos.

A execução `sn-remount-volumes` do script pode ajudá-lo a identificar volumes de armazenamento com falha adicionais.

- Você verificou que a desativação de um nó de storage não está em andamento ou interrompeu o procedimento de desativação do nó. (No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção Decommission**.)
- Você verificou que uma expansão não está em andamento. (No Gerenciador de Grade, selecione **Manutenção tarefas de manutenção expansão**.)
- Analisou os avisos relativos à recuperação da unidade do sistema Storage Node.

  "Rever avisos para recuperação da unidade do sistema Storage Node"

> 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` (consulte a etapa para script de pós-instalação) 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 Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
```

```
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Na saída de exemplo, um volume de armazenamento foi remontado com sucesso e três volumes de armazenamento tiveram erros.

- `/dev/sdb` Passou a verificação de consistência do sistema de arquivos XFS e teve uma estrutura de volume válida, então foi remontada com sucesso. Os dados em dispositivos que são remontados pelo script são preservados.
- `/dev/sdc` Falha na verificação de consistência do sistema de arquivos XFS porque o volume de armazenamento era novo ou corrompido.
- `/dev/sdd` não foi possível montar porque o disco não foi inicializado ou o superbloco do disco estava corrompido. Quando o script não consegue montar um volume de armazenamento, ele pergunta se você deseja executar a verificação de consistência do sistema de arquivos.
  - Se o volume de armazenamento estiver 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:

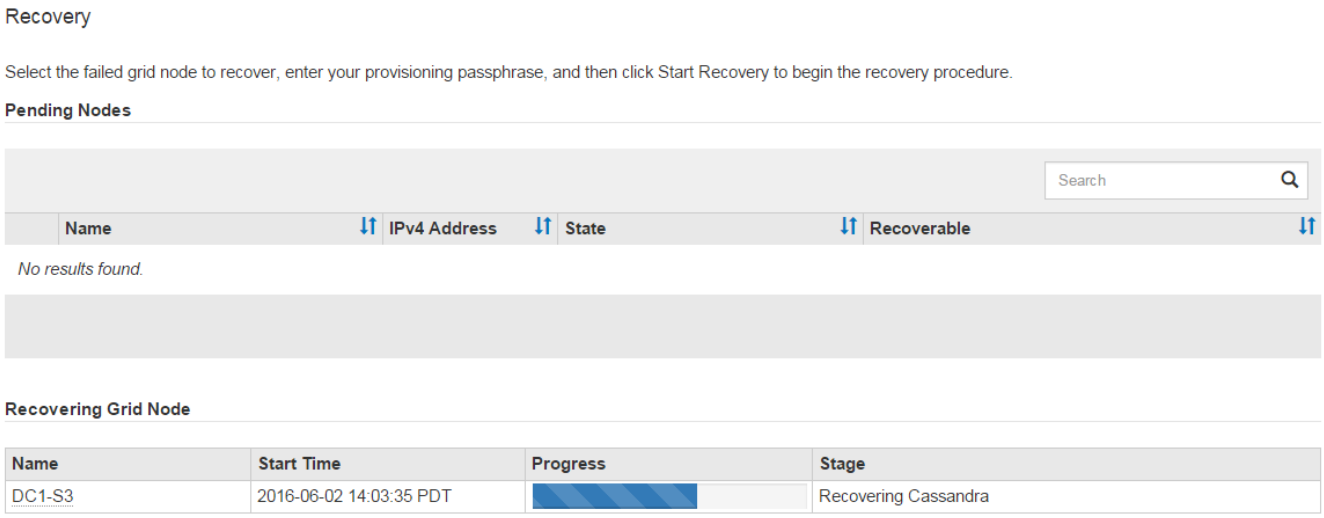
- O script pode levar horas para ser executado.
- Em geral, você deve deixar a sessão SSH sozinha enquanto o script estiver sendo executado.
- Não pressione **Ctrl C** enquanto a sessão SSH estiver ativa.
- O script será executado em segundo plano se ocorrer uma interrupção da rede e terminar a sessão 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 você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

5. à medida que o `sn-recovery-postinstall.sh` script é executado, monitore a página recuperação no Gerenciador de Grade.

A barra de progresso e a coluna Estágio na página recuperação fornecem um status de alto nível `sn-recovery-postinstall.sh` do script.



Depois que o `sn-recovery-postinstall.sh` script iniciar os serviços no nó, você pode restaurar os dados do objeto para quaisquer volumes de armazenamento que foram formatados pelo script, conforme descrito nesse procedimento.

Informações relacionadas

"Rever avisos para recuperação da unidade do sistema Storage Node"

"Restaurar dados de objetos para um volume de armazenamento, se necessário"

Restaurar dados de objetos para um volume de armazenamento, se necessário

Se o `sn-recovery-postinstall.sh` script for necessário para reformatar um ou mais volumes de storage com falha, você deverá restaurar os dados de objeto para o volume de storage reformatado de outros nós de storage e nós de arquivamento. Essas etapas não são necessárias a menos que um ou mais volumes de armazenamento tenham sido reformatados.

O que você vai precisar

- Você deve ter confirmado que o nó de armazenamento recuperado tem um estado de conexão de **Connected*** ✔ **na guia *Nodes Overview** no Gerenciador de Grade.

Sobre esta tarefa

Os dados de objetos podem ser restaurados de outros nós de storage, um nó de arquivamento ou um pool de storage de nuvem, supondo que as regras de ILM da grade tenham sido configuradas de modo que as cópias de objetos estejam disponíveis.

> ⓘ Se uma regra ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.

> ⓘ Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID deverá emitir várias solicitações ao endpoint do pool de armazenamento em nuvem para restaurar os dados do objeto. Antes de executar esse procedimento, entre em Contato com o suporte técnico para obter ajuda na estimativa do período de tempo de recuperação e dos custos associados.

> ⓘ Se a única cópia restante de um objeto estiver em um nó de arquivo, os dados do objeto serão recuperados do nó de arquivo. Devido à latência associada a recuperações de sistemas de storage de arquivamento externo, a restauração de dados de objetos para um nó de storage a partir de um nó de arquivamento demora mais do que a restauração de cópias de outros nós de storage.

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. Você usa opções diferentes com o `repair-data` script, com base se você está restaurando dados replicados ou apagando dados codificados, como segue:

- **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
```

- **Dados codificados de apagamento (EC)**: Dois comandos estão disponíveis para restaurar dados

codificados de apagamento, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

As reparações de dados codificados de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis. Você pode rastrear reparos de dados codificados de apagamento com este comando:

```
repair-data show-ec-repair-status
```

> O trabalho de reparação EC reserva temporariamente uma grande quantidade de armazenamento. Os alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparação EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparação EC é concluído, quer o trabalho tenha falhado ou sido bem-sucedido.

Para obter mais informações sobre como usar o `repair-data` script, digite `repair-data --help` a partir da linha de comando do nó Admin 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. 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`
3. Se todos os volumes de armazenamento tiverem falhado, repare o nó inteiro. (Se apenas alguns volumes tiverem falhado, avance para o passo seguinte.)

   > 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.

   - Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

     Este comando repara os dados replicados em um nó de storage chamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

- Se sua grade contiver dados codificados de apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

  Este comando repara os dados codificados de 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 de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

- Se a grade tiver dados replicados e codificados para apagamento, execute os dois comandos.

4. Se apenas alguns dos volumes tiverem falhado, repare os volumes afetados.

   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.

   - Se a grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

     - Volume único*: Este comando restaura dados replicados para o volume `0002` em um nó de armazenamento chamado SG-DC-SN3:

       ```
       repair-data start-replicated-volume-repair --nodes SG-DC-SN3
       --volumes 0002
       ```

       Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo `0003` para `0009` um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3
--volume-range 0003-0009
```

Vários volumes não em uma sequência: Este comando restaura dados replicados para volumes `0001`, `0005` e `0008` em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3
--volumes 0001,0005,0008
```

+

> À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

- Se sua grade contiver dados codificados de apagamento, use o `start-ec-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

  - Volume único*: Este comando restaura os dados codificados de apagamento para o volume `0007` em um nó de armazenamento chamado SG-DC-SN3:

    ```
    repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes
    0007
    ```

    Intervalo de volumes: Este comando restaura os dados codificados de 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 de 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 de apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

- Se a grade tiver dados replicados e codificados para apagamento, execute os dois comandos.

5. Monitore o reparo de dados replicados.
   a. Selecione **nós nó de armazenamento a ser reparado ILM**.
   b. Utilize os atributos na secção avaliação para determinar se as reparações estão concluídas.

      Quando os reparos estiverem concluídos, o atributo aguardando - todos indica objetos 0D.

   c. Para monitorar o reparo com mais detalhes, selecione **suporte Ferramentas topologia de grade**.
   d. Selecione **Grid Storage Node a ser reparado LDR Data Store**.
   e. 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.

6. Monitore o reparo de dados codificados de apagamento e tente novamente quaisquer solicitações que possam ter falhado.
   a. Determinar o status dos reparos de dados codificados de apagamento:

      - 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.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est Bytes Affected/Repaired
Retry Repair
================================================================================
=============
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0 Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0 Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0 Yes
```

b. 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 83930030303133434:

   ```
   repair-data start-ec-node-repair --repair-id 83930030303133434
   ```

   Este comando tenta novamente uma reparação de volume com falha, utilizando a ID de reparação 83930030303133434:

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

Informações relacionadas

"Administrar o StorageGRID"

"Monitorizar Resolução de problemas"

Verificar o estado de armazenamento após recuperar uma unidade de sistema Storage Node

Depois de recuperar a unidade do sistema para um nó de armazenamento, você deve verificar se o estado desejado do nó de armazenamento está definido como on-line e garantir que o estado estará on-line por padrão sempre que o servidor nó de

armazenamento for reiniciado.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- 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.

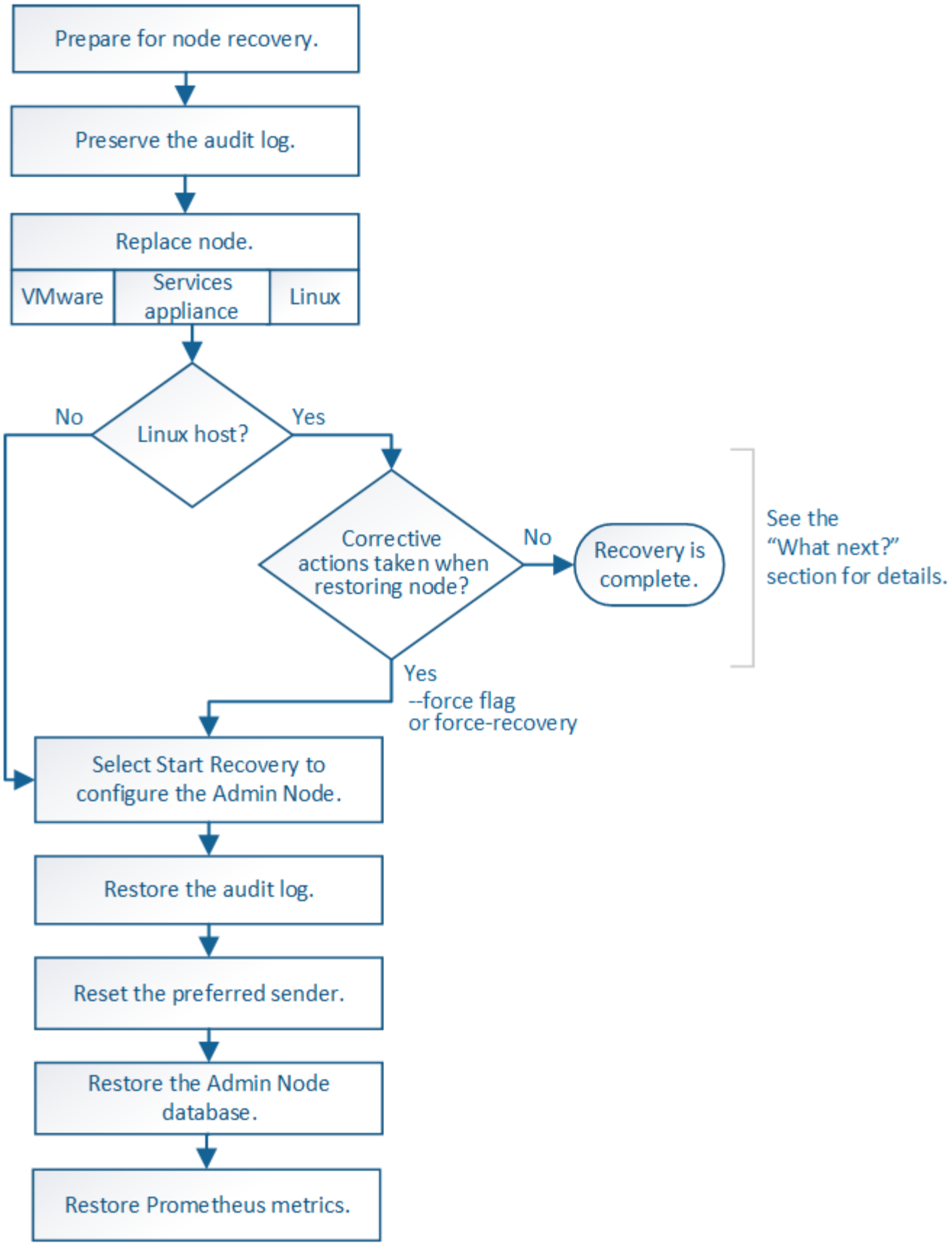
3. Se o estado de armazenamento - desejado estiver definido como somente leitura, execute as seguintes etapas:
   a. Clique na guia **Configuração**.
   b. Na lista suspensa **Estado de armazenamento - desejado**, selecione **Online**.
   c. Clique em **aplicar alterações**.
   d. Clique na guia **Visão geral** e confirme se os valores de **Estado de armazenamento — desejado** e **Estado de armazenamento — atual** são atualizados para Online.

Recuperando-se de falhas do nó de administrador

O processo de recuperação para um nó Admin depende se é o nó Admin primário ou um nó Admin não primário.

Sobre esta tarefa

As etapas de alto nível para recuperar um nó de administração primário ou não primário são as mesmas, embora os detalhes das etapas sejam diferentes.



Siga sempre o procedimento de recuperação correto para o nó Admin que está a recuperar. Os procedimentos parecem os mesmos em um nível alto, mas diferem nos detalhes.

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

Opções

- "Recuperando-se de falhas do nó de administração principal"
- "Recuperando-se de falhas no nó de administração não primário"

Recuperando-se de falhas do nó de administração principal

Você deve concluir um conjunto específico de tarefas para recuperar de uma falha de nó de administrador principal. O nó de administração principal hospeda o serviço do nó de gerenciamento de configuração (CMN) para a grade.

Sobre esta tarefa

Um nó de administração principal com falha deve ser substituído imediatamente. O serviço CMN (Configuration Management Node) no nó Admin primário é responsável pela emissão de blocos de identificadores de objetos para a grade. Esses identificadores são atribuídos a objetos à medida que são ingeridos. Novos objetos não podem ser ingeridos a menos que existam identificadores disponíveis. A ingestão de objetos pode continuar enquanto o CMN não estiver disponível porque o fornecimento de identificadores de aproximadamente um mês é armazenado em cache na grade. No entanto, depois que os identificadores armazenados em cache são esgotados, nenhum novo objeto pode ser adicionado.

> Você deve reparar ou substituir um nó de administração principal com falha em aproximadamente um mês ou a grade pode perder sua capacidade de ingerir novos objetos. O período de tempo exato depende da sua taxa de ingestão de objetos: Se você precisar de uma avaliação mais precisa do período de tempo para sua grade, entre em Contato com o suporte técnico.

Passos

- "Copiar registos de auditoria a partir do nó de administração principal avariado"
- "Substituindo o nó de administração principal"
- "Configurar o nó de administração principal de substituição"
- "Restaurando o log de auditoria no nó de administração primário recuperado"
- "Redefinindo o remetente preferido no nó de administração principal recuperado"
- "Restaurando o banco de dados Admin Node ao recuperar um Admin Node primário"
- "Restaurando métricas Prometheus ao recuperar um nó Admin primário"

Copiar registos de auditoria a partir do nó de administração principal avariado

Se você for capaz de copiar logs de auditoria do nó de administração principal com falha, você deve preservá-los para manter o Registro da grade de atividade e uso do sistema. Você pode restaurar os logs de auditoria preservados para o nó de administração principal recuperado depois que ele estiver ativo e em execução.

Este procedimento copia os arquivos de log de auditoria do nó de administração com falha para um local temporário em um nó de grade separado. Esses logs de auditoria preservados podem então ser copiados para o nó de administração de substituição. Os logs de auditoria não são copiados automaticamente para o novo nó de administração.

Dependendo do tipo de falha, talvez você não consiga copiar logs de auditoria de um nó de administrador com

falha. Se a implantação tiver apenas um Admin Node, o Admin Node recuperado inicia a gravação de eventos para o log de auditoria em um novo arquivo vazio e os dados gravados anteriormente são perdidos. Se a implantação incluir mais de um nó Admin, você poderá recuperar os logs de auditoria de outro nó Admin.

> Se os logs de auditoria não estiverem acessíveis no nó Admin com falha agora, você poderá acessá-los mais tarde, por exemplo, após a recuperação do host.

1. Inicie sessão no nó de administração com falha, se possível. Caso contrário, faça login no nó de administração principal ou em outro nó de administração, se disponível.
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Pare o serviço AMS para impedir que ele crie um novo arquivo de log:`service ams stop`
3. Renomeie o arquivo audit.log para que ele não substitua o arquivo existente quando você copiá-lo para o nó Admin recuperado.

   Renomeie audit.log para um nome de arquivo numerado exclusivo, como aaaa-mm-dd.txt.1. Por exemplo, você pode renomear o arquivo audit.log para 2015-10-25.txt,1`cd /var/local/audit/export/`

4. Reinicie o serviço AMS: `service ams start`
5. Crie o diretório para copiar todos os arquivos de log de auditoria para um local temporário em um nó de grade separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Quando solicitado, insira a senha para admin.

6. Copiar todos os ficheiros de registo de auditoria: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Quando solicitado, insira a senha para admin.

7. Faça logout como root: `exit`

Substituindo 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	"Substituindo um nó VMware"
Linux	"Substituindo um nó Linux"
Aparelhos de serviços SG100 e SG1000	"Substituir um dispositivo de serviços"
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Configurar o nó de administração principal de substituição

O nó de substituição deve ser configurado como nó de administração principal para o seu sistema StorageGRID.

O que você vai precisar

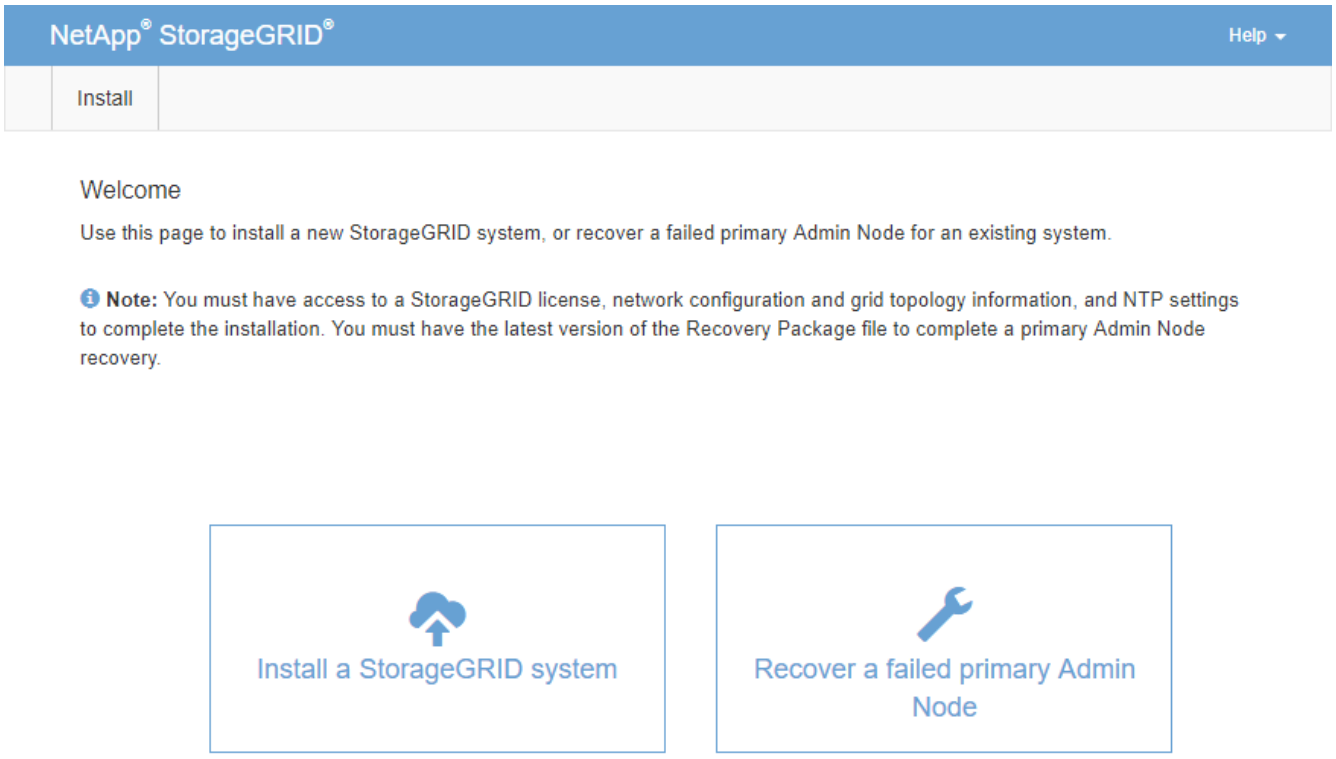
- Para nós de administração primários hospedados em máquinas virtuais, a máquina virtual deve ser implantada, ativada e inicializada.
- Para nós de administração primários hospedados em um dispositivo de serviços, você substituiu o dispositivo e instalou o software. Consulte o guia de instalação do seu aparelho.

  "Aparelhos de serviços SG100 SG1000"

- Tem de ter a cópia de segurança mais recente do ficheiro do pacote de recuperação (`sgws-recovery-package-id-revision.zip`).
- Você deve ter a senha de provisionamento.

Passos

1. Abra o navegador da Web e navegue até `https://primary_admin_node_ip`.



2. Clique em **Recover a failed Primary Admin Node** (recuperar um nó de administrador principal principal)
3. Carregue o backup mais recente do pacote de recuperação:
   a. Clique em **Procurar**.
   b. Localize o arquivo mais recente do Pacote de recuperação para o seu sistema StorageGRID e clique em **Open**.
4. Introduza a frase-passe de aprovisionamento.
5. Clique em **Iniciar recuperação**.

   O processo de recuperação começa. O Gerenciador de Grade pode ficar indisponível por alguns minutos à medida que os serviços necessários forem iniciados. Quando a recuperação estiver concluída, a página de início de sessão é apresentada.

6. Se o logon único (SSO) estiver ativado para o seu sistema StorageGRID e a confiança da parte confiável do nó que você recuperou foi configurada para usar o certificado padrão do servidor de interface de gerenciamento, atualizar (ou excluir e recriar) a confiança da parte confiável do nó nos Serviços de Federação do ative Directory (AD FS). Use o novo certificado de servidor padrão que foi gerado durante o processo de recuperação do Admin Node.

   Para configurar uma confiança de parte confiável, consulte as instruções para administrar o StorageGRID. Para acessar o certificado padrão do servidor, faça login no shell de comando do nó Admin. Vá para `/var/local/mgmt-api` o diretório e selecione o `server.crt` arquivo.

7. Determine se você precisa aplicar um hotfix.
   a. Faça login no Gerenciador de Grade usando um navegador compatível.
   b. Selecione **nós**.

c. Na lista à esquerda, selecione o nó de administração principal.

d. Na guia Visão geral, observe a versão exibida no campo **versão do software**.

e. Selecione qualquer outro nó de grade.

f. Na guia Visão geral, observe a versão exibida no campo **versão do software**.

- Se as versões exibidas nos campos **versão do software** forem as mesmas, não será necessário aplicar um hotfix.
- Se as versões exibidas nos campos **versão do software** forem diferentes, você deve aplicar um hotfix para atualizar o nó de administração primário recuperado para a mesma versão.

Informações relacionadas

"Administrar o StorageGRID"

"Procedimento de correção do StorageGRID"

Restaurando o log de auditoria no nó de administração primário recuperado

Se você conseguiu preservar o log de auditoria do nó de administração principal com falha, você pode copiá-lo para o nó de administração principal que está recuperando.

- O Admin Node recuperado deve ser instalado e em execução.
- Você deve ter copiado os logs de auditoria para outro local depois que o nó Admin original falhou.

Se um nó Admin falhar, os logs de auditoria salvos nesse nó Admin são potencialmente perdidos. Pode ser possível preservar dados de perda copiando logs de auditoria do nó de administração com falha e restaurando esses logs de auditoria para o nó de administração recuperado. Dependendo da falha, talvez não seja possível copiar logs de auditoria do nó de administração com falha. Nesse caso, se a implantação tiver mais de um nó Admin, você poderá recuperar logs de auditoria de outro nó Admin à medida que os logs de auditoria são replicados para todos os nós Admin.

Se houver apenas um nó Admin e o log de auditoria não puder ser copiado do nó com falha, o nó Admin recuperado inicia a gravação de eventos para o log de auditoria como se a instalação fosse nova.

Você deve recuperar um nó Admin o mais rápido possível para restaurar a funcionalidade de log.

1. Faça login no nó de administração recuperado:

   a. Introduza o seguinte comando: `ssh admin@recovery_Admin_Node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   Depois de iniciar sessão como root, o aviso muda de `$` para `#`.

2. Verifique quais arquivos de auditoria foram preservados: `cd /var/local/audit/export`

3. Copie os arquivos de log de auditoria preservados para o Admin Node recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Quando solicitado, insira a senha para admin.

4. Para segurança, exclua os logs de auditoria do nó de grade com falha depois de verificar se eles foram copiados com sucesso para o nó de administração recuperado.
5. Atualize as configurações de usuário e grupo dos arquivos de log de auditoria no Admin Node recuperado: `chown ams-user:bycast *`
6. Faça logout como root: `exit`

Você também deve restaurar qualquer acesso de cliente pré-existente ao compartilhamento de auditoria. Para obter mais informações, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Redefinindo o remetente preferido no nó de administração principal recuperado

Se o nó de administração principal que está a recuperar estiver atualmente definido como o remetente preferido de notificações de alerta, notificações de alarme e mensagens AutoSupport, tem de reconfigurar esta definição.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- O Admin Node recuperado deve ser instalado e em execução.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**.
2. Selecione o Admin Node recuperado na lista suspensa **Preferred Sender**.
3. Clique em **aplicar alterações**.

Informações relacionadas

"Administrar o StorageGRID"

Restaurando o banco de dados Admin Node ao recuperar um Admin Node primário

Se você quiser manter as informações históricas sobre atributos, alarmes e alertas em um nó de administrador principal que falhou, você pode restaurar o banco de dados do nó de administrador. Você só pode restaurar esse banco de dados se o sistema StorageGRID incluir outro nó de administrador.

- O Admin Node recuperado deve ser instalado e em execução.
- O sistema StorageGRID deve incluir pelo menos dois nós de administração.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter a senha de provisionamento.

Se um nó Admin falhar, as informações históricas armazenadas em seu banco de dados Admin Node serão perdidas. Esta base de dados inclui as seguintes informações:

- Histórico de alertas

- Histórico de alarmes
- Dados de atributos históricos, que são usados nos gráficos e relatórios de texto disponíveis na página **suporte Ferramentas topologia de Grade**.

Quando você recupera um Admin Node, o processo de instalação do software cria um banco de dados Admin Node vazio no nó recuperado. No entanto, o novo banco de dados inclui apenas informações para servidores e serviços que atualmente fazem parte do sistema ou adicionados posteriormente.

Se você restaurou um nó de administrador principal e seu sistema StorageGRID tiver outro nó de administrador, você poderá restaurar as informações históricas copiando o banco de dados do nó de administrador de um nó de administrador não primário (o *nó de administrador de origem*) para o nó de administrador principal recuperado. Se o sistema tiver apenas um nó de administração principal, não poderá restaurar a base de dados do nó de administração.

> Copiar o banco de dados Admin Node pode levar várias horas. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no Admin Node de origem.

1. Faça login no nó de administração de origem:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. No Admin Node de origem, pare o serviço MI: `service mi stop`
3. No Admin Node de origem, pare o serviço Management Application Program Interface (mgmt-api): `service mgmt-api stop`
4. Execute as seguintes etapas no nó de administração recuperado:
   a. Faça login no nó de administração recuperado:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   b. Parar o serviço MI: `service mi stop`
   c. Pare o serviço mgmt-api: `service mgmt-api stop`
   d. Adicione a chave privada SSH ao agente SSH. Introduza:`ssh-add`
   e. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
   f. Copie o banco de dados do Admin Node de origem para o Admin Node recuperado: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Quando solicitado, confirme se você deseja substituir o banco de dados MI no Admin Node recuperado.

      O banco de dados e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado.

h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza:`ssh-add -D`

5. Reinicie os serviços no Admin Node de origem: `service servermanager start`

Restaurando métricas Prometheus ao recuperar um nó Admin primário

Opcionalmente, você pode manter as métricas históricas mantidas pelo Prometheus em um nó de administração principal que falhou. As métricas Prometheus só podem ser restauradas se o seu sistema StorageGRID incluir outro nó Admin.

- O Admin Node recuperado deve ser instalado e em execução.
- O sistema StorageGRID deve incluir pelo menos dois nós de administração.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter a senha de provisionamento.

Se um nó Admin falhar, as métricas mantidas no banco de dados Prometheus no nó Admin serão perdidas. Quando você recupera o Admin Node, o processo de instalação do software cria um novo banco de dados Prometheus. Depois que o nó de administração recuperado é iniciado, ele Registra as métricas como se você tivesse executado uma nova instalação do sistema StorageGRID.

Se você restaurou um nó de administrador principal e seu sistema StorageGRID tiver outro nó de administrador, você poderá restaurar as métricas históricas copiando o banco de dados Prometheus de um nó de administrador não primário (o *nó de administrador de origem*) para o nó de administrador principal recuperado. Se o seu sistema tiver apenas um nó Admin principal, não poderá restaurar a base de dados Prometheus.

> Copiar o banco de dados Prometheus pode levar uma hora ou mais. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no Admin Node de origem.

1. Faça login no nó de administração de origem:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. No Admin Node de origem, pare o serviço Prometheus: `service prometheus stop`
3. Execute as seguintes etapas no nó de administração recuperado:
   a. Faça login no nó de administração recuperado:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   b. Pare o serviço Prometheus: `service prometheus stop`

c. Adicione a chave privada SSH ao agente SSH. Introduza:`ssh-add`

d. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

e. Copie o banco de dados Prometheus do nó Admin de origem para o nó Admin recuperado: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no nó Admin recuperado.

O banco de dados Prometheus original e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado. É apresentado o seguinte estado:

Banco de dados clonado, iniciando serviços

a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza:`ssh-add -D`

4. Reinicie o serviço Prometheus no Admin Node de origem.`service prometheus start`

Recuperando-se de falhas no nó de administração não primário

Você deve concluir as tarefas a seguir para se recuperar de uma falha não primária do Admin Node. Um nó de administração hospeda o serviço CMN (Configuration Management Node) e é conhecido como nó de administração principal. Embora você possa ter vários nós de administração, cada sistema StorageGRID inclui apenas um nó de administração principal. Todos os outros nós de administração são nós de administração não primários.

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

Passos

- "Copiar registos de auditoria a partir do nó de administração não primário com falha"
- "Substituindo um nó de administração não primário"
- "Selecionando Iniciar recuperação para configurar um nó de administração não primário"
- "Restaurando o log de auditoria no nó de administração não primário recuperado"
- "Redefinir o remetente preferido no nó de administração não primário recuperado"
- "Restaurando o banco de dados Admin Node ao recuperar um Admin Node não primário"
- "Restaurando métricas Prometheus ao recuperar um nó Admin não primário"

Copiar registos de auditoria a partir do nó de administração não primário com falha

Se você conseguir copiar logs de auditoria do nó de administração com falha, você deve preservá-los para manter o Registro da grade de atividade e uso do sistema. Você pode restaurar os logs de auditoria preservados para o nó de administração não primário recuperado depois que ele estiver ativo e em execução.

Este procedimento copia os arquivos de log de auditoria do nó de administração com falha para um local temporário em um nó de grade separado. Esses logs de auditoria preservados podem então ser copiados

para o nó de administração de substituição. Os logs de auditoria não são copiados automaticamente para o novo nó de administração.

Dependendo do tipo de falha, talvez você não consiga copiar logs de auditoria de um nó de administrador com falha. Se a implantação tiver apenas um Admin Node, o Admin Node recuperado inicia a gravação de eventos para o log de auditoria em um novo arquivo vazio e os dados gravados anteriormente são perdidos. Se a implantação incluir mais de um nó Admin, você poderá recuperar os logs de auditoria de outro nó Admin.

> Se os logs de auditoria não estiverem acessíveis no nó Admin com falha agora, você poderá acessá-los mais tarde, por exemplo, após a recuperação do host.

1. Inicie sessão no nó de administração com falha, se possível. Caso contrário, faça login no nó de administração principal ou em outro nó de administração, se disponível.
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
2. Pare o serviço AMS para impedir que ele crie um novo arquivo de log:`service ams stop`
3. Renomeie o arquivo audit.log para que ele não substitua o arquivo existente quando você copiá-lo para o nó Admin recuperado.

   Renomeie audit.log para um nome de arquivo numerado exclusivo, como aaaa-mm-dd.txt.1. Por exemplo, você pode renomear o arquivo audit.log para 2015-10-25.txt,1`cd /var/local/audit/export/`
4. Reinicie o serviço AMS: `service ams start`
5. Crie o diretório para copiar todos os arquivos de log de auditoria para um local temporário em um nó de grade separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Quando solicitado, insira a senha para admin.
6. Copiar todos os ficheiros de registo de auditoria: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Quando solicitado, insira a senha para admin.
7. Faça logout como root: `exit`

Substituindo um 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	"Substituindo um nó VMware"
Linux	"Substituindo um nó Linux"
Aparelhos de serviços SG100 e SG1000	"Substituir um dispositivo de serviços"
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Selecionando Iniciar recuperação para configurar um nó de administração não primário

Depois de substituir um nó Admin não primário, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

O que você vai precisar

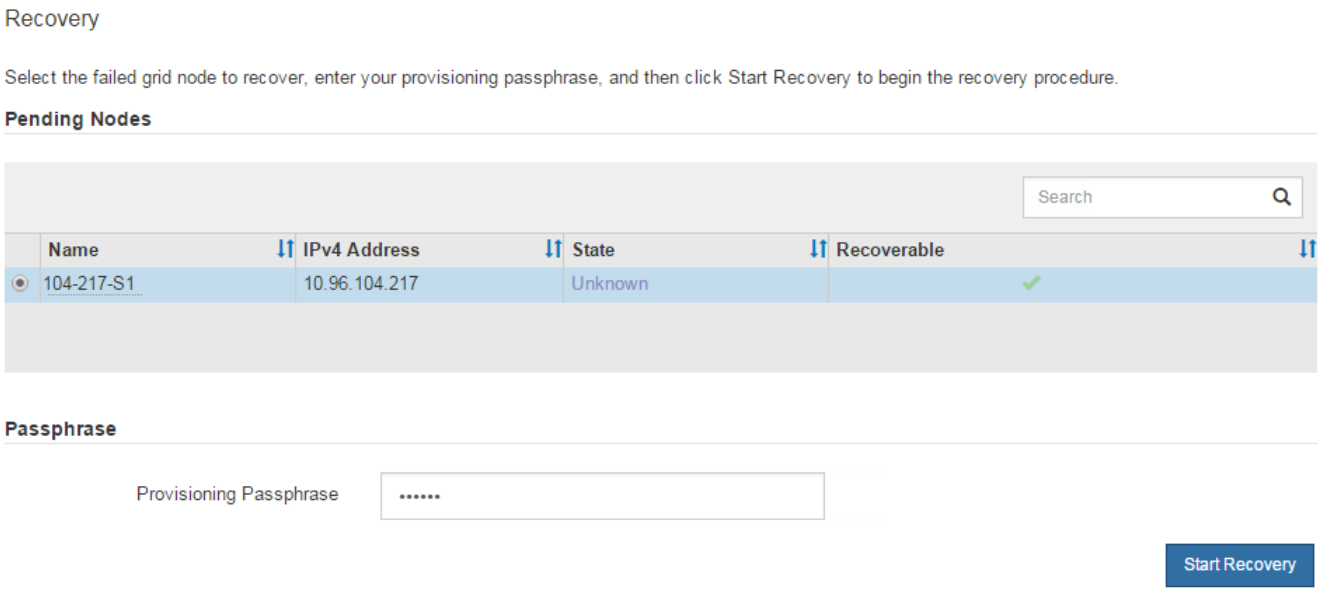
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado e configurado o nó de substituição.

Passos

1. No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção recuperação**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

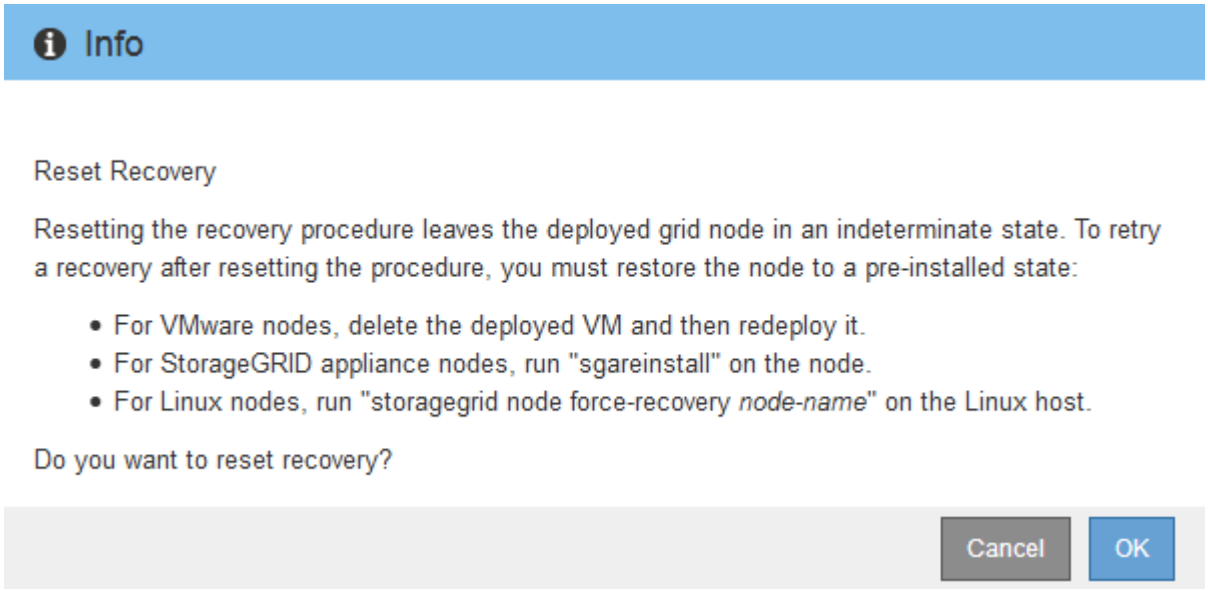
   Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de 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 Info (informações) 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.

6. Se o logon único (SSO) estiver ativado para o seu sistema StorageGRID e a confiança da parte confiável do nó que você recuperou foi configurada para usar o certificado padrão do servidor de interface de gerenciamento, atualizar (ou excluir e recriar) a confiança da parte confiável do nó nos Serviços de Federação do ative Directory (AD FS). Use o novo certificado de servidor padrão que foi gerado durante o processo de recuperação do Admin Node.

> Para configurar uma confiança de parte confiável, consulte as instruções para administrar o StorageGRID. Para acessar o certificado padrão do servidor, faça login no shell de comando do nó Admin. Vá para `/var/local/mgmt-api` o diretório e selecione o `server.crt` arquivo.

Informações relacionadas

"Administrar o StorageGRID"

"Preparação de um aparelho para reinstalação (apenas substituição da plataforma)"

Restaurando o log de auditoria no nó de administração não primário recuperado

Se você conseguiu preservar o log de auditoria do nó de administração não primário com falha, de modo que as informações de log de auditoria histórica sejam mantidas, você pode copiá-lo para o nó de administração não primário que você está recuperando.

- O Admin Node recuperado deve ser instalado e em execução.
- Você deve ter copiado os logs de auditoria para outro local depois que o nó Admin original falhou.

Se um nó Admin falhar, os logs de auditoria salvos nesse nó Admin são potencialmente perdidos. Pode ser possível preservar dados de perda copiando logs de auditoria do nó de administração com falha e restaurando esses logs de auditoria para o nó de administração recuperado. Dependendo da falha, talvez não seja possível copiar logs de auditoria do nó de administração com falha. Nesse caso, se a implantação tiver mais de um nó Admin, você poderá recuperar logs de auditoria de outro nó Admin à medida que os logs de auditoria são replicados para todos os nós Admin.

Se houver apenas um nó Admin e o log de auditoria não puder ser copiado do nó com falha, o nó Admin recuperado inicia a gravação de eventos para o log de auditoria como se a instalação fosse nova.

Você deve recuperar um nó Admin o mais rápido possível para restaurar a funcionalidade de log.

1. Faça login no nó de administração recuperado:

   a. Digite o seguinte comando
   `ssh admin@recovery_Admin_Node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   Depois de iniciar sessão como root, o aviso muda de `$` para `#`.

2. Verifique quais arquivos de auditoria foram preservados:

   ```
   cd /var/local/audit/export
   ```

3. Copie os arquivos de log de auditoria preservados para o Admin Node recuperado:

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   Quando solicitado, insira a senha para admin.

4. Para segurança, exclua os logs de auditoria do nó de grade com falha depois de verificar se eles foram copiados com sucesso para o nó de administração recuperado.
5. Atualize as configurações de usuário e grupo dos arquivos de log de auditoria no Admin Node recuperado:

   ```
   chown ams-user:bycast *
   ```

6. Faça logout como root: `exit`

Você também deve restaurar qualquer acesso de cliente pré-existente ao compartilhamento de auditoria. Para obter mais informações, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Redefinir o remetente preferido no nó de administração não primário recuperado

Se o nó de administração não primário que está a recuperar estiver atualmente definido como o remetente preferido de notificações de alerta, notificações de alarme e mensagens AutoSupport, tem de reconfigurar esta definição no sistema StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- O Admin Node recuperado deve ser instalado e em execução.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**.
2. Selecione o Admin Node recuperado na lista suspensa **Preferred Sender**.
3. Clique em **aplicar alterações**.

Informações relacionadas

"Administrar o StorageGRID"

Restaurando o banco de dados Admin Node ao recuperar um Admin Node não primário

Se você quiser manter as informações históricas sobre atributos, alarmes e alertas em um nó de administração não primário que falhou, você pode restaurar o banco de dados do nó de administração do nó principal.

- O Admin Node recuperado deve ser instalado e em execução.
- O sistema StorageGRID deve incluir pelo menos dois nós de administração.
- Tem de ter o `Passwords.txt` ficheiro.

- Você deve ter a senha de provisionamento.

Se um nó Admin falhar, as informações históricas armazenadas em seu banco de dados Admin Node serão perdidas. Esta base de dados inclui as seguintes informações:

- Histórico de alertas
- Histórico de alarmes
- Dados de atributos históricos, que são usados nos gráficos e relatórios de texto disponíveis na página **suporte Ferramentas topologia de Grade**.

Quando você recupera um Admin Node, o processo de instalação do software cria um banco de dados Admin Node vazio no nó recuperado. No entanto, o novo banco de dados inclui apenas informações para servidores e serviços que atualmente fazem parte do sistema ou adicionados posteriormente.

Se você restaurou um nó de administração não primário, você poderá restaurar as informações históricas copiando o banco de dados do nó de administração do nó principal (o *nó de administração de origem*) para o nó recuperado.

> Copiar o banco de dados Admin Node pode levar várias horas. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no nó de origem.

1. Faça login no nó de administração de origem:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Execute o seguinte comando a partir do Admin Node de origem. Em seguida, insira a senha de provisionamento, se solicitado. `recover-access-points`
3. No Admin Node de origem, pare o serviço MI: `service mi stop`
4. No Admin Node de origem, pare o serviço Management Application Program Interface (mgmt-api): `service mgmt-api stop`
5. Execute as seguintes etapas no nó de administração recuperado:
   a. Faça login no nó de administração recuperado:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   b. Parar o serviço MI: `service mi stop`
   c. Pare o serviço mgmt-api: `service mgmt-api stop`
   d. Adicione a chave privada SSH ao agente SSH. Introduza:`ssh-add`
   e. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
   f. Copie o banco de dados do Admin Node de origem para o Admin Node recuperado:

`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Quando solicitado, confirme se você deseja substituir o banco de dados MI no Admin Node recuperado.

   O banco de dados e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado.

h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza:`ssh-add -D`

6. Reinicie os serviços no Admin Node de origem: `service servermanager start`

Restaurando métricas Prometheus ao recuperar um nó Admin não primário

Opcionalmente, você pode manter as métricas históricas mantidas pelo Prometheus em um nó Admin não primário que falhou.

- O Admin Node recuperado deve ser instalado e em execução.
- O sistema StorageGRID deve incluir pelo menos dois nós de administração.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter a senha de provisionamento.

Se um nó Admin falhar, as métricas mantidas no banco de dados Prometheus no nó Admin serão perdidas. Quando você recupera o Admin Node, o processo de instalação do software cria um novo banco de dados Prometheus. Depois que o nó de administração recuperado é iniciado, ele Registra as métricas como se você tivesse executado uma nova instalação do sistema StorageGRID.

Se você restaurou um nó Admin não primário, você poderá restaurar as métricas históricas copiando o banco de dados Prometheus do nó Admin primário (o *source Admin Node*) para o nó Admin recuperado.

> Copiar o banco de dados Prometheus pode levar uma hora ou mais. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no Admin Node de origem.

1. Faça login no nó de administração de origem:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. No Admin Node de origem, pare o serviço Prometheus: `service prometheus stop`
3. Execute as seguintes etapas no nó de administração recuperado:
   a. Faça login no nó de administração recuperado:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`

iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

b. Pare o serviço Prometheus: `service prometheus stop`

c. Adicione a chave privada SSH ao agente SSH. Introduza:`ssh-add`

d. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

e. Copie o banco de dados Prometheus do nó Admin de origem para o nó Admin recuperado: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no nó Admin recuperado.

O banco de dados Prometheus original e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado. É apresentado o seguinte estado:

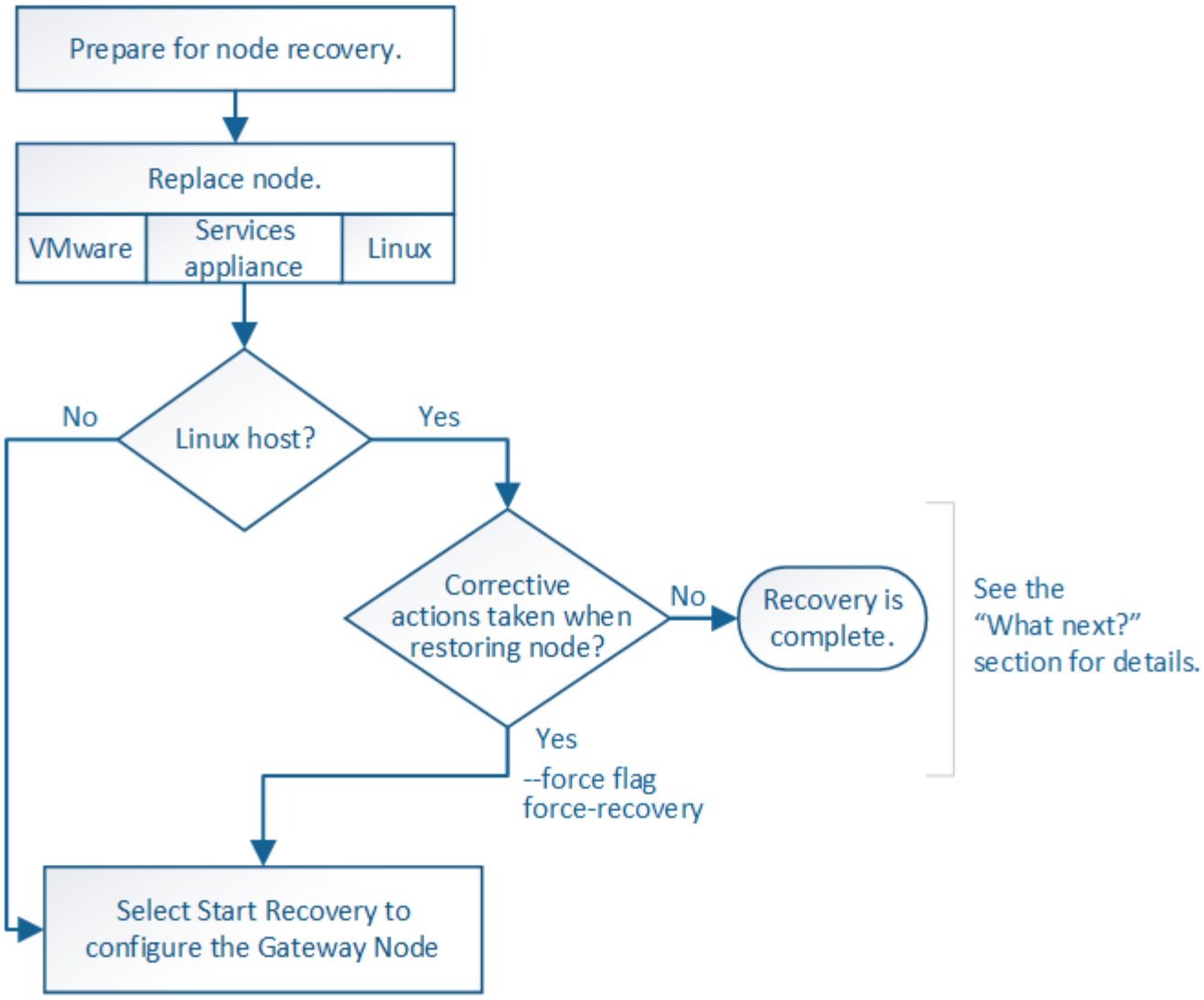
Banco de dados clonado, iniciando serviços

a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza:`ssh-add -D`

4. Reinicie o serviço Prometheus no Admin Node de origem.`service prometheus start`

Recuperando-se de falhas do Gateway Node

Você deve concluir uma sequência de tarefas na ordem exata para recuperar de uma falha do Gateway Node.



Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

Passos

- "Substituindo um nó de gateway"
- "Selecione Iniciar recuperação para configurar um nó de gateway"

Substituindo um 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	"Substituindo um nó VMware"
Linux	"Substituindo um nó Linux"
Aparelhos de serviços SG100 e SG1000	"Substituir um dispositivo de serviços"
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Selecione Iniciar recuperação para configurar um nó de gateway

Depois de substituir um nó de gateway, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

O que você vai precisar

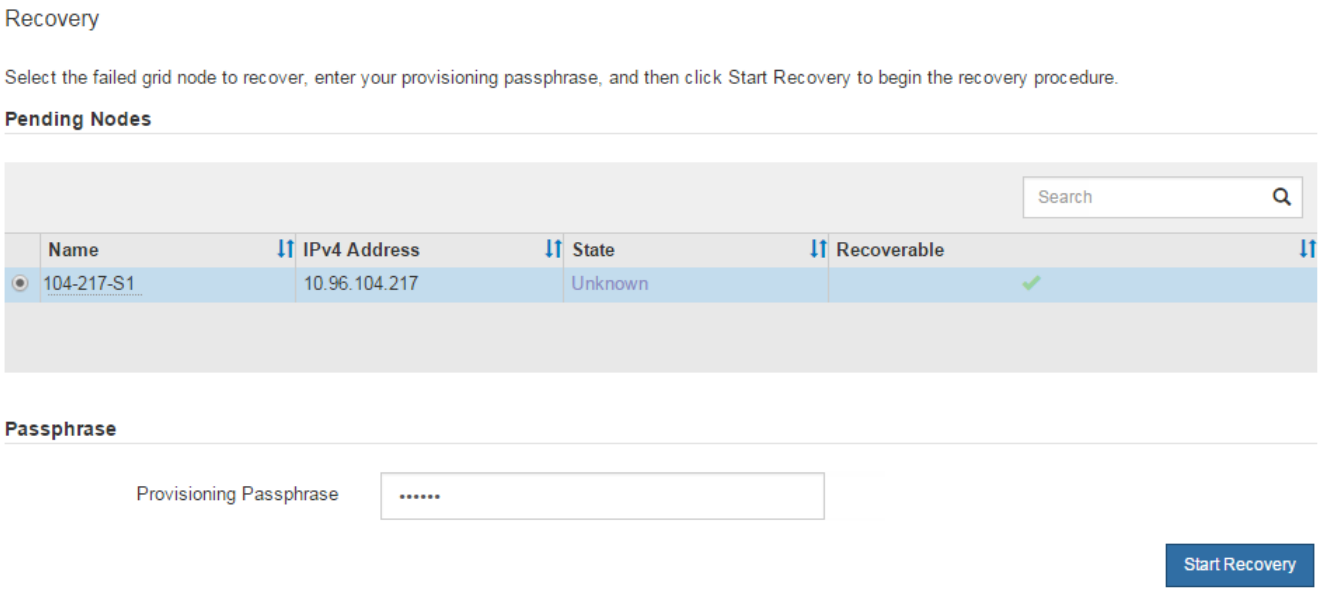
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado e configurado o nó de substituição.

Passos

1. No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção recuperação**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

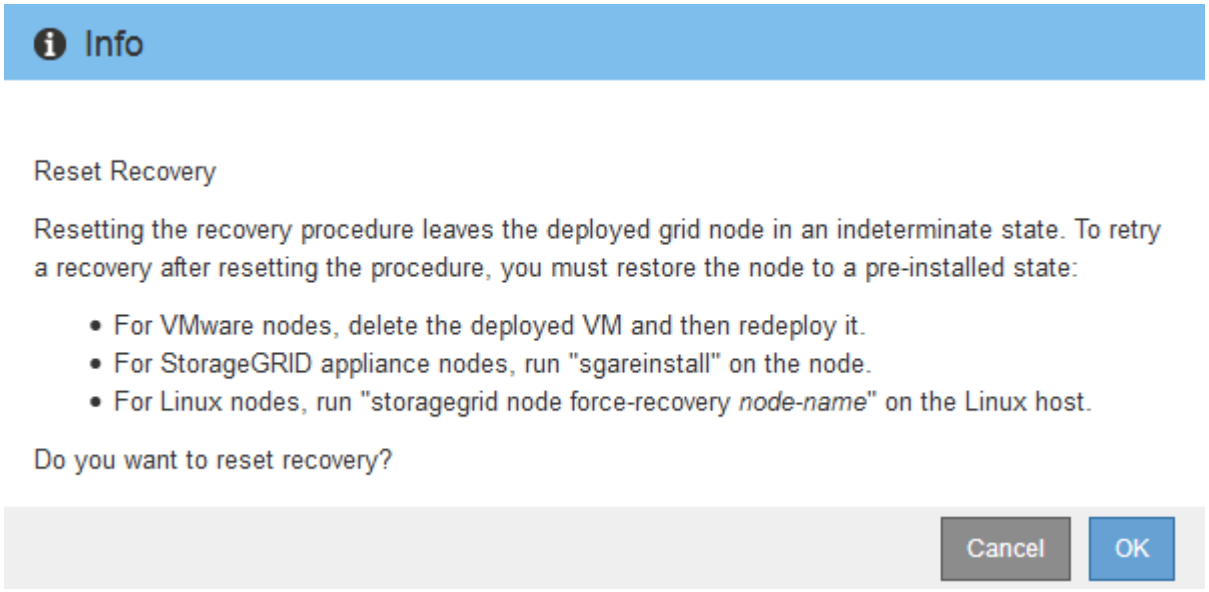
   Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de 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 Info (informações) 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:

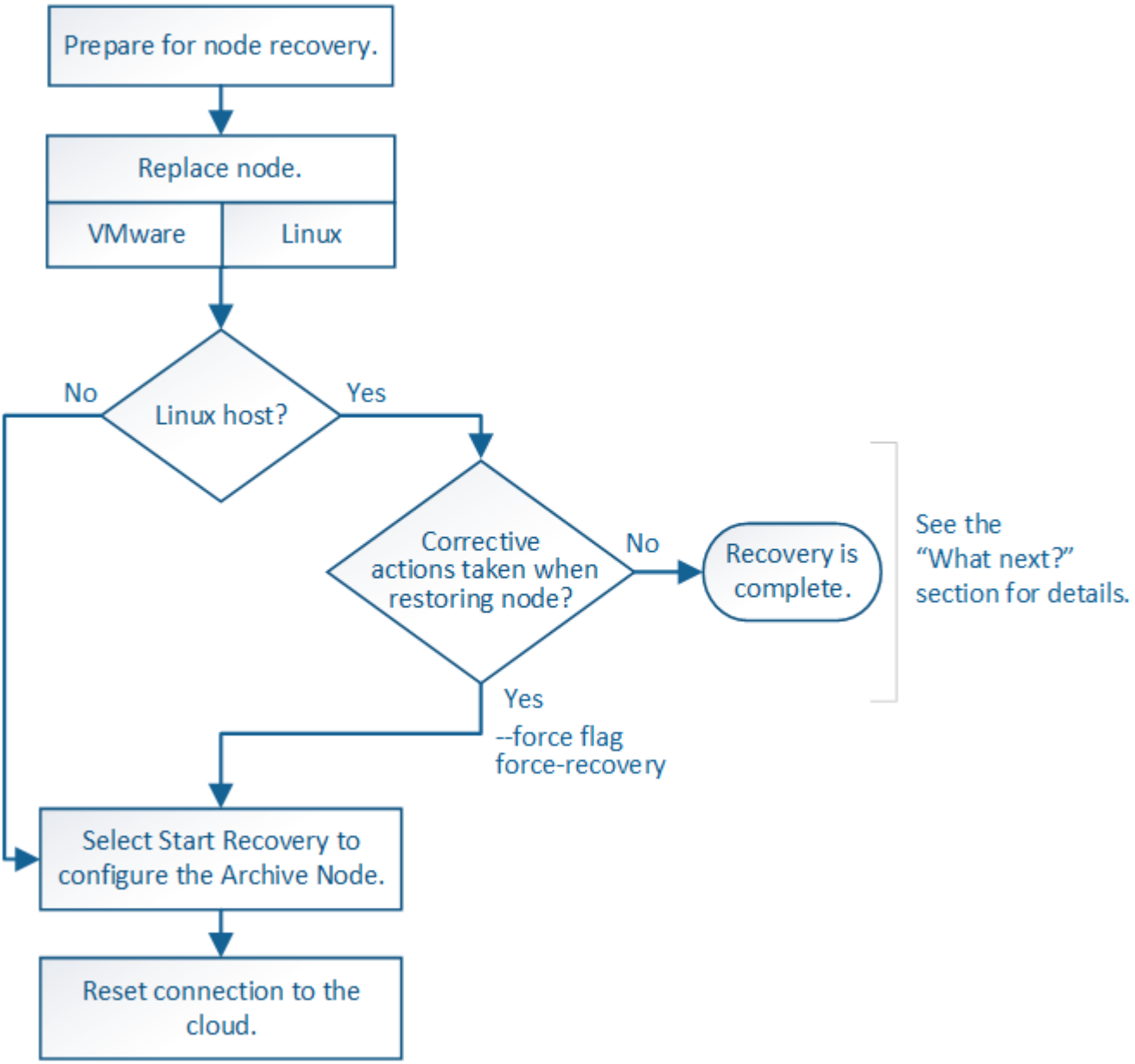
- **VMware**: Exclua o nó de grade virtual implantado. Em seguida, quando estiver pronto para reiniciar a recuperação, reimplante o nó.
- * Linux*: Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`
- **Appliance**: Se você quiser repetir a recuperação após redefinir o procedimento, você deve restaurar o nó do dispositivo para um estado pré-instalado executando `sgareinstall` no nó.

Informações relacionadas

"Preparação de um aparelho para reinstalação (apenas substituição da plataforma)"

Recuperando-se de falhas do nó de arquivamento

Você deve concluir uma sequência de tarefas na ordem exata para recuperar de uma falha de nó de arquivo.



Sobre esta tarefa

A recuperação do nó de arquivamento é afetada pelos seguintes problemas:

- Se a política ILM estiver configurada para replicar uma única cópia.

  Em um sistema StorageGRID configurado para fazer uma única cópia de objetos, uma falha de nó de arquivo pode resultar em uma perda irrecuperável de dados. Se houver uma falha, todos esses objetos são perdidos; no entanto, você ainda deve executar procedimentos de recuperação para "limpar" seu sistema StorageGRID e limpar as informações de objetos perdidos do banco de dados.

- Se ocorrer uma falha do nó de arquivamento durante a recuperação do nó de storage.

  Se o nó de arquivo falhar ao processar recuperações em massa como parte de uma recuperação do nó de armazenamento, você deve repetir o procedimento para recuperar cópias de dados de objeto para o nó de armazenamento desde o início para garantir que todos os dados de objeto recuperados do nó de arquivo sejam restaurados para o nó de armazenamento.

Passos

- "Substituindo um nó de arquivo"
- "Selecionar Iniciar recuperação para configurar um nó de arquivo"
- "Redefinir a conexão do Archive Node à nuvem"

Substituindo um nó de arquivo

Para recuperar um nó de arquivo, você deve primeiro substituir o nó.

Você deve selecionar o procedimento de substituição do nó para sua plataforma. As etapas para substituir um nó são as mesmas para todos os tipos de nós de grade.

Plataforma	Procedimento
VMware	"Substituindo um nó VMware"
Linux	"Substituindo um nó Linux"
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Selecionar Iniciar recuperação para configurar um nó de arquivo

Depois de substituir um nó de arquivo, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

O que você vai precisar

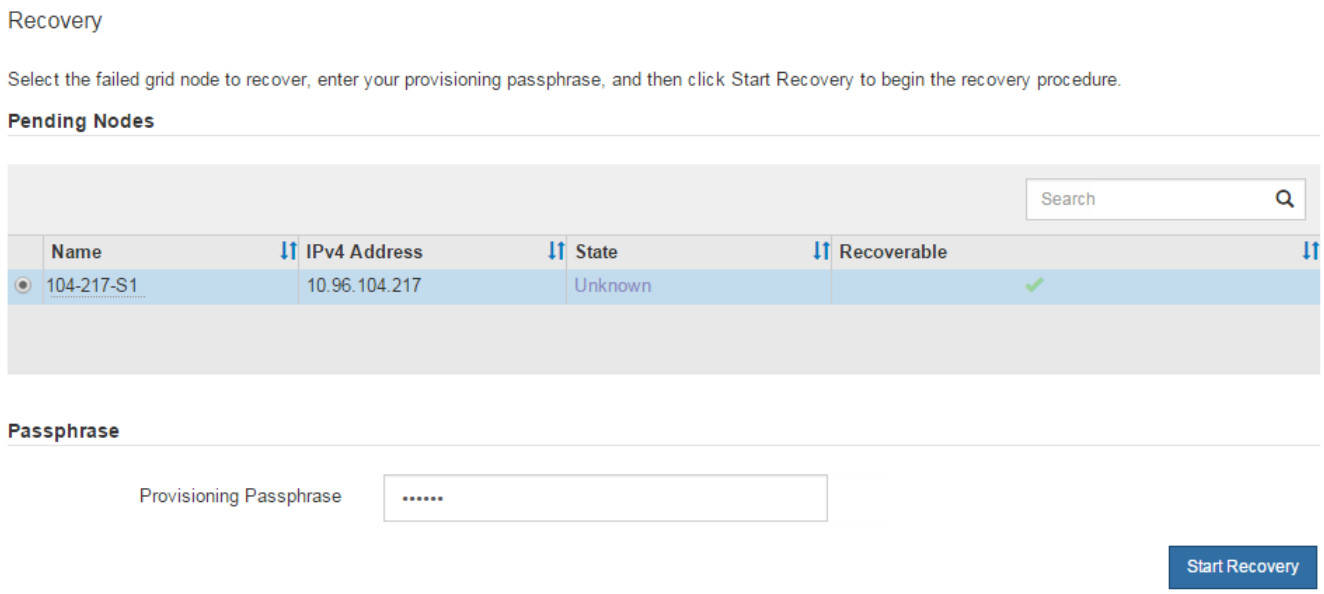
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado e configurado o nó de substituição.

Passos

1. No Gerenciador de Grade, selecione **Manutenção tarefas de Manutenção recuperação**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

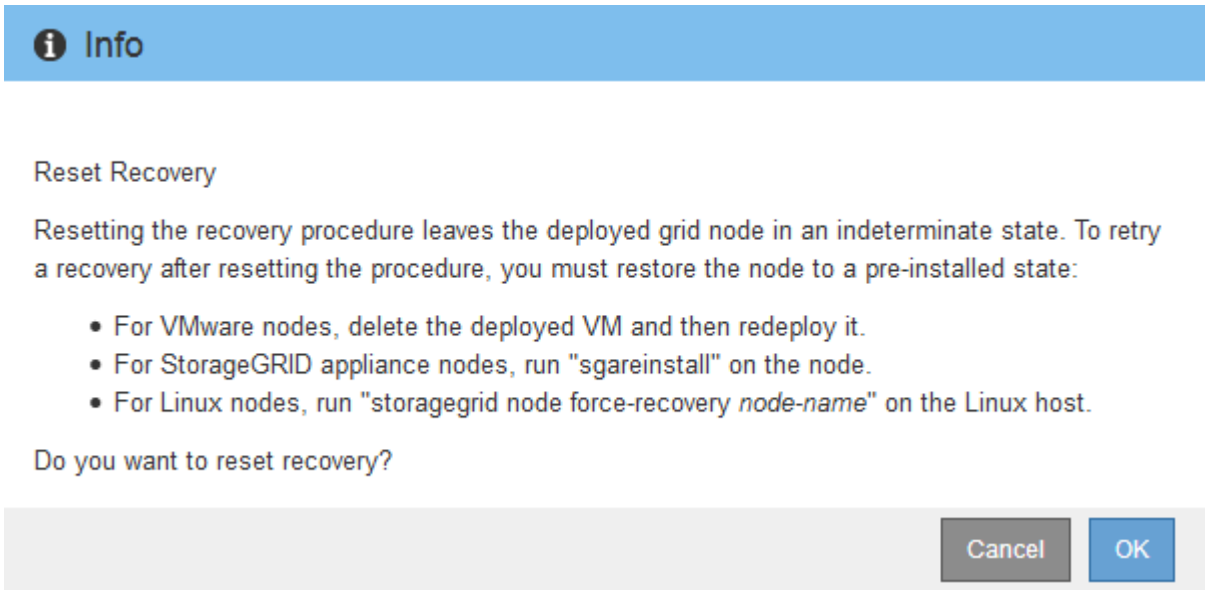
Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de 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 Info (informações) 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`

Redefinir a conexão do Archive Node à nuvem

Depois de recuperar um nó de arquivo que segmenta a nuvem através da API S3, você precisa modificar as configurações para redefinir as conexões. Um alarme de Estado de replicação de saída (ORSU) é acionado se o nó de arquivo não conseguir recuperar dados de objeto.

> Se o seu nó de arquivo se conetar ao armazenamento externo por meio do middleware TSM, o nó será redefinido automaticamente e você não precisará reconfigurar.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione **Archive Node** > **ARC** > **Target**.
3. Edite o campo **chave de acesso** inserindo um valor incorreto e clique em **aplicar alterações**.
4. Edite o campo **chave de acesso** inserindo o valor correto e clique em **aplicar alterações**.

Todos os tipos de nós de grade: Substituindo um nó VMware

Quando você recupera um nó StorageGRID com falha que foi hospedado no VMware, você deve remover o nó com falha e implantar um nó de recuperação.

O que você vai precisar

Você deve ter determinado que a máquina virtual não pode ser restaurada e deve ser substituída.

Sobre esta tarefa

Você usa o VMware vSphere Web Client para remover primeiro a máquina virtual associada ao nó de grade com falha. Em seguida, você pode implantar uma nova máquina virtual.

Este procedimento é apenas uma etapa no processo de recuperação do nó de grade. O procedimento de remoção e implantação de nós é o mesmo para todos os nós da VMware, incluindo nós de administração, nós de storage, nós de gateway e nós de arquivamento.

Passos

1. Faça login no VMware vSphere Web Client.
2. Navegue para a máquina virtual com falha no nó de grade.
3. Anote todas as informações necessárias para implantar o nó de recuperação.
   a. Clique com o botão direito do Mouse na máquina virtual, selecione a guia **Editar configurações** e observe as configurações em uso.
   b. Selecione a guia **vApp Options** para exibir e gravar as configurações de rede do nó de grade.
4. Se o nó de grade com falha for um nó de armazenamento, determine se algum dos discos rígidos virtuais

usados para armazenamento de dados não está danificado e preserve-os para refixação ao nó de grade recuperado.

5. Desligue a máquina virtual.
6. Selecione **ações** > **todas as ações do vCenter** > **Excluir do disco** para excluir a máquina virtual.
7. Implante uma nova máquina virtual para ser o nó de substituição e conete-a a uma ou mais redes StorageGRID.

   Ao implantar o nó, você pode opcionalmente remapear as portas dos nós ou aumentar as configurações de CPU ou memória.

   > Depois de implantar o novo nó, você pode adicionar novos discos virtuais de acordo com seus requisitos de armazenamento, reanexar quaisquer discos rígidos virtuais preservados do nó de grade com falha removido anteriormente ou ambos.

   Para obter instruções:

   "Instale o VMware" > implantando um nó StorageGRID como uma máquina virtual

8. Conclua o procedimento de recuperação do nó, com base no tipo de nó que está a recuperar.

Tipo de nó	Vá para
Nó de administração principal	"Configurar o nó de administração principal de substituição"
Nó de administração não primário	"Selecionando Iniciar recuperação para configurar um nó de administração não primário"
Nó de gateway	"Selecione Iniciar recuperação para configurar um nó de gateway"
Nó de storage	"Selecionando Iniciar recuperação para configurar um nó de armazenamento"
Nó de arquivo	"Selecionar Iniciar recuperação para configurar um nó de arquivo"

Todos os tipos de nó de grade: Substituindo um nó Linux

Se uma falha exigir que você implante um ou mais novos hosts físicos ou virtuais ou reinstale o Linux em um host existente, você deve implantar e configurar o host de substituição antes de recuperar o nó da grade. Este procedimento é uma etapa do processo de recuperação do nó de grade para todos os tipos de nós de grade.

"Linux" refere-se a uma implantação Red Hat Enterprise Linux, Ubuntu, CentOS ou Debian. Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

Este procedimento só é executado como uma etapa no processo de recuperação de nós de storage baseados em software, nós de administração primários ou não primários, nós de gateway ou nós de arquivamento. As etapas são idênticas independentemente do tipo de nó de grade que você está recuperando.

Se mais de um nó de grade estiver hospedado em um host Linux físico ou virtual, você poderá recuperar os

nós de grade em qualquer ordem. No entanto, a recuperação de um nó Admin primário primeiro, se presente, impede que a recuperação de outros nós de grade pare, pois eles tentam entrar em Contato com o nó Admin primário para se Registrar para recuperação.

1. "Implantando novos hosts Linux"
2. "Restaurando nós de grade para o host"
3. "O que vem a seguir: Executando etapas adicionais de recuperação, se necessário"

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Implantando novos hosts Linux

Com algumas exceções, você prepara os novos hosts como fez durante o processo de instalação inicial.

Para implantar hosts Linux novos ou reinstalados físicos ou virtuais, siga o procedimento para preparar os hosts nas instruções de instalação do StorageGRID para o seu sistema operacional Linux.

Este procedimento inclui etapas para realizar as seguintes tarefas:

1. Instale o Linux.
2. Configure a rede host.
3. Configurar o armazenamento do host.
4. Instale o Docker.
5. Instale o serviço de host do StorageGRID.

> Pare depois de concluir a tarefa "Instalar o serviço de host do StorageGRID" nas instruções de instalação. Não inicie a tarefa "implantando nós de grade".

Ao executar estas etapas, observe as seguintes diretrizes importantes:

- Certifique-se de usar os mesmos nomes de interface de host usados no host original.
- Se você usar o storage compartilhado para oferecer suporte aos nós do StorageGRID ou tiver movido algumas ou todas as unidades de disco ou SSDs dos nós com falha para os nós de substituição, será necessário restabelecer os mesmos mapeamentos de storage que estavam presentes no host original. Por exemplo, se você usou WWIDs e aliases `/etc/multipath.conf` como recomendado nas instruções de instalação, certifique-se de usar os mesmos pares alias/WWID no `/etc/multipath.conf` host de substituição.
- Se o nó StorageGRID usar o storage atribuído a partir de um sistema NetApp AFF, confirme se o volume não tem uma política de disposição em camadas do FabricPool habilitada. A desativação da disposição em camadas do FabricPool para volumes usados com nós do StorageGRID simplifica a solução de problemas e as operações de storage.

> Nunca use o FabricPool para categorizar dados relacionados ao StorageGRID de volta ao próprio StorageGRID. A disposição em camadas de dados do StorageGRID de volta para o StorageGRID aumenta a complexidade operacional e a solução de problemas.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Restaurando nós de grade para o host

Para restaurar um nó de grade com falha para um novo host Linux, você restaura o arquivo de configuração do nó usando os comandos apropriados.

Ao fazer uma nova instalação, você cria um arquivo de configuração de nó para cada nó de grade a ser instalado em um host. Ao restaurar um nó de grade para um host de substituição, você restaura ou substitui o arquivo de configuração do nó para qualquer nó de grade com falha.

Se algum volume de armazenamento de bloco tiver sido preservado do host anterior, talvez seja necessário executar procedimentos de recuperação adicionais. Os comandos nesta seção ajudam a determinar quais procedimentos adicionais são necessários.

Passos

- "Restauração e validação de nós de grade"
- "Iniciando o serviço de host do StorageGRID"
- "Recuperando nós que não iniciam normalmente"

Restauração e validação de nós de grade

Você deve restaurar os arquivos de configuração de grade para todos os nós de grade com falha e, em seguida, validar os arquivos de configuração de grade e resolver quaisquer erros.

Sobre esta tarefa

Você pode importar qualquer nó de grade que deve estar presente no host, desde que seu `/var/local` volume não tenha sido perdido como resultado da falha do host anterior. Por exemplo, o `/var/local` volume ainda pode existir se você usou armazenamento compartilhado para volumes de dados do sistema StorageGRID, conforme descrito nas instruções de instalação do StorageGRID para o seu sistema operacional Linux. A importação do nó restaura o arquivo de configuração do nó para o host.

Se não for possível importar nós ausentes, você deve recriar seus arquivos de configuração de grade.

Em seguida, você deve validar o arquivo de configuração de grade e resolver quaisquer problemas de rede ou armazenamento que possam ocorrer antes de reiniciar o StorageGRID. Quando você cria novamente o arquivo de configuração para um nó, você deve usar o mesmo nome para o nó de substituição usado para o nó que você está recuperando.

Consulte as instruções de instalação para obter mais informações sobre a localização `/var/local` do volume de um nó.

Passos

1. Na linha de comando do host recuperado, liste todos os nós de grade StorageGRID configurados atualmente:`sudo storagegrid node list`

   Se nenhum nó de grade estiver configurado, não haverá saída. Se alguns nós de grade estiverem configurados, espere a saída no seguinte formato:

```
Name                Metadata-Volume
=============================================================
dc1-adm1            /dev/mapper/sgws-adm1-var-local
dc1-gw1             /dev/mapper/sgws-gw1-var-local
dc1-sn1             /dev/mapper/sgws-sn1-var-local
dc1-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 voltar a se juntar à grade, conforme descrito em ""executando etapas de recuperação adicionais, se necessário".

3. Para nós de grade que não têm um `/var/local` volume, recrie o arquivo de configuração do nó para restaurá-lo para o host.

   Siga as diretrizes em ""criando arquivos de configuração de nó"" nas instruções de instalação.

   > Quando você cria novamente o arquivo de configuração para um nó, você deve usar o mesmo nome para o nó de substituição usado para o nó que você está recuperando. Para implantações Linux, verifique se o nome do arquivo de configuração contém o nome do nó. Você deve usar as mesmas interfaces de rede, bloquear mapeamentos de dispositivos e endereços IP quando possível. Essa prática minimiza a quantidade de dados que precisa ser copiada para o nó durante a recuperação, o que pode tornar a recuperação significativamente mais rápida (em alguns casos, minutos em vez de semanas).

   > Se você usar quaisquer novos dispositivos de bloco (dispositivos que o nó StorageGRID não usou anteriormente) como valores para qualquer uma das variáveis de configuração que começam `BLOCK_DEVICE_` quando você está recriando o arquivo de configuração para um nó, certifique-se de seguir todas as diretrizes em "'corrigir erros de dispositivo de bloco ausente.'"

4. Execute o seguinte comando no host recuperado para listar todos os nós do StorageGRID.

   ```
   sudo storagegrid node list
   ```

5. Valide o arquivo de configuração de nó para cada nó de grade cujo nome foi mostrado na saída da lista de nós do StorageGRID:

   ```
   sudo storagegrid node validate node-name
   ```

   Você deve resolver quaisquer erros ou avisos antes de iniciar o serviço host do StorageGRID. As seções a seguir fornecem mais detalhes sobre erros que podem ter significado especial durante a recuperação.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Correção de erros de interface de rede em falta"

"Correção de erros de dispositivo de bloco em falta"

"O que vem a seguir: Executando etapas adicionais de recuperação, se necessário"

Correção de erros de interface de rede em falta

Se a rede host não estiver configurada corretamente ou se um nome estiver incorreto, ocorrerá um erro quando o StorageGRID verificar o mapeamento especificado no `/etc/storagegrid/nodes/node-name.conf` arquivo.

Você pode ver um erro ou aviso correspondente a este padrão:

`Checking configuration file `/etc/storagegrid/nodes/node-name.conf` para o nó node-name...»`
`ERROR: node-name: GRID_NETWORK_TARGET = host-interface-name` *Node-name*: Interface '*host-interface-name*' não existe

O erro pode ser reportado para a rede de Grade, a rede Admin ou a rede Cliente. Esse erro significa que o `/etc/storagegrid/nodes/node-name.conf` arquivo mapeia a rede StorageGRID indicada para a interface do host chamada `host-interface-name`, mas não há nenhuma interface com esse nome no host atual.

Se você receber esse erro, verifique se você concluiu as etapas em "implantar 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).

Informações relacionadas

"Implantando novos hosts Linux"

Correção de erros de dispositivo de bloco em falta

O sistema verifica se cada nó recuperado mapeia para um arquivo especial válido de dispositivo de bloco ou um softlink válido para um arquivo especial de dispositivo de bloco. Se o StorageGRID encontrar mapeamento inválido no `/etc/storagegrid/nodes/node-name.conf` arquivo, um erro de dispositivo de bloco ausente será exibido.

Se observar um erro correspondente a este padrão:

`Checking configuration file /etc/storagegrid/nodes/node-name.conf for node node-name...`
`ERROR: node-name: BLOCK_DEVICE_PURPOSE = path-name node-name: path-name não existe`

Isso significa que `/etc/storagegrid/nodes/node-name.conf` mapeia o dispositivo de bloco usado por *node-name* para FINS para o caminho-nome dado no sistema de arquivos Linux, mas não há um arquivo especial válido de dispositivo de bloco ou softlink para um arquivo especial de dispositivo de bloco, nesse local.

Verifique se você concluiu as etapas em ""implantando novos hosts Linux"". Use os mesmos nomes de dispositivos persistentes para todos os dispositivos de bloco que foram usados no host original.

Se você não conseguir restaurar ou recriar o arquivo especial de dispositivo de bloco ausente, você pode alocar um novo dispositivo de bloco com o tamanho e categoria de armazenamento apropriados e editar o arquivo de configuração de nó para alterar o valor de block_DEVICE_PURPOSE para apontar para o novo arquivo especial de dispositivo de bloco.

Determine o tamanho e a categoria de armazenamento apropriados nas tabelas na seção "requisitos de armazenamento" das instruções de instalação do seu sistema operacional Linux. Revise as recomendações em ""Configurando o armazenamento do host"" antes de prosseguir com a substituição do dispositivo de bloco.

> Se você precisar fornecer um novo dispositivo de armazenamento de bloco para qualquer uma das variáveis de arquivo de configuração começando com `BLOCK_DEVICE_` porque o dispositivo de bloco original foi perdido com o host com falha, verifique se o novo dispositivo de bloco está desformatado antes de tentar outros procedimentos de recuperação. O novo dispositivo de bloco será desformatado se você estiver usando armazenamento compartilhado e tiver criado um novo volume. Se você não tiver certeza, execute o seguinte comando contra qualquer novo dispositivo de armazenamento de bloco arquivos especiais.

> Execute o seguinte comando apenas para novos dispositivos de armazenamento de bloco. Não execute este comando se você acredita que o armazenamento de bloco ainda contém dados válidos para o nó que está sendo recuperado, pois quaisquer dados no dispositivo serão perdidos.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Informações relacionadas

"Implantando novos hosts Linux"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Iniciando 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.

1. Execute os seguintes comandos em cada host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Execute o seguinte comando para garantir que a implantação está em andamento:

   `sudo storagegrid node status node-name`

   Para qualquer nó que retorna um status de não-execução ou parado, execute o seguinte comando:

   `sudo storagegrid node start node-name`

3. Se você já ativou e iniciou o serviço de host StorageGRID (ou se não tiver certeza se o serviço foi ativado e iniciado), execute também o seguinte comando:

```
sudo systemctl reload-or-restart storagegrid
```

Recuperando nós que não iniciam normalmente

Se um nó StorageGRID não se juntar novamente à grade normalmente e não aparecer como recuperável, ele pode estar corrompido. Você pode forçar o nó para o modo de recuperação.

Para forçar o nó para o modo de recuperação:

`sudo storagegrid node force-recovery node-name`

Antes de emitir este comando, confirme se a configuração de rede do nó está correta; pode ter falhado em reingressar na grade devido a mapeamentos de interface de rede incorretos ou um endereço IP ou gateway de rede de Grade incorreto.

Depois de emitir o `storagegrid node force-recovery node-name` comando, você deve executar etapas adicionais de recuperação para *node-name*.

Informações relacionadas

"O que vem a seguir: Executando etapas adicionais de recuperação, se necessário"

O que vem a seguir: Executar 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	"Configurar o nó de administração principal de substituição"
Nó de administração não primário	"Selecionando Iniciar recuperação para configurar um nó de administração não primário"
Nó de gateway	"Selecione Iniciar recuperação para configurar um nó de gateway"
Nó de arquivo	"Selecionar Iniciar recuperação para configurar um nó de arquivo"
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	"Selecionando Iniciar recuperação para configurar um nó de armazenamento"

Tipo de recuperação	Próximo passo
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.	"Recuperando-se de uma falha do volume de storage em que a unidade do sistema está intacta"

Substituindo um nó com falha por um dispositivo de serviços

Você pode usar um dispositivo de serviços SG100 ou SG1000 para recuperar um nó de gateway com falha, um nó de administrador não primário com falha ou um nó de administrador principal com falha hospedado em VMware, um host Linux ou um dispositivo de serviços. Este procedimento é uma etapa do procedimento de recuperação do nó de grade.

O que você vai precisar

- Você deve ter determinado que uma das seguintes situações é verdadeira:
  - A máquina virtual que hospeda o nó não pode ser restaurada.
  - O host físico ou virtual do Linux para o nó de grade falhou e deve ser substituído.
  - O dispositivo de serviços que hospeda o nó de grade deve ser substituído.
- Você deve certificar-se de que a versão do Instalador de dispositivos StorageGRID no utilitário de serviços corresponde à versão de software do seu sistema StorageGRID, conforme descrito em instalação e manutenção de hardware para verificar e atualizar a versão do Instalador de dispositivos StorageGRID.

  "Aparelhos de serviços SG100 SG1000"

> Não implante um dispositivo de serviço SG100 e SG1000 no mesmo local. Pode resultar em performance imprevisível.

Sobre esta tarefa

Você pode usar um dispositivo de serviços SG100 ou SG1000 para recuperar um nó de grade com falha nos seguintes casos:

- O nó com falha foi hospedado no VMware ou Linux (mudança de plataforma)
- O nó com falha foi hospedado em um dispositivo de serviços (substituição da plataforma)

Passos

- "Instalar um dispositivo de serviços (apenas mudança de plataforma)"
- "Preparação de um aparelho para reinstalação (apenas substituição da plataforma)"
- "Iniciar a instalação de software em um dispositivo de serviços"
- "Instalação do dispositivo de serviços de monitoramento"

Instalar um dispositivo de serviços (apenas mudança de plataforma)

Quando você estiver recuperando um nó de grade com falha hospedado no VMware ou em um host Linux e estiver usando um dispositivo de serviços SG100 ou SG1000 para o nó de substituição, primeiro instale o novo hardware do dispositivo usando o mesmo nome do nó que o nó com falha.

Você deve ter as seguintes informações sobre o nó com falha:

- **Nome do nó**: Você deve instalar o utilitário de serviços usando o mesmo nome do nó que o nó com falha.
- **Endereços IP**: Você pode atribuir ao utilitário de serviços os mesmos endereços IP que o nó com falha, que é a opção preferida, ou você pode selecionar um novo endereço IP não utilizado em cada rede.

Execute este procedimento somente se você estiver recuperando um nó com falha hospedado no VMware ou Linux e estiver substituindo-o por um nó hospedado em um dispositivo de serviços.

1. Siga as instruções para instalar um novo dispositivo de serviços SG100 ou SG1000.
2. Quando for solicitado um nome de nó, use o nome do nó do nó com falha.

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

Preparação de um 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.

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.

Iniciar a instalação de software em um dispositivo de serviços

Para instalar um nó de gateway ou nó de administrador em um dispositivo de serviços SG100 ou SG1000, use o Instalador de dispositivos StorageGRID, que está incluído no dispositivo.

O que você vai precisar

- O dispositivo deve ser instalado em um rack, conetado às redes e ligado.
- Os links de rede e endereços IP devem ser configurados para o dispositivo usando o Instalador de dispositivos StorageGRID.
- Se você estiver instalando um nó de gateway ou um nó de administrador não primário, você saberá o endereço IP do nó de administrador principal para a grade StorageGRID.
- Todas as sub-redes de rede de grade listadas na página Configuração IP do Instalador de dispositivos StorageGRID devem ser definidas na Lista de sub-redes de rede de grade no nó de administração principal.

Para obter instruções para concluir estas tarefas de pré-requisito, consulte as instruções de instalação e manutenção de um dispositivo de serviços SG100 ou SG1000.

- Você deve estar usando um navegador da Web compatível.
- Você deve saber um dos endereços IP atribuídos ao dispositivo. Você pode usar o endereço IP da rede Admin, da rede Grid ou da rede Client.
- Se você está instalando um nó de administrador principal, você tem os arquivos de instalação Ubuntu ou Debian para esta versão do StorageGRID disponíveis.

> Uma versão recente do software StorageGRID é pré-carregada no equipamento de serviços durante o fabrico. Se a versão pré-carregada do software corresponder à versão que está a ser utilizada na implementação do StorageGRID, não necessita dos ficheiros de instalação.

Sobre esta tarefa

Para instalar o software StorageGRID em um dispositivo de serviços SG100 ou SG1000:

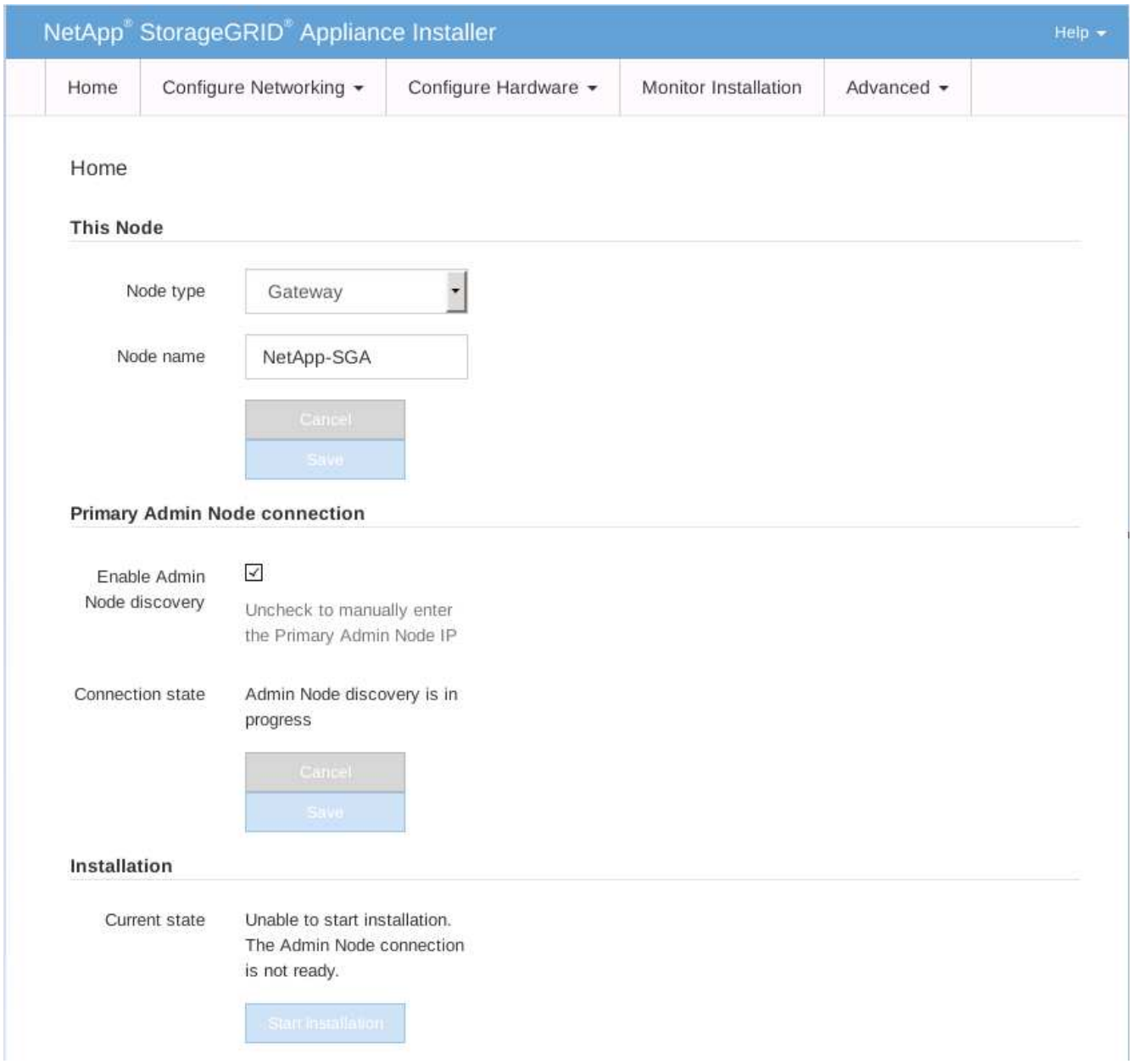
- Para um nó de administração principal, especifique o nome do nó e, em seguida, carregue os pacotes de software apropriados (se necessário).
- Para um nó de administração não primário ou um nó de gateway, especifique ou confirme o endereço IP do nó de administração principal e o nome do nó.
- Inicie a instalação e aguarde à medida que os volumes estão configurados e o software está instalado.
- No decorrer do processo, a instalação é interrompida. Para retomar a instalação, você deve entrar no Gerenciador de Grade e configurar o nó pendente como um substituto para o nó com falha.
- Depois de configurar o nó, o processo de instalação do appliance é concluído e o appliance é reinicializado.

Passos

1. Abra um navegador e insira um dos endereços IP do dispositivo de serviços SG100 ou SG1000.

`https://Controller_IP:8443`

A página inicial do instalador do dispositivo StorageGRID é exibida.



2. Para instalar um nó de administração principal:

   a. Na seção este nó, para **tipo de nó**, selecione **Admin principal**.

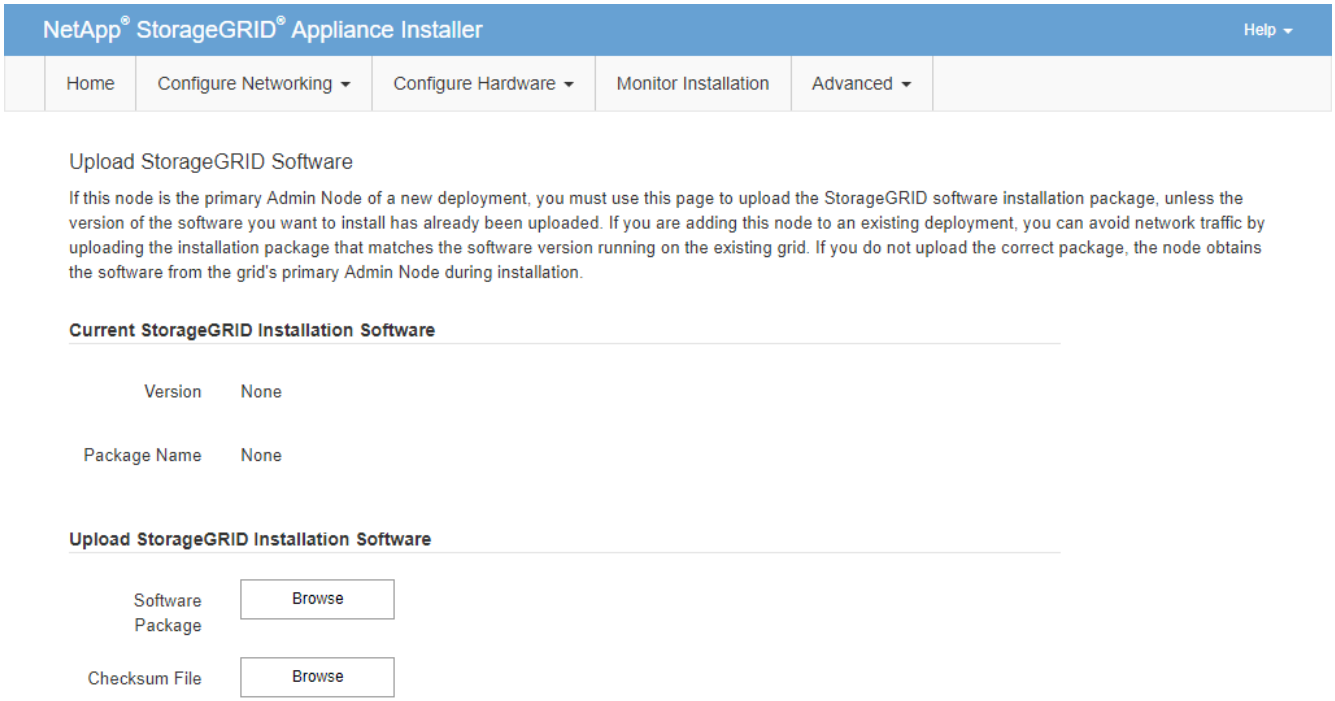
   b. No campo **Nome do nó**, insira o mesmo nome que foi usado para o nó que você está recuperando e clique em **Salvar**.

   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".
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 instalação e manutenção do seu aparelho.

5. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.

   O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

   > Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor** na barra de menus.

Informações relacionadas

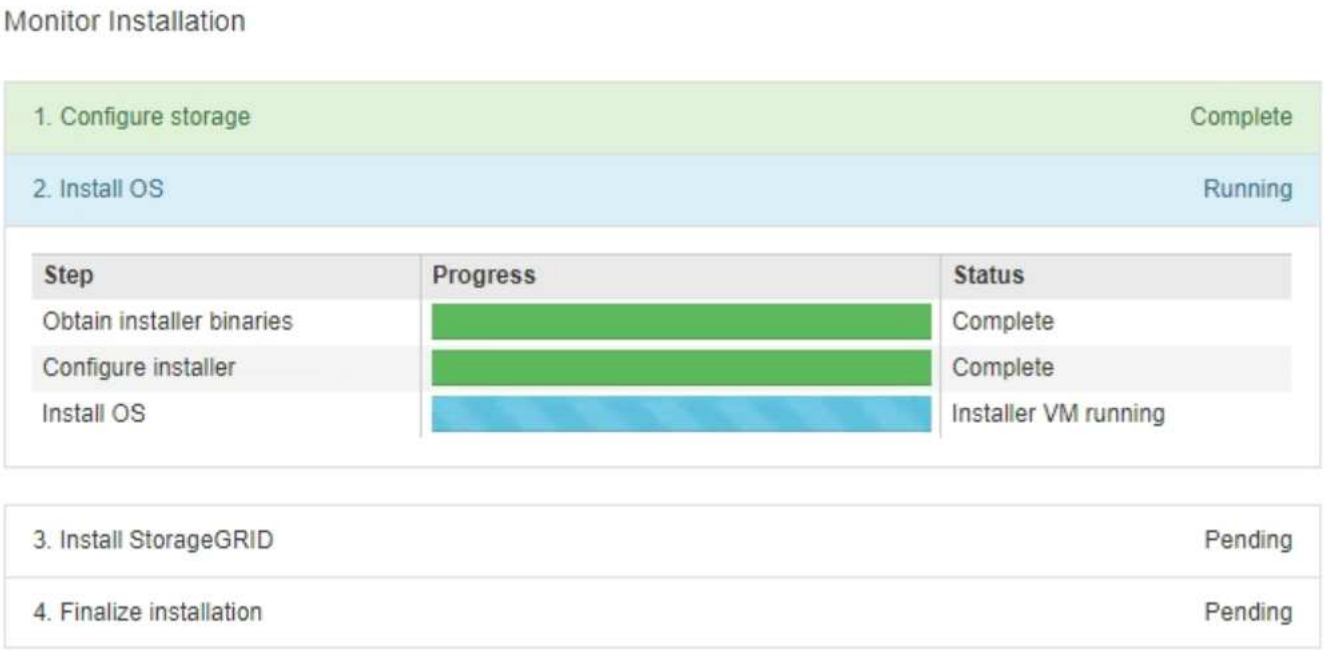
"Aparelhos de serviços SG100 SG1000"

Instalação do dispositivo de serviços de monitoramento

O Instalador de dispositivos StorageGRID fornece o status até que a instalação esteja concluída. Quando a instalação do software estiver concluída, o dispositivo é reinicializado.

1. Para monitorar o progresso da instalação, clique em **Monitor Installation** na barra de menus.

   A página Instalação do monitor mostra o progresso da instalação.



A barra de status azul indica qual tarefa está atualmente em andamento. As barras de estado verdes indicam tarefas concluídas com êxito.

> ⓘ O instalador garante que as tarefas concluídas em uma instalação anterior não sejam executadas novamente. Se você estiver reexecutando uma instalação, todas as tarefas que não precisam ser executadas novamente serão mostradas com uma barra de status verde e um status de ""pulado"".

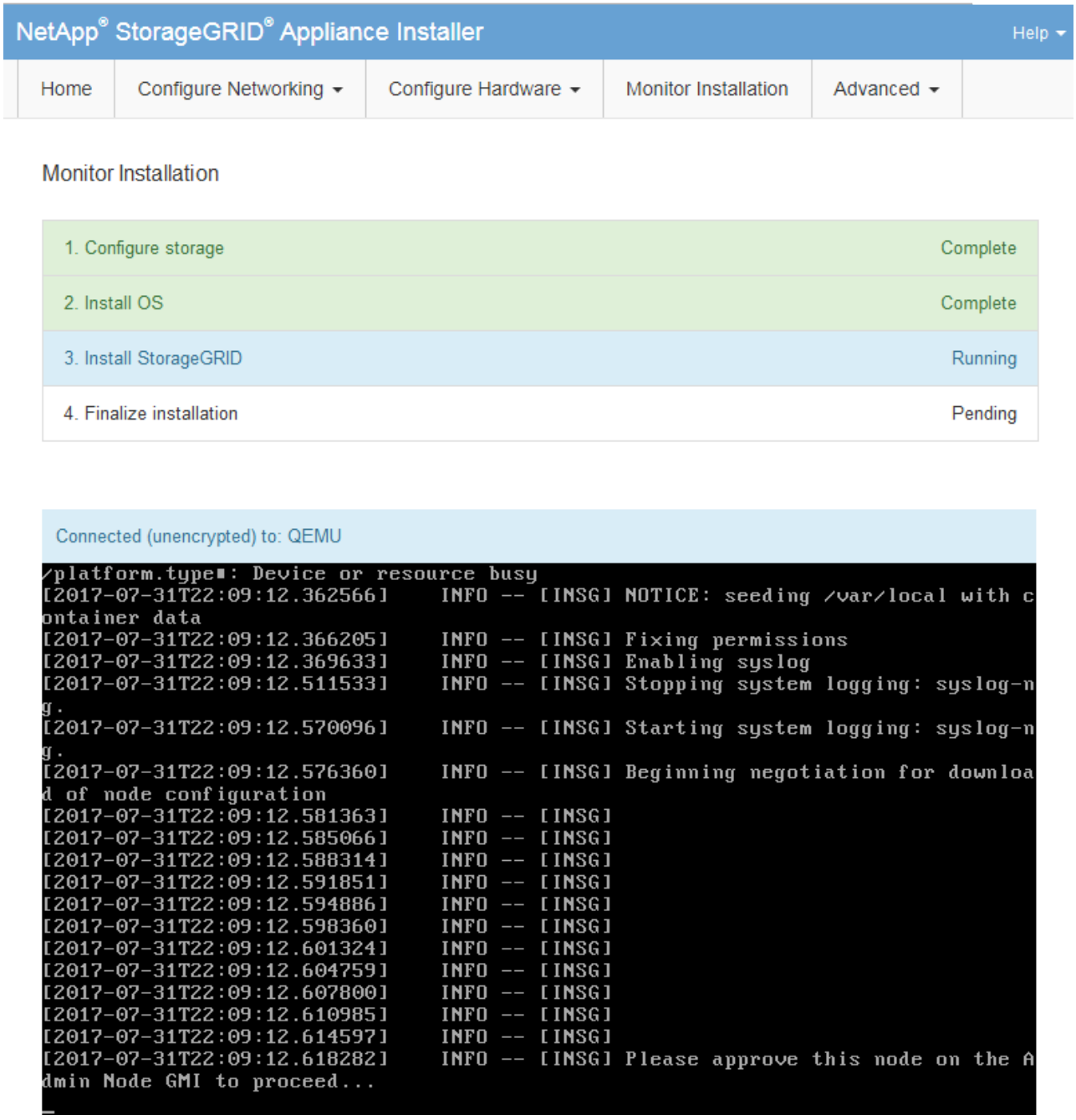
2. Reveja o progresso das duas primeiras fases de instalação.
   - **1. Configurar armazenamento**

     Durante este estágio, o instalador limpa qualquer configuração existente das unidades e configura as configurações do host.

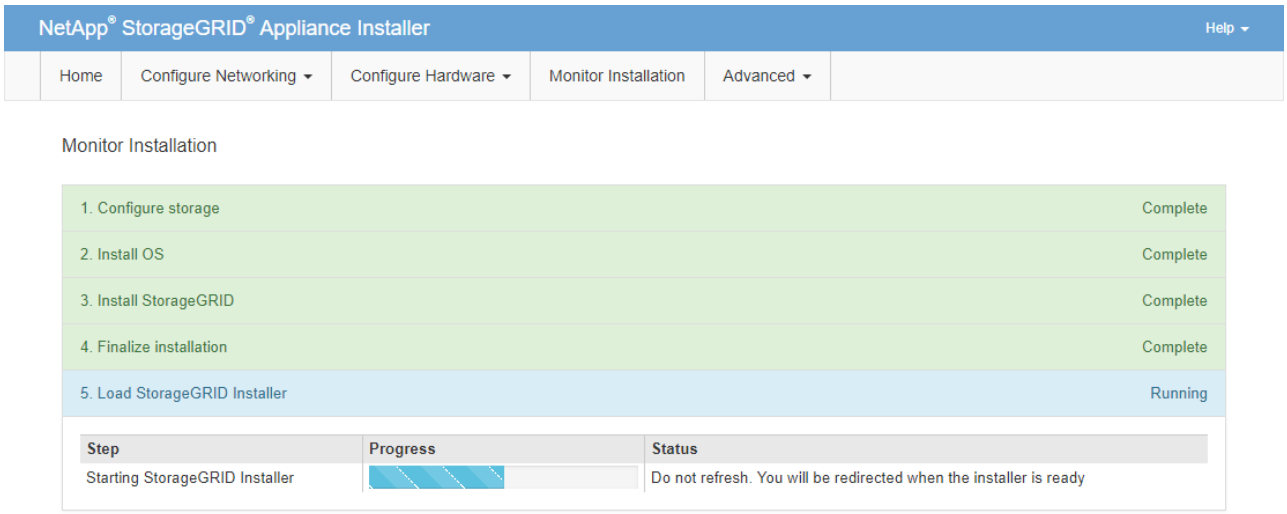
   - **2. Instale o os**

     Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID do nó de administração principal para o dispositivo ou instala o sistema operativo base a partir do pacote de instalação do nó de administração principal.

3. Continue a monitorizar o progresso da instalação até que ocorra uma das seguintes situações:
   - Para nós de Gateway de dispositivo ou nós de administração de dispositivo não-primário, o estágio **Install StorageGRID** é pausado e uma mensagem é exibida no console incorporado, solicitando que você aprove esse nó no nó de administrador usando o Gerenciador de grade.



- 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 um nó de gateway"
Nó de administração não primário	"Selecionando Iniciar recuperação para configurar um nó de administração não primário"
Nó de administração principal	"Configurar o nó de administração principal de substituição"

Como a recuperação do local é realizada pelo suporte técnico

Se um local StorageGRID inteiro falhar ou se vários nós de storage falharem, entre em Contato com o suporte técnico. O suporte técnico avaliará sua situação, desenvolverá um plano de recuperação e recuperará os nós ou o local com falha de uma maneira que atenda aos objetivos de negócios, otimize o tempo de recuperação e evite a perda desnecessária de dados.

A recuperação do local só pode ser realizada por suporte técnico.

Os sistemas StorageGRID são resilientes a uma grande variedade de falhas e você pode executar com sucesso muitos procedimentos de recuperação e manutenção. No entanto, é difícil criar um procedimento simples e generalizado de recuperação do local, porque as etapas detalhadas dependem de fatores específicos para sua situação. Por exemplo:

- **Seus objetivos de negócios**: Após a perda completa de um site da StorageGRID, você deve avaliar a melhor forma de atender aos seus objetivos de negócios. Por exemplo, você deseja reconstruir o site perdido no local? Pretende substituir o site Lost StorageGRID numa nova localização? A situação de cada cliente é diferente, e seu plano de recuperação deve ser projetado para atender às suas prioridades.
- **Natureza exata da falha**: Antes de iniciar uma recuperação do local, é importante estabelecer se algum nó no local com falha está intacto ou se algum nó de armazenamento contém objetos recuperáveis. Se você reconstruir nós ou volumes de storage que contenham dados válidos, poderá ocorrer perda

desnecessária de dados.

- **Ative ILM policy**: O número, tipo e localização das cópias de objetos em sua grade é controlado por sua política ILM ativa. As especificidades da sua política de ILM podem afetar a quantidade de dados recuperáveis, bem como as técnicas específicas necessárias para a recuperação.

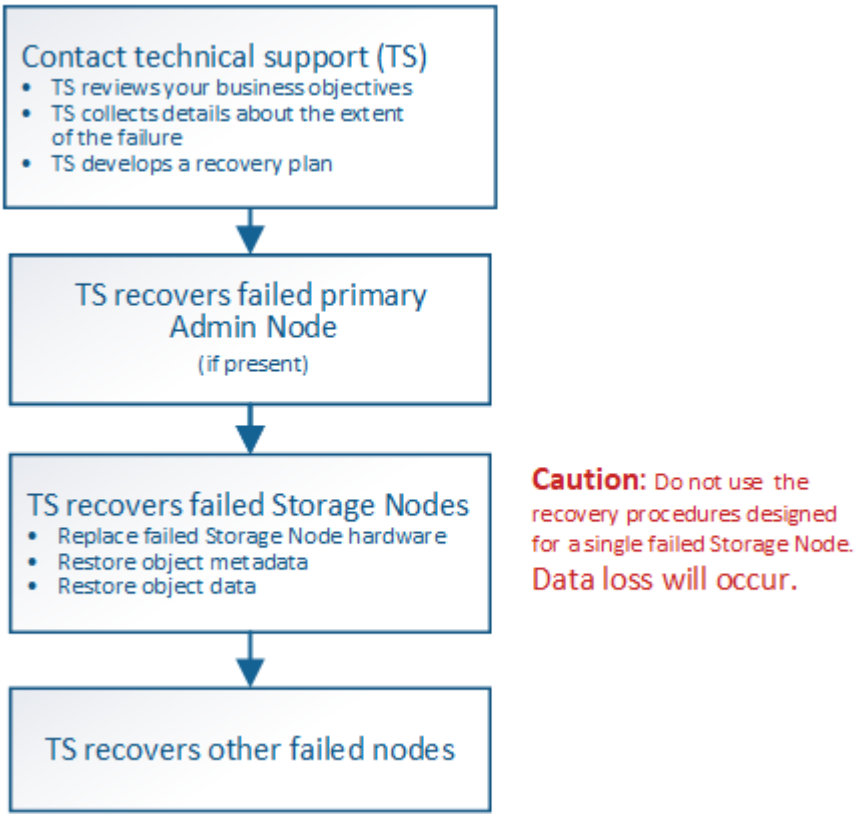
  Se um site contém a única cópia de um objeto e o site é perdido, o objeto é perdido.

- **Consistência de bucket (ou container)**: O nível de consistência aplicado a um bucket (ou container) afeta se o StorageGRID replica totalmente os metadados de objetos para todos os nós e sites antes de informar ao cliente que a ingestão de objetos foi bem-sucedida. Se o seu nível de consistência permitir consistência, alguns metadados de objetos podem ter sido perdidos na falha do site. Isso pode afetar a quantidade de dados recuperáveis e, potencialmente, os detalhes do procedimento de recuperação.
- **Histórico de alterações recentes**: Os detalhes do seu procedimento de recuperação podem ser afetados se algum procedimento de manutenção estava em andamento no momento da falha ou se alguma alteração recente foi feita à sua política de ILM. O suporte técnico deve avaliar o histórico recente de sua grade, bem como sua situação atual antes de iniciar uma recuperação do local.

Visão geral da recuperação do local

Esta é uma visão geral do processo que o suporte técnico usa para recuperar um site com falha.

A recuperação do local só pode ser realizada por suporte técnico.



1. Entre em Contato com o suporte técnico.

   O suporte técnico faz uma avaliação detalhada da falha e trabalha com você para analisar seus objetivos de negócios. Com base nessas informações, o suporte técnico desenvolve um plano de recuperação adaptado à sua situação.

2. O suporte técnico recupera o nó de administração principal se ele tiver falhado.
3. O suporte técnico recupera todos os nós de storage, seguindo este resumo:

   a. Substitua o hardware do nó de armazenamento ou as máquinas virtuais conforme necessário.

   b. Restaurar metadados de objetos para o site com falha.

   c. Restaure os dados do objeto para os nós de storage recuperados.

> A perda de dados ocorrerá se os procedimentos de recuperação para um único nó de armazenamento com falha forem usados.

> Quando um site inteiro falhou, comandos especializados são necessários para restaurar objetos e metadados de objetos com sucesso.

4. O suporte técnico recupera outros nós com falha.

   Depois que os metadados e os dados do objeto tiverem sido recuperados, os nós de Gateway com falha, os nós de administrador não primários ou os nós de arquivo podem ser recuperados usando procedimentos padrão.

Informações relacionadas

"Desativação do local"

Procedimento de desativação

Você pode executar um procedimento de desativação para remover permanentemente nós de grade ou um site inteiro do sistema StorageGRID.

Para remover um nó de grade ou um local, execute um dos seguintes procedimentos de desativação:

- Execute um **node desactivation** para remover um ou mais nós, que podem estar em um ou mais sites. Os nós removidos podem estar online e conetados ao sistema StorageGRID, ou podem estar offline e desconetados.
- Execute um **desativação do site conetado** para remover um site no qual todos os nós estão conetados ao StorageGRID.
- Execute um **Desligamento do local desconetado** para remover um local no qual todos os nós são desconetados do StorageGRID.

> Antes de executar uma desativação do site desconetada, 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.

Se um site contiver uma mistura de nós conetados (✔) e desconetados (⬢ ou ?), você deverá colocar todos os nós offline novamente online.

Informações relacionadas

"Desativação do nó de grade"

"Desativação do local"

Desativação do nó de grade

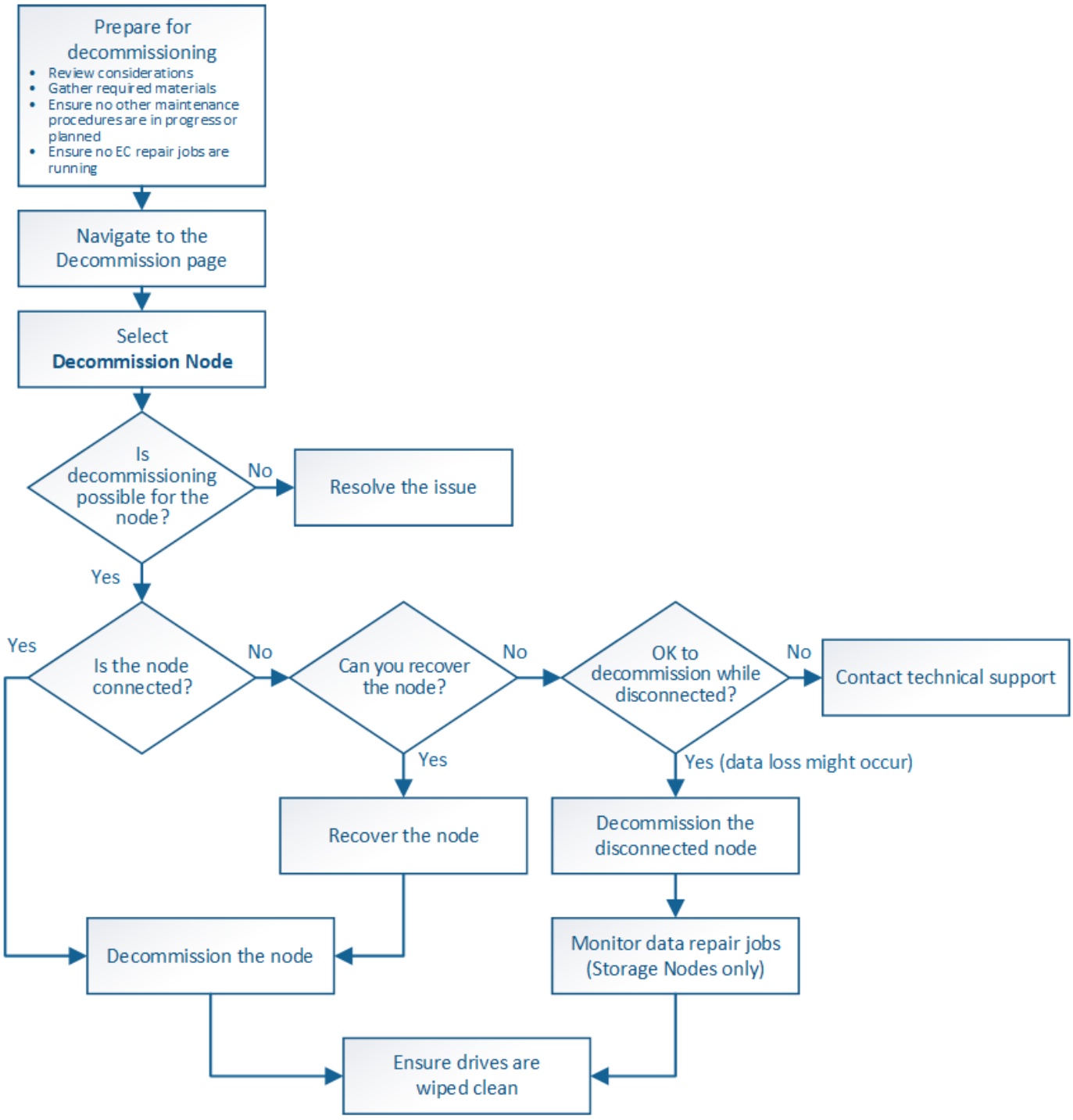
Você pode usar o procedimento de desativação do nó para remover um ou mais nós de storage, nós de gateway ou nós de administração não primários em um ou mais locais. Não é possível desativar o nó de administração principal ou um nó de arquivo.

Em geral, você deve desativar os nós de grade somente enquanto eles estiverem conetados ao sistema StorageGRID e todos os nós estiverem em estado normal (tenha ícones verdes nas páginas **nós** e na página **nós de desintegração**). No entanto, se necessário, você pode desativar um nó de grade que está desconetado. Antes de remover um nó desconetado, certifique-se de entender as implicações e restrições desse processo.

Use o procedimento de desativação do nó quando qualquer uma das seguintes situações for verdadeira:

- Você adicionou um nó de storage maior ao sistema e deseja remover um ou mais nós de storage menores, preservando ao mesmo tempo objetos.
- Você exige menos storage total.
- Você não precisa mais de um nó de gateway.
- Você não precisa mais de um nó de administrador não primário.
- Sua grade inclui um nó desconetado que você não pode recuperar ou trazer de volta on-line.

O fluxograma mostra as etapas de alto nível para a desativação de nós de grade.



Passos

- "Preparando-se para desativar os nós de grade"
- "Recolha de materiais necessários"
- "Acessando a página Decommission Nodes"
- "Desativação de nós de grade desconetados"
- "Desativação de nós de grade conetados"
- "Pausar e retomar o processo de desativação dos nós de storage"
- "Solução de problemas de desativação do nó"

Preparando-se para desativar os nós de grade

Você deve analisar as considerações para remover nós de grade e confirmar que nenhum trabalho de reparo está ativo para dados codificados de apagamento.

Passos

- "Considerações para a desativação de nós de storage"
- "Verificação de trabalhos de reparação de dados"

Considerações para a desativação de nós de grade

Antes de iniciar este procedimento para desativar um ou mais nós, você deve entender as implicações da remoção de cada tipo de nó. Após a desativação bem-sucedida de um nó, seus serviços serão desativados e o nó será desligado automaticamente.

Você não pode desativar um nó se isso deixar o StorageGRID em um estado inválido. As seguintes regras são aplicadas:

- Não é possível desativar o nó de administração principal.
- Não é possível desativar os nós de arquivo.
- Não é possível desativar um nó de administrador ou um nó de gateway se uma de suas interfaces de rede fizer parte de um grupo de alta disponibilidade (HA).
- Não é possível desativar um nó de armazenamento se a sua remoção afetar o quórum de ADC.
- Não é possível desativar um nó de storage se for necessário para a política ILM ativa.
- Você não deve desativar mais de 10 nós de storage em um único procedimento de nó de compactação.
- Não é possível desativar um nó conetado se a grade incluir nenhum nó desconetado (nós cuja integridade é desconhecida ou administrativamente inoperante). Primeiro, você deve desativar ou recuperar os nós desconetados.
- Se sua grade contiver vários nós desconetados, o software exige que você os desative ao mesmo tempo, o que aumenta o potencial de resultados inesperados.
- Se um nó desconetado não puder ser removido (por exemplo, um nó de armazenamento necessário para o quórum de ADC), nenhum outro nó desconetado poderá ser removido.
- Se você quiser substituir um dispositivo mais antigo por um dispositivo mais novo, considere usar o procedimento de clonagem do nó do dispositivo em vez de desativar o nó antigo e adicionar o novo nó em uma expansão.

  "Clonagem do nó do dispositivo"

> Não remova a máquina virtual de um nó de grade ou outros recursos até que seja instruído a fazê-lo em procedimentos de desativação.

Considerações para a desativação de nós de administração ou de um nó de gateway

Reveja as seguintes considerações antes de desativar um nó de administrador ou um nó de gateway.

- O procedimento de desativação requer acesso exclusivo a alguns recursos do sistema, portanto, você

deve confirmar que nenhum outro procedimento de manutenção está sendo executado.

- Não é possível desativar o nó de administração principal.
- Não é possível desativar um nó de administrador ou um nó de gateway se uma de suas interfaces de rede fizer parte de um grupo de alta disponibilidade (HA). Primeiro, é necessário remover as interfaces de rede do grupo HA. Consulte as instruções para administrar o StorageGRID.
- Conforme necessário, você pode alterar com segurança a política de ILM ao desativar um nó de gateway ou um nó de administrador.
- Se você desativar um nó de administrador e o logon único (SSO) estiver ativado para seu sistema StorageGRID, lembre-se de remover a confiança de parte confiável do nó dos Serviços de Federação do ative Directory (AD FS).

Informações relacionadas

"Administrar o StorageGRID"

Considerações para a desativação de nós de storage

Se você pretende desativar um nó de storage, deve entender como o StorageGRID gerencia os dados e os metadados do objeto nesse nó.

As considerações e restrições a seguir se aplicam ao descomissionamento de nós de storage:

- O sistema deve, em todos os momentos, incluir nós de armazenamento suficientes para satisfazer os requisitos operacionais, incluindo o quórum de ADC e a política de ILM ativa. Para satisfazer essa restrição, talvez seja necessário adicionar um novo nó de armazenamento em uma operação de expansão antes de poder desativar um nó de armazenamento existente.
- Se o nó de storage for desconetado ao desativá-lo, o sistema deverá reconstruir os dados usando dados dos nós de storage conetados, o que pode resultar em perda de dados.
- Quando você remove um nó de armazenamento, grandes volumes de dados de objeto devem ser transferidos pela rede. Embora essas transferências não devam afetar as operações normais do sistema, elas podem ter um impactos na quantidade total de largura de banda de rede consumida pelo sistema StorageGRID.
- As tarefas associadas à desativação do nó de storage recebem uma prioridade menor do que as tarefas associadas às operações normais do sistema. Isso significa que a desativação não interfere nas operações normais do sistema StorageGRID e não precisa ser programada para um período de inatividade do sistema. Como a desativação é realizada em segundo plano, é difícil estimar quanto tempo o processo levará para ser concluído. Em geral, a desativação termina mais rapidamente quando o sistema está silencioso ou se apenas um nó de armazenamento está sendo removido de cada vez.
- Pode levar dias ou semanas para desativar um nó de storage. Planeie este procedimento em conformidade. Embora o processo de desativação seja projetado para não impactar as operações do sistema, ele pode limitar outros procedimentos. Em geral, você deve executar quaisquer atualizações ou expansões planeadas do sistema antes de remover nós de grade.
- Os procedimentos de desativação que envolvem nós de storage podem ser pausados durante determinados estágios para permitir que outros procedimentos de manutenção sejam executados, se necessário, e retomados assim que forem concluídos.
- Não é possível executar operações de reparo de dados em nenhum nó de grade quando uma tarefa de desativação está em execução.
- Você não deve fazer alterações na política de ILM enquanto um nó de storage estiver sendo desativado.
- Quando você remove um nó de storage, os dados no nó são migrados para outros nós de grade; no

entanto, esses dados não são completamente removidos do nó de grade desativado. Para remover dados de forma permanente e segura, você deve limpar as unidades do nó de grade desativado após o procedimento de desativação ser concluído.

- Quando você desativa um nó de armazenamento, os seguintes alertas e alarmes podem ser enviados e você pode receber notificações de e-mail e SNMP relacionadas:
  - **Não é possível se comunicar com o alerta node**. Esse alerta é acionado quando você desativa um nó de armazenamento que inclui o serviço ADC. O alerta é resolvido quando a operação de desativação é concluída.
  - Alarme VSTU (Estado da verificação do objeto). Este alarme de nível de aviso indica que o nó de armazenamento está a entrar no modo de manutenção durante o processo de desativação.
  - Alarme CASA (Data Store Status). Esse alarme de nível principal indica que o banco de dados Cassandra está caindo porque os serviços pararam.

Informações relacionadas

"Restaurar dados de objetos para um volume de armazenamento, se necessário"

"Entendendo o quórum de ADC"

"Rever a política de ILM e a configuração de armazenamento"

"Desativação de nós de storage desconetados"

"Consolidação de nós de storage"

"Desativação de vários nós de storage"

Entendendo o quórum de ADC

Talvez você não consiga desativar certos nós de armazenamento em um local de data center se muito poucos serviços do controlador de domínio administrativo (ADC) permanecessem após a desativação. Esse serviço, que é encontrado em alguns nós de storage, mantém informações de topologia de grade e fornece serviços de configuração para a grade. O sistema StorageGRID requer que um quórum de serviços ADC esteja disponível em cada local e em todos os momentos.

Não é possível desativar um nó de armazenamento se a remoção do nó fizer com que o quórum de ADC deixe de ser atendido. Para satisfazer o quórum de ADC durante a desativação, um mínimo de três nós de armazenamento em cada local de data center deve ter o serviço ADC. Se um local de data center tiver mais de três nós de storage com o serviço ADC, uma maioria simples desses nós deve permanecer disponível após a desativação ((0,5 * `Storage Nodes with ADC`) e 1).

Por exemplo, suponha que um site de data center inclua atualmente seis nós de storage com serviços ADC e que você queira desativar três nós de storage. Devido ao requisito de quórum do ADC, você deve concluir dois procedimentos de desativação, como segue:

- No primeiro procedimento de desativação, você deve garantir que quatro nós de armazenamento com serviços ADC permaneçam disponíveis ((0,5 * 6) -1) . Isso significa que você só pode desativar dois nós de storage inicialmente.
- No segundo procedimento de desativação, você pode remover o terceiro nó de armazenamento porque o quórum de ADC agora requer apenas três serviços ADC para permanecer disponível ((0,5 * 4) e 1).

Se você precisar desativar um nó de armazenamento, mas não puder devido ao requisito de quórum de ADC, você deve adicionar um novo nó de armazenamento em uma expansão e especificar que ele deve ter um serviço ADC. Em seguida, você pode desativar o nó de storage existente.

Informações relacionadas

"Expanda sua grade"

Rever a política de ILM e a configuração de armazenamento

Se você planeja desativar um nó de storage, deve revisar a política de ILM do sistema StorageGRID antes de iniciar o processo de desativação.

Durante a desativação, todos os dados de objetos são migrados do nó de storage desativado para outros nós de storage.

> A política ILM que você tem *durante* a desativação será a usada *após* a desativação. Você deve garantir que essa política atenda aos requisitos de dados antes de iniciar a desativação e após a conclusão da desativação.

Deve rever as regras da política ILM ativa para garantir que o sistema StorageGRID continuará a ter capacidade suficiente do tipo correto e nos locais corretos para acomodar a desativação de um nó de armazenamento.

Considere o seguinte:

- Será possível que os serviços de avaliação ILM copiem dados de objetos de modo que as regras ILM sejam satisfeitas?
- O que acontece se um site ficar temporariamente indisponível enquanto a desativação estiver em andamento? Cópias adicionais podem ser feitas em um local alternativo?
- Como o processo de desativação afetará a distribuição final do conteúdo? Conforme descrito em ""consolidando nós de storage"", você deve adicionar novos nós de storage antes de desativar os antigos. Se você adicionar um nó de storage de substituição maior após a desativação de um nó de storage menor, os nós de storage antigos poderão estar próximos da capacidade e o novo nó de storage quase não terá conteúdo. A maioria das operações de gravação para novos dados de objetos seria direcionada para o novo nó de storage, reduzindo a eficiência geral das operações do sistema.
- O sistema incluirá, em todos os momentos, nós de storage suficientes para satisfazer a política de ILM ativa?

> Uma política de ILM que não pode ser satisfeita levará a backlogs e alarmes e pode interromper a operação do sistema StorageGRID.

Verifique se a topologia proposta que resultará do processo de desativação satisfaz a política de ILM, avaliando os fatores listados na tabela.

Área a avaliar	Notas
Capacidade disponível	Haverá capacidade de armazenamento suficiente para acomodar todos os dados de objetos armazenados no sistema StorageGRID, incluindo as cópias permanentes de dados de objetos atualmente armazenados no nó de armazenamento para serem desativados?haverá capacidade suficiente para lidar com o crescimento esperado de dados de objetos armazenados por um intervalo de tempo razoável após a conclusão da desativação?
Localização do armazenamento	Se ainda houver capacidade suficiente no sistema StorageGRID como um todo, a capacidade nos locais certos está em conformidade com as regras de negócios do sistema StorageGRID?
Tipo de armazenamento	Haverá armazenamento suficiente do tipo apropriado após a conclusão da desativação? Por exemplo, as regras do ILM podem ditar que o conteúdo seja movido de um tipo de armazenamento para outro à medida que o conteúdo envelhece. Nesse caso, você deve garantir que o armazenamento suficiente do tipo apropriado esteja disponível na configuração final do sistema StorageGRID.

Informações relacionadas

"Consolidação de nós de storage"

"Gerenciar objetos com ILM"

"Expanda sua grade"

Desativação de nós de storage desconetados

Você deve entender o que pode acontecer se você desativar um nó de armazenamento enquanto ele estiver desconetado (integridade é desconhecido ou administrativamente inativo).

Quando você desativa um nó de storage desconetado da grade, o StorageGRID usa dados de outros nós de storage para reconstruir os dados do objeto e os metadados que estavam no nó desconetado. Ele faz isso iniciando automaticamente os trabalhos de reparo de dados no final do processo de desativação.

Antes de desativar um nó de storage desconetado, esteja ciente do seguinte:

- Você nunca deve desativar um nó desconetado, a menos que tenha certeza de que ele não pode ser colocado on-line ou recuperado.

> Não execute este procedimento se você acredita que pode ser possível recuperar dados de objeto do nó. Em vez disso, entre em Contato com o suporte técnico para determinar se a recuperação do nó é possível.

- Se um nó de armazenamento desconetado contiver a única cópia de um objeto, esse objeto será perdido quando você desativar o nó. As tarefas de reparo de dados só podem reconstruir e recuperar objetos se houver pelo menos uma cópia replicada ou fragmentos codificados de apagamento suficientes nos nós de storage que estão atualmente conetados.

- Quando você desativa um nó de storage desconetado, o procedimento de desativação é concluído com relativa rapidez. No entanto, os trabalhos de reparação de dados podem demorar dias ou semanas a ser executados e não são monitorizados pelo procedimento de desativação. Você deve monitorar manualmente esses trabalhos e reiniciá-los conforme necessário. Consulte as instruções sobre a reparação de dados de monitorização.

  "Verificação de trabalhos de reparação de dados"

- Se você desativar mais de um nó de storage desconetado de cada vez, poderá ocorrer perda de dados. O sistema pode não conseguir reconstruir dados se houver poucas cópias de dados de objetos, metadados ou fragmentos codificados por apagamento permanecerem disponíveis.

  Se você tiver mais de um nó de armazenamento desconetado que não possa recuperar, entre em Contato com o suporte técnico para determinar o melhor curso de ação.

Consolidação de nós de storage

Você pode consolidar os nós de storage para reduzir a contagem de nós de storage para um local ou implantação, aumentando a capacidade de storage.

Ao consolidar os nós de storage, você expande o sistema StorageGRID para adicionar nós de storage de capacidade novos e maiores e, em seguida, desativar os nós de storage de capacidade antigos e menores. Durante o procedimento de desativação, os objetos são migrados dos nós de armazenamento antigos para os novos nós de armazenamento.

Por exemplo, você pode adicionar dois nós de storage de capacidade novos e maiores para substituir três nós de storage mais antigos. Primeiro, você usaria o procedimento de expansão para adicionar os dois nós de storage novos e maiores e, em seguida, usaria o procedimento de desativação para remover os três nós de storage de capacidade antigos e menores.

Ao adicionar nova capacidade antes de remover nós de storage existentes, você garante uma distribuição mais equilibrada dos dados pelo sistema StorageGRID. Você também reduz a possibilidade de que um nó de armazenamento existente possa ser empurrado para além do nível de marca d'água de armazenamento.

Informações relacionadas

"Expanda sua grade"

Desativação de vários nós de storage

Se você precisar remover mais de um nó de storage, poderá desativá-los sequencialmente ou em paralelo.

- Se você desativar os nós de storage sequencialmente, deverá aguardar que o primeiro nó de storage conclua a desativação antes de começar a desativar o próximo nó de storage.
- Se você desativar os nós de storage em paralelo, os nós de storage processarão simultaneamente as tarefas de desativação de todos os nós de storage que estão sendo desativados. Isso pode resultar em uma situação em que todas as cópias permanentes de um arquivo são marcadas como "somente reativas", desativando temporariamente a exclusão em grades onde essa funcionalidade está ativada.

Verificação de trabalhos de reparação de dados

Antes de desativar um nó de grade, você deve confirmar que nenhum trabalho de reparo

de dados está ativo. Se alguma reparação tiver falhado, tem de as reiniciar e permitir que sejam concluídas antes de executar o procedimento de desativação.

Se precisar desativar um nó de armazenamento desconetado, você também concluirá estes passos após a conclusão do procedimento de desativação para garantir que o trabalho de reparo de dados foi concluído com êxito. Você deve garantir que todos os fragmentos codificados de apagamento que estavam no nó removido foram restaurados com sucesso.

Essas etapas se aplicam somente a sistemas que tenham objetos codificados por apagamento.

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

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

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Verifique se existem reparações em curso: `repair-data show-ec-repair-status`
   - Se nunca tiver executado um trabalho de reparação de dados, a saída é `No job found`. Não é necessário reiniciar quaisquer trabalhos de reparação.
   - Se o trabalho de reparação de dados tiver sido executado anteriormente ou estiver em execução atualmente, a saída lista as informações para a reparação. Cada reparação tem um ID de reparação exclusivo. Vá para a próxima etapa.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
================================================================================
===========
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. Se o Estado para todas as reparações for `Success`, não é necessário reiniciar quaisquer trabalhos de reparação.
4. Se o estado de qualquer reparação for `Failure`, tem de reiniciar a reparação.
   a. Obtenha a ID de reparação para a reparação com falha a partir da saída.
   b. Executar o `repair-data start-ec-node-repair` comando.

Utilize a `--repair-id` opção para especificar a ID de reparação. Por exemplo, se você quiser tentar novamente um reparo com a ID de reparo 949292, execute este comando: `repair-data start-ec-node-repair --repair-id 949292`

c. Continuar a acompanhar o estado das reparações de dados CE até que o Estado para todas as reparações seja `Success`de .

Recolha de 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 transferir o ficheiro de pacote de recuperação mais recente `.zip`(`sgws-recovery-package-`*`id-revision`*`.zip`). Você pode usar o arquivo Pacote de recuperação para restaurar o sistema se ocorrer uma falha.
`Passwords.txt` ficheiro	Este arquivo contém as senhas necessárias para acessar os nós de grade na linha de comando e está incluído no Pacote de recuperação.
Frase-passe do 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"

"Transferir o pacote de recuperação"

Acessando a página Decommission Nodes

Quando você acessa a página Decommission Nodes no Grid Manager, você pode ver rapidamente quais nós podem ser desativados.

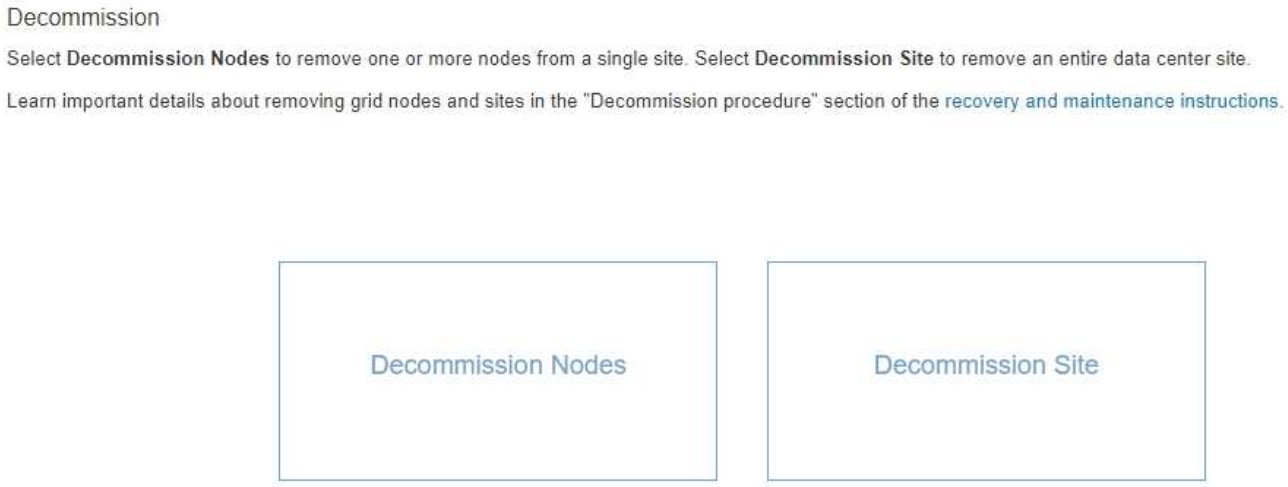
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.

Passos

1. Selecione **Manutenção** > **tarefas de Manutenção** > **Desmontagem**.

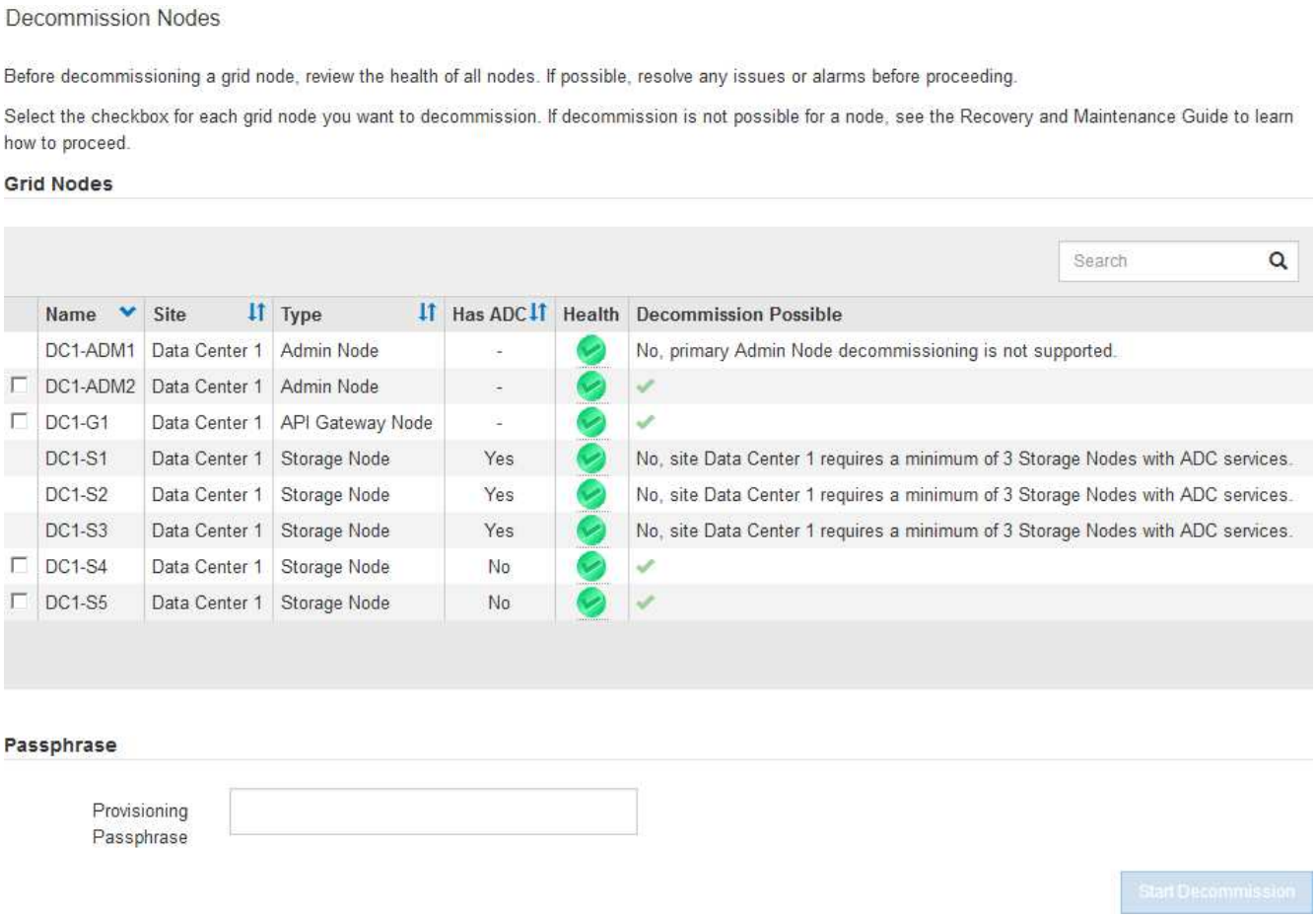
   A página Decommission é exibida.



2. Clique no botão **Decommission Nodes**.

   A página Decommission Nodes (nós de desintegração) é exibida. Nesta página, você pode:

   - Determine quais nós de grade podem ser desativados atualmente.
   - Veja a integridade de todos os nós de grade
   - Classifique a lista em ordem crescente ou decrescente por **Nome**, **Site**, **tipo** ou **ADC**.
   - Insira termos de pesquisa para encontrar rapidamente nós específicos. Por exemplo, esta página mostra todos os nós de grade em um único data center. A coluna Decmmission possible indica que você pode desativar o nó de administração não primário, o nó de gateway e dois dos cinco nós de storage.



3. Revise a coluna **Decommission possible** para cada nó que você deseja desativar.

   Se um nó de grade pode ser desativado, essa coluna inclui uma marca de seleção verde e a coluna mais à esquerda inclui uma caixa de seleção. Se um nó não puder ser desativado, essa coluna descreve o problema. Se houver mais de um motivo pelo qual um nó não pode ser desativado, o motivo mais crítico será exibido.

Desativar possível motivo	Descrição	Passos para resolver
Não, a desativação do tipo de nó não é suportada.	Não é possível desativar o nó de administração principal ou um nó de arquivo.	Nenhum.

Desativar possível motivo	Descrição	Passos para resolver
Não, pelo menos um nó de grade está desconetado. **Nota:** esta mensagem é mostrada apenas para nós de grade conetados.	Você não pode 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	Vá para etapa que lista as opções de procedimento de desativação.
Não, um ou mais nós necessários estão atualmente desconetados e devem ser recuperados. **Nota:** esta mensagem é mostrada apenas para nós de grade desconetados.	Você não pode desativar um nó de grade desconetado se um ou mais nós necessários também forem desconetados (por exemplo, um nó de armazenamento que é necessário para o quórum de ADC).	a. Reveja as mensagens possíveis de desintegração para todos os nós desconetados. b. Determine quais nós não podem ser desativados porque 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: *X*. 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. Consulte as instruções para administrar o StorageGRID.
Não, o local *x* requer um mínimo de *n* nós de armazenamento com serviços ADC.	**Somente nós de storage.** Você não pode desativar um nó de storage se nós insuficientes permanecessem no local para oferecer suporte aos requisitos de quórum de ADC.	Execute uma expansão. Adicione um novo nó de armazenamento ao site e especifique que ele deve ter um serviço ADC. Consulte informações sobre o quórum ADC.

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.** Você não pode 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 de apagamento para 4 codificação de apagamento a mais de 2 anos, pelo menos 6 nós de storage devem permanecer.	Para cada perfil de codificação de apagamento afetado, execute uma das seguintes etapas, com base em como o perfil está sendo usado: • **Usado na política ILM ativa**: Execute uma expansão. Adicione nós de storage novos suficientes para permitir que a codificação de apagamento continue. Consulte as instruções para expandir o StorageGRID. • **Usado em uma regra ILM, mas não na política ILM ativa**: Edite ou exclua a regra e desative o perfil de codificação de apagamento. • **Não usado em nenhuma regra ILM**: Desative o perfil de codificação de apagamento. **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 sobre como desativar um perfil de codificação de apagamento nas instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

4. se a desativação for possível para o nó, determine qual procedimento você precisa executar:

Se sua grade inclui…	Ir para…
Quaisquer nós de grade desconetados	"Desativação de nós de grade desconetados"
Somente nós de grade conetados	"Desativação de nós de grade conetados"

Informações relacionadas

"Verificação de trabalhos de reparação de dados"

"Entendendo o quórum de ADC"

"Gerenciar objetos com ILM"

"Expanda sua grade"

"Administrar o StorageGRID"

Talvez seja necessário desativar um nó que não esteja conetado à grade no momento (aquele cuja Saúde é desconhecida ou administrativamente inativa).

O que você vai precisar

- Você entende os requisitos e considerações para a desativação de nós de grade.

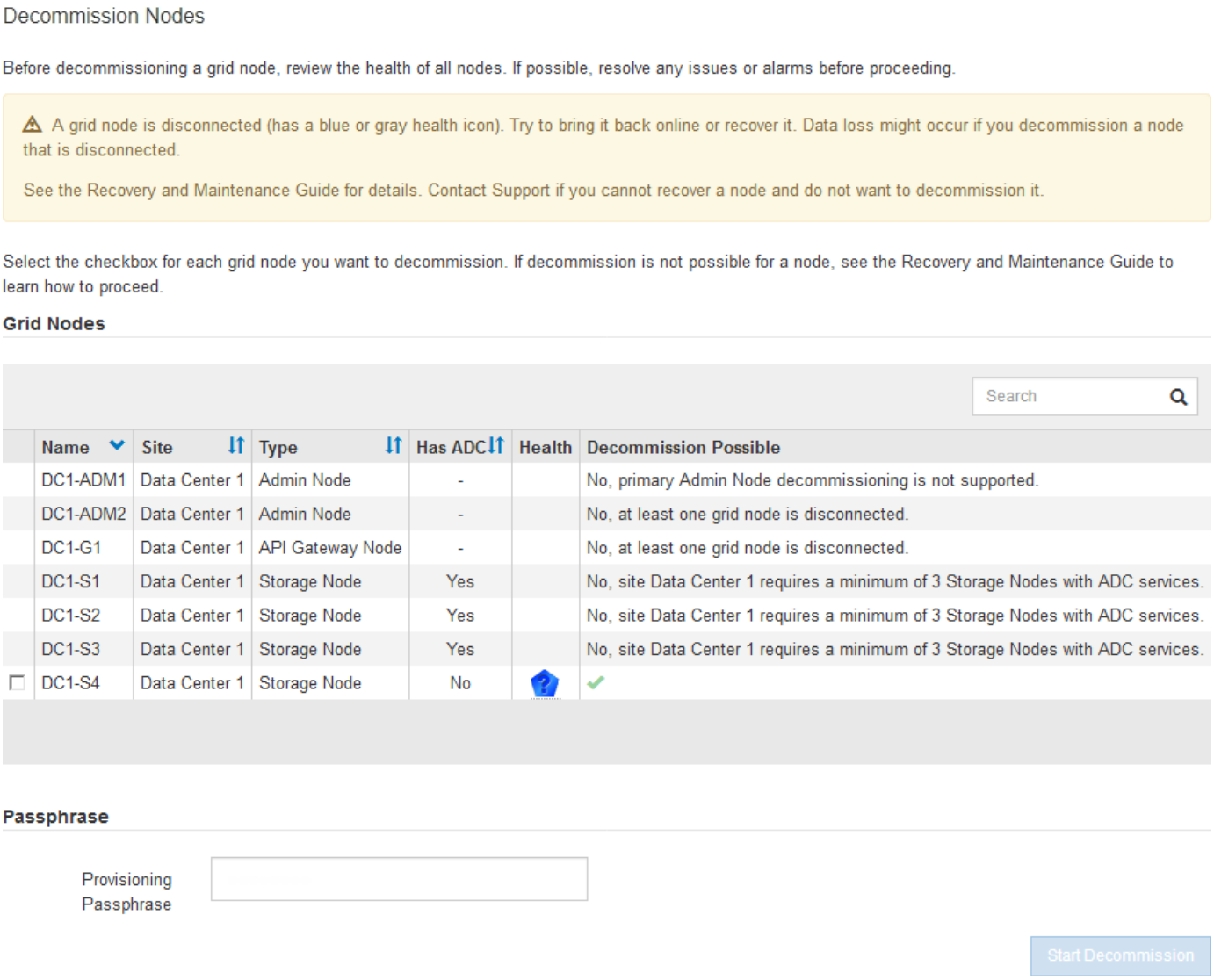
  "Considerações para a desativação de nós de grade"

- Você obteve todos os itens pré-requisitos.
- Você garantiu que nenhum trabalho de reparo de dados está ativo.

  "Verificação de trabalhos de reparação de dados"

- Você confirmou que a recuperação do nó de storage não está em andamento em nenhum lugar da grade. Se estiver, você deve esperar até que qualquer reconstrução do Cassandra executada como parte da recuperação esteja concluída. Você pode então prosseguir com a desativação.
- Você garantiu que outros procedimentos de manutenção não serão executados enquanto o procedimento de desativação do nó estiver em execução, a menos que o procedimento de desativação do nó esteja pausado.
- A coluna **Decommission possible** para o nó ou nós desconetados que você deseja desativar inclui uma marca de seleção verde.
- Você deve ter a senha de provisionamento.

Você pode identificar nós desconetados procurando por ícones desconhecidos (azul) ou administrativamente para baixo (cinza) na coluna **Saúde**. No exemplo, o nó de storage chamado DC1-S4 é desconetado; todos os outros nós estão conetados.



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 ao mesmo tempo, o que aumenta o potencial de resultados inesperados.

> Tenha muito cuidado ao desativar mais de um nó de grade desconetado de cada vez, especialmente se você estiver selecionando vários nós de storage desconetados.

- Se um nó desconetado não puder ser removido (por exemplo, um nó de armazenamento necessário para o quórum de ADC), nenhum outro nó desconetado poderá ser removido.

Antes de desativar um **nó de armazenamento** desconetado, observe o seguinte

- Você nunca deve desativar um nó de armazenamento desconetado, a menos que tenha certeza de que ele não pode ser colocado on-line ou recuperado.

> Se você acredita que os dados do objeto ainda podem ser recuperados do nó, não execute este procedimento. Em vez disso, entre em Contato com o suporte técnico para determinar se a recuperação do nó é possível.

- Se você desativar mais de um nó de storage desconetado, poderá ocorrer perda de dados. O sistema pode não ser capaz de reconstruir dados se não houver cópias suficientes de objetos, fragmentos codificados para apagamento ou metadados de objetos permanecerem disponíveis.

  > Se você tiver mais de um nó de armazenamento desconetado que não possa recuperar, entre em Contato com o suporte técnico para determinar o melhor curso de ação.

- Quando você desativa um nó de storage desconetado, o StorageGRID inicia os trabalhos de reparo de dados no final do processo de desativação. Essas tarefas tentam reconstruir os dados do objeto e os metadados armazenados no nó desconetado.
- Quando você desativa um nó de storage desconetado, o procedimento de desativação é concluído com relativa rapidez. No entanto, os trabalhos de reparação de dados podem demorar dias ou semanas a ser executados e não são monitorizados pelo procedimento de desativação. Você deve monitorar manualmente esses trabalhos e reiniciá-los conforme necessário. Consulte as instruções sobre a reparação de dados de monitorização.

  "Verificação de trabalhos de reparação de dados"

- 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.

Antes de desativar um **Admin Node** ou **Gateway Node** desconetado, observe o seguinte:

- Ao desativar um nó Admin desconetado, você perderá os logs de auditoria desse nó; no entanto, esses logs também devem existir no nó Admin principal.
- Você pode desativar um Gateway Node com segurança enquanto ele estiver desconetado.

Passos

1. Tente colocar todos os nós de grade desconetados novamente on-line ou recuperá-los.

   Consulte os procedimentos de recuperação para obter instruções.

2. Se você não conseguir recuperar um nó de grade desconetado e quiser desativá-lo enquanto ele estiver desconetado, marque a caixa de seleção desse nó.

   > Se sua grade contiver vários nós desconetados, o software exige que você os desative ao mesmo tempo, o que aumenta o potencial de resultados inesperados.

   > Tenha muito cuidado ao selecionar 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.

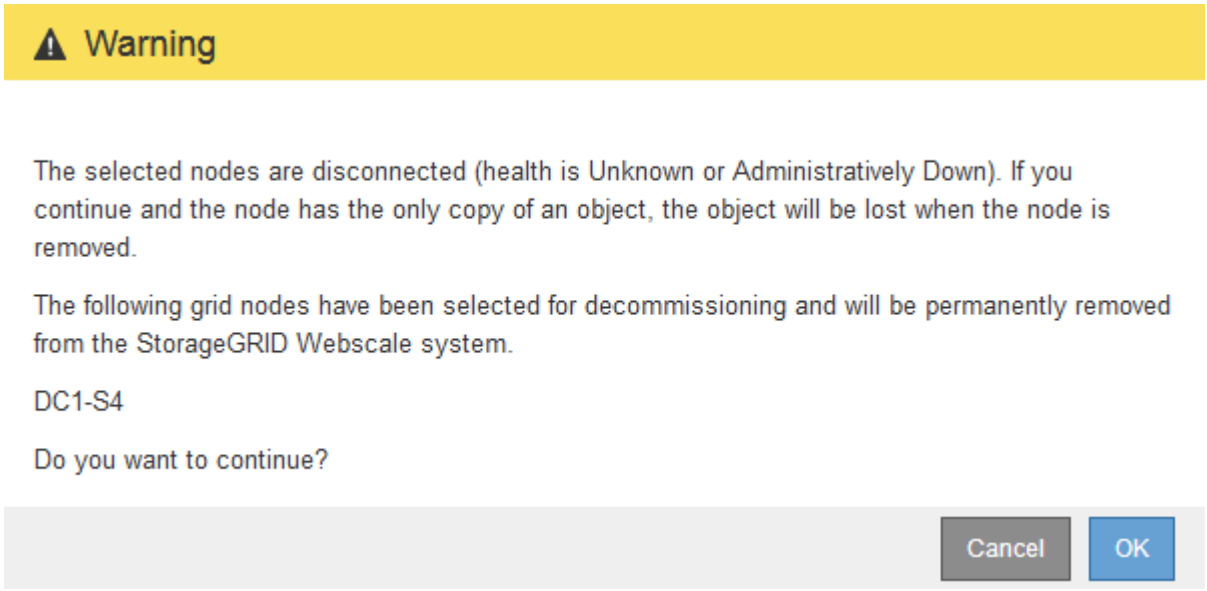
3. Introduza a frase-passe de aprovisionamento.

   O botão **Start Decommission** está ativado.

4. Clique em **Start Decommission**.

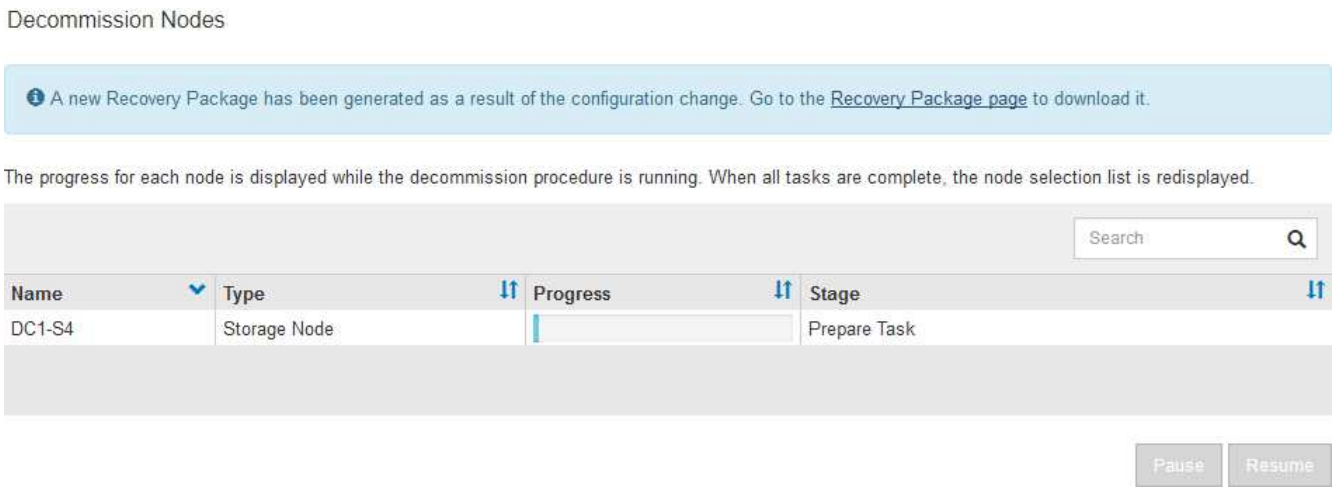
   Um aviso é exibido, indicando que você selecionou um nó desconetado e que os dados do objeto serão

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 **Manutenção sistema Pacote de recuperação** para acessar a página Pacote de recuperação. Em seguida, baixe o `.zip` arquivo.

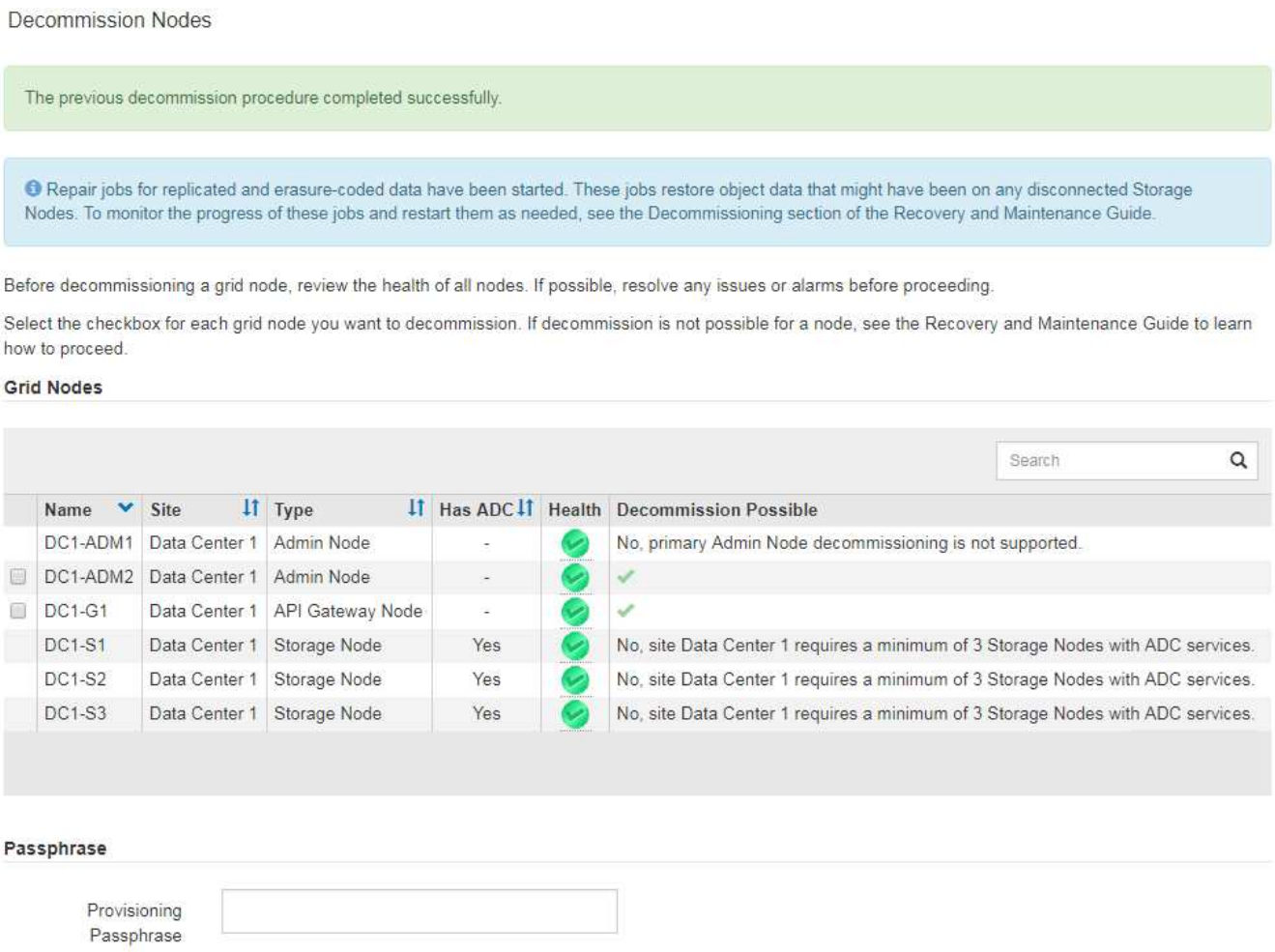
   Consulte as instruções para baixar o pacote de recuperação.

   > 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 estiver a desativar um nó de armazenamento, monitorize o estado dos trabalhos de reparação de dados que são iniciados automaticamente durante o processo de desativação.
   a. Selecione **Support** > **Tools** > **Grid Topology**.
   b. Selecione **StorageGRID deployment** no topo da árvore de topologia de Grade.
   c. Na guia Visão geral, localize a seção atividade ILM.
   d. 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.

e. Use os seguintes comandos para rastrear ou reiniciar reparos:

   - Use o `repair-data show-ec-repair-status` comando para rastrear reparos de dados codificados de apagamento.
   - Use o `repair-data start-ec-node-repair` comando com a `--repair-id` opção para reiniciar um reparo com falha. Consulte as instruções para verificar os trabalhos de reparação de dados.

10. Continue a monitorizar o estado das reparações de dados CE até que todos os trabalhos de reparação tenham sido concluídos com êxito.

    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.

Siga estas etapas depois de concluir o procedimento de desativação:

- Certifique-se de que as unidades do nó de grade desativado estão limpas. Utilize uma ferramenta ou serviço de limpeza de dados disponíveis no mercado para remover dados das unidades de forma permanente e segura.
- Se você desativou um nó de dispositivo e os dados no dispositivo foram protegidos usando criptografia de nó, use o Instalador de dispositivos StorageGRID para limpar a configuração do servidor de gerenciamento de chaves (limpar KMS). Você deve limpar a configuração do KMS se quiser adicionar o dispositivo a outra grade.

  "Aparelhos de serviços SG100 SG1000"

  "SG5600 dispositivos de armazenamento"

  "SG5700 dispositivos de armazenamento"

  "SG6000 dispositivos de armazenamento"

Informações relacionadas

"Procedimentos de recuperação do nó de grade"

"Transferir o pacote de recuperação"

"Verificação de trabalhos de reparação de dados"

Desativação de nós de grade conetados

Você pode desativar e remover permanentemente nós que estão conetados à grade.

O que você vai precisar

- Você entende os requisitos e considerações para a desativação de nós de grade.

  "Considerações para a desativação de nós de grade"

- 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, 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.
- 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.
- 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. Consulte as instruções para verificar os trabalhos de reparação de dados.

> Não remova a máquina virtual de um nó de grade ou outros recursos até que seja instruído a fazê-lo neste procedimento.

Passos

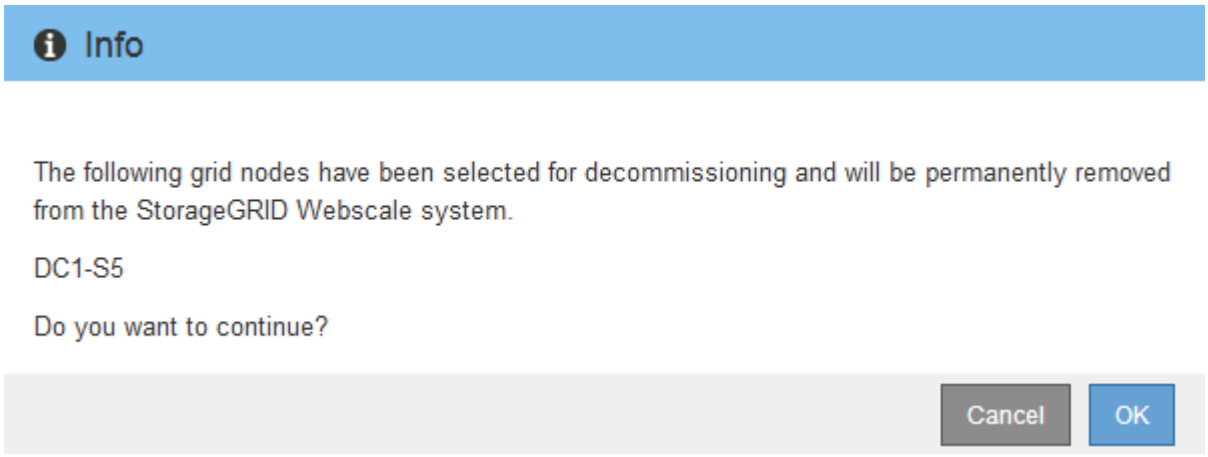
1. Na página Decommission Nodes, marque a caixa de seleção para cada nó de grade que deseja desativar.

2. Introduza a frase-passe de aprovisionamento.

   O botão **Start Decommission** está ativado.

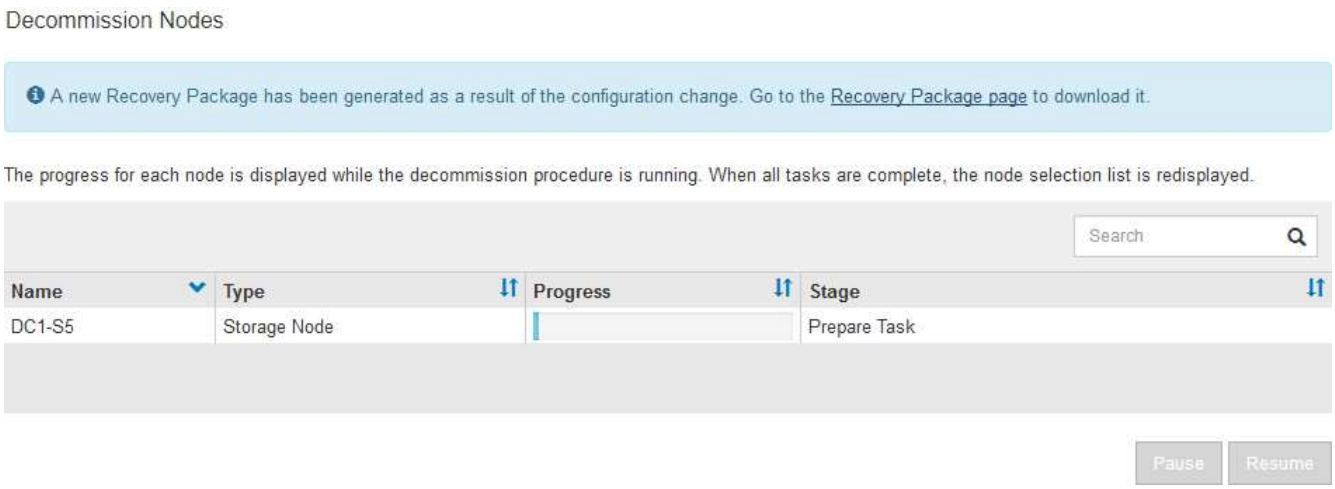
3. Clique em **Start Decommission**.

   É apresentada uma caixa de diálogo de confirmação.



4. Revise a lista de nós selecionados e clique em **OK**.

   O procedimento de desativação do nó é iniciado e o progresso é exibido para cada nó. Durante o procedimento, um novo pacote de recuperação é gerado para mostrar a alteração da configuração da grade.



> Não coloque um nó de armazenamento offline após o início do procedimento de desativação. Alterar o estado pode resultar em algum conteúdo não ser copiado para outros locais.

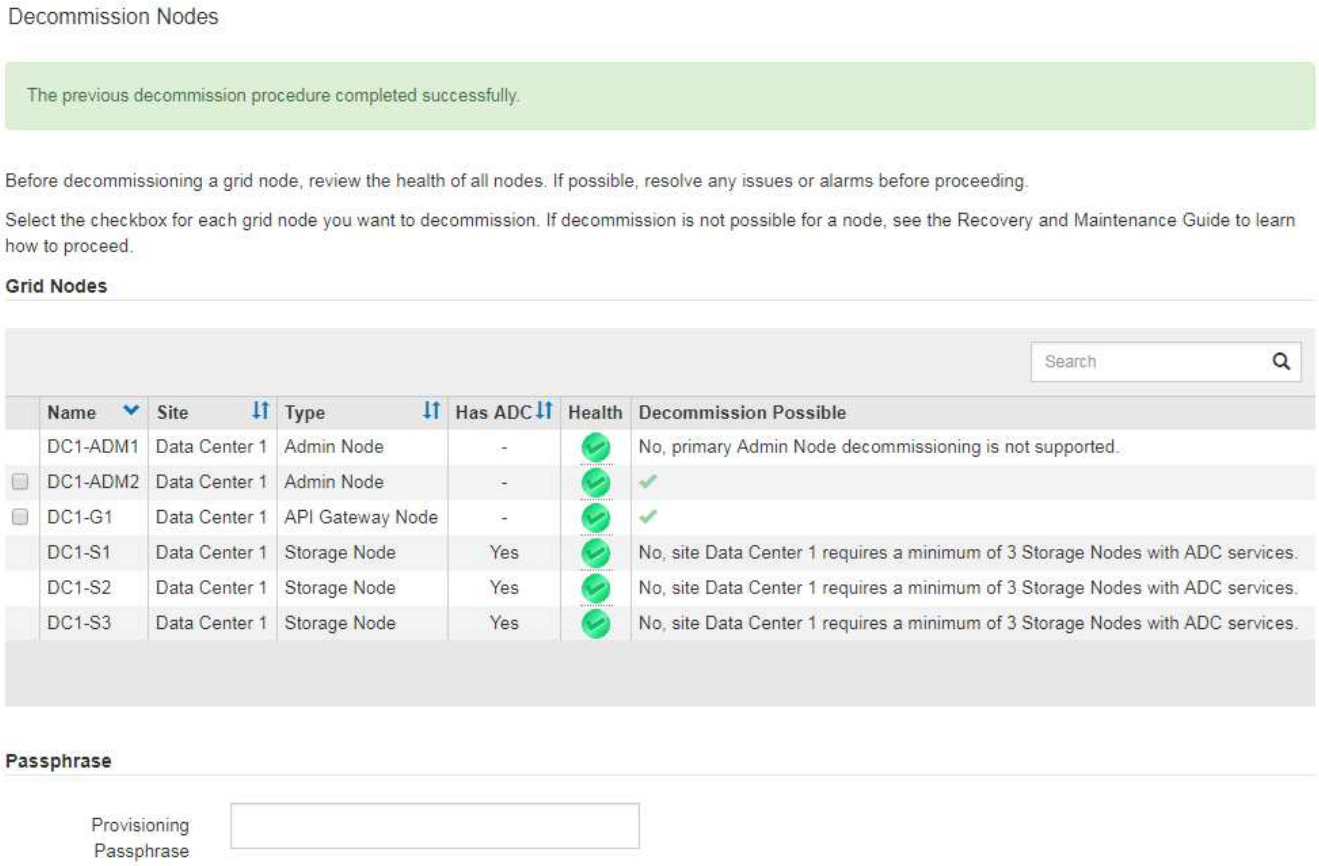
5. Assim que o novo Pacote de recuperação estiver disponível, clique no link ou selecione **Manutenção sistema Pacote de recuperação** para acessar a página Pacote de recuperação. Em seguida, baixe o `.zip` arquivo.

   Consulte as instruções para baixar o pacote de recuperação.

Baixe o pacote de recuperação o mais rápido possível para garantir que você possa recuperar sua grade se algo der errado durante o procedimento de desativação.

6. Monitore periodicamente a página Decommission Nodes para garantir que todos os nós selecionados sejam desativados com êxito.

   Os nós de storage podem levar dias ou semanas para serem desativados. Quando todas as tarefas estiverem concluídas, a lista de seleção de nós é reexibida com uma mensagem de sucesso.



7. Siga o passo apropriado para a sua plataforma. Por exemplo:
   - * Linux*: Você pode querer desanexar os volumes e excluir os arquivos de configuração de nó criados durante a instalação.
   - **VMware**: Você pode querer usar a opção "Excluir do disco" do vCenter para excluir a máquina virtual. Você também pode precisar excluir quaisquer discos de dados que sejam independentes da máquina virtual.
   - **StorageGRID Appliance**: O nó appliance reverte automaticamente para um estado não implantado, onde você pode acessar o Instalador de dispositivos StorageGRID. Pode desligar o aparelho ou adicioná-lo a outro sistema StorageGRID.

Siga estas etapas depois de concluir o procedimento de desativação do nó:

- Certifique-se de que as unidades do nó de grade desativado estão limpas. Utilize uma ferramenta ou serviço de limpeza de dados disponíveis no mercado para remover dados das unidades de forma permanente e segura.
- Se você desativou um nó de dispositivo e os dados no dispositivo foram protegidos usando criptografia de nó, use o Instalador de dispositivos StorageGRID para limpar a configuração do servidor de

gerenciamento de chaves (limpar KMS). Você deve limpar a configuração do KMS se quiser usar o dispositivo em outra grade.

"Aparelhos de serviços SG100 SG1000"

"SG5600 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG6000 dispositivos de armazenamento"

Informações relacionadas

"Verificação de trabalhos de reparação de dados"

"Transferir o pacote de recuperação"

"Instale o Red Hat Enterprise Linux ou CentOS"

Pausar e retomar o processo de desativação dos nós de storage

Se necessário, você pode pausar o procedimento de desativação de um nó de armazenamento durante determinados estágios. Você deve pausar a desativação em um nó de storage antes de iniciar um segundo procedimento de manutenção. Depois que o outro procedimento for concluído, você pode retomar a desativação.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.

Passos

1. Selecione **Manutenção** > **tarefas de Manutenção** > **Desmontagem**.

   A página Decommission é exibida.

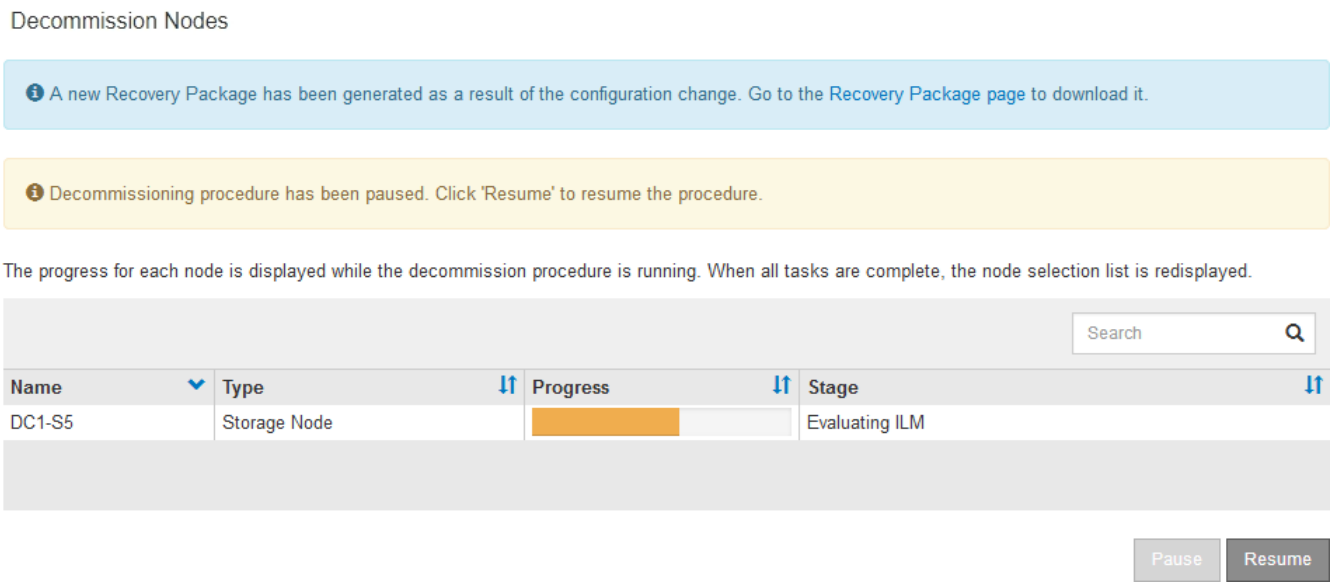
2. Clique em **Decommission Nodes**.

   A página Decommission Nodes (nós de desintegração) é exibida. Quando o procedimento de desativação atinge uma das seguintes etapas, o botão **Pausa** é ativado.

   - Avaliando o ILM
   - Desativação de dados codificados de apagamento

3. Clique em **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, clique em **Resume** para prosseguir com a desativação.

Solução de problemas de desativação do nó

Se o procedimento de desativação do nó parar por causa de um erro, você pode executar etapas específicas para solucionar o problema.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Se você desligar o nó da grade sendo desativado, a tarefa será interrompida até que o nó da grade seja reiniciado. O nó da grade deve estar online.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Na árvore Grid Topology, expanda cada entrada Storage Node e verifique se os serviços DDS e LDR estão ambos online.

   Para realizar a desativação do nó de storage, os serviços DDS do sistema StorageGRID (hospedados por nós de storage) devem estar online. Este é um requisito da reavaliação do ILM.

3. Para exibir as tarefas de grade ativa, selecione **nó de administração principal CMN tarefas de grade Visão geral**.
4. Verifique o estado da tarefa de desativação da grelha.

   a. Se o status da tarefa de grade de desativação indicar um problema ao salvar pacotes de tarefas de grade, selecione **nó Admin primário CMN Eventos Visão geral**

   b. Verifique o número de relés de auditoria disponíveis.

      Se o atributo Available Audit Relay for um ou mais, o serviço CMN estará conetado a pelo menos um serviço ADC. Os serviços ADC atuam como relés de Auditoria.

   O serviço CMN deve estar conetado a pelo menos um serviço ADC e a maioria (50% mais um) dos

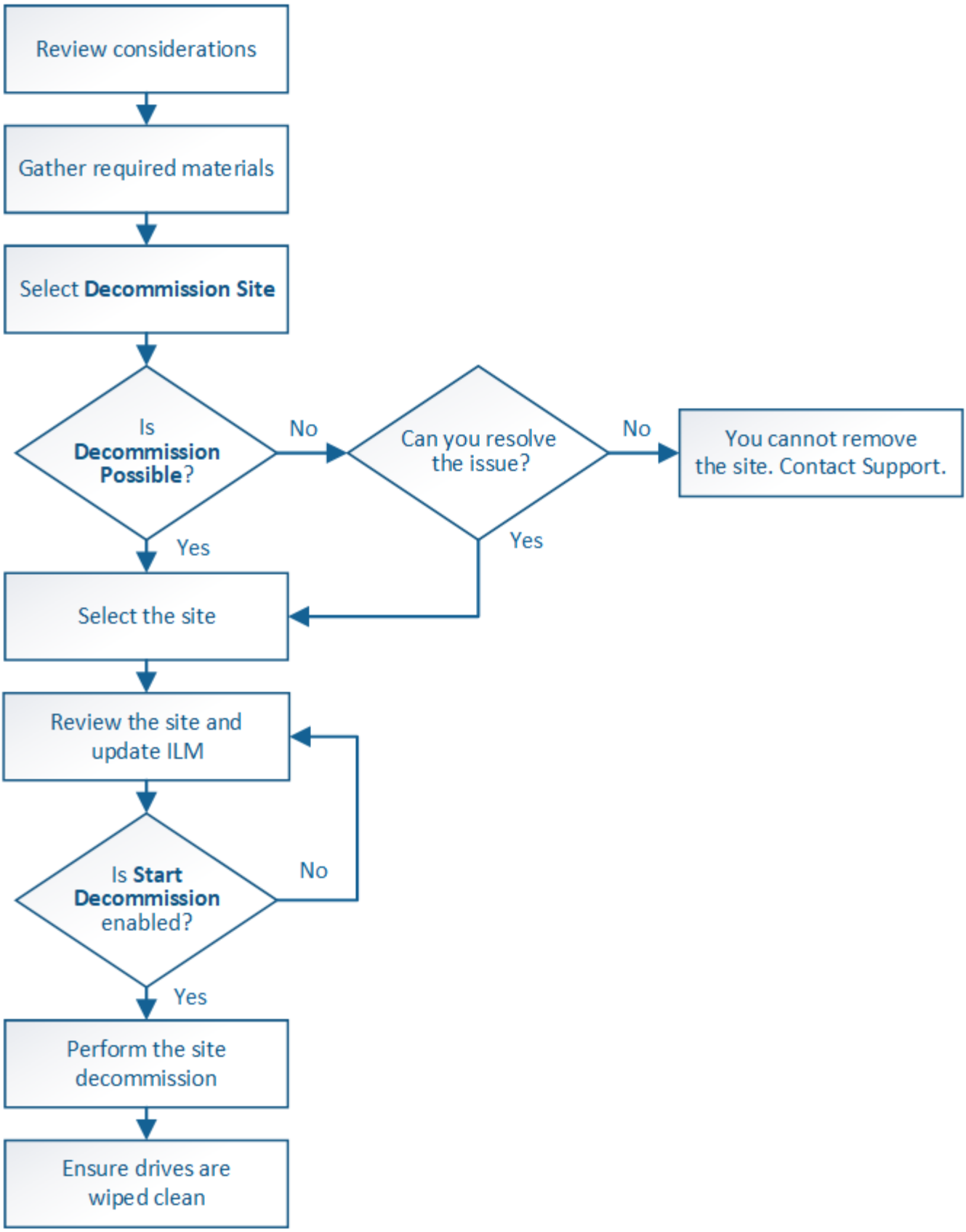
serviços ADC do sistema StorageGRID deve estar disponível para que uma tarefa de grade passe de um estágio de desativação para outro e termine.

a. Se o serviço CMN não estiver conetado a serviços ADC suficientes, verifique se os nós de storage estão online e verifique a conetividade de rede entre o nó de administração principal e os nós de storage.

Desativação do local

Talvez seja necessário remover um site de data center do sistema StorageGRID. Para remover um site, você deve desativá-lo.

O fluxograma mostra as etapas de alto nível para a desativação de um local.



Passos

- "Considerações para remover um site"
- "Recolha de materiais necessários"

- "Passo 1: Selecione Site"
- "Passo 2: Ver detalhes"
- "Passo 3: Revise a Política de ILM"
- "Passo 4: Remover referências ILM"
- "Etapa 5: Resolver conflitos de nó (e iniciar a desativação)"
- "Passo 6: Monitorar a desintegração"

Considerações para remover um site

Antes de usar o procedimento de desativação do site para remover um site, você deve revisar as considerações.

O que acontece quando você desativa um site

Ao desativar um site, o StorageGRID remove permanentemente todos os nós do site e do próprio site do sistema StorageGRID.

Quando o procedimento de desativação do local estiver concluído:

- Você não pode mais usar o StorageGRID para visualizar ou acessar o site ou qualquer um dos nós no site.
- Você não pode mais usar pools de storage ou perfis de codificação de apagamento que se referissem ao site. Quando o StorageGRID descompacta um site, ele remove automaticamente esses pools de armazenamento e desativa esses perfis de codificação de apagamento.

Diferenças entre os procedimentos de desativação do local 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 de administração principal.
- Não é possível desativar um site que inclua um nó de arquivo.
- Não é possível desativar um local se algum dos nós tiver uma interface que pertença a um grupo de alta disponibilidade (HA). Você deve editar o grupo de HA para remover a interface do nó ou remover todo o grupo de HA.
- Não é possível desativar um local se ele contiver uma mistura de nós conetados ( ) e desconetados (ou).
- Não é possível desativar um local se qualquer nó em qualquer outro local estiver desconetado (ou).
- Não é possível iniciar o procedimento de desativação do local se uma operação de reparação ec-node estiver em curso. Consulte o tópico a seguir para rastrear reparos de dados codificados por apagamento.

  "Verificação de trabalhos de reparação de dados"

- Enquanto o procedimento de desativação do site está em execução:
  - Você não pode criar regras ILM que se referem ao site que está sendo desativado. Você também não pode editar uma regra ILM existente para se referir ao site.
  - Não é possível executar outros procedimentos de manutenção, como expansão ou atualização.

    Se você precisar executar outro procedimento de manutenção durante a desativação de um site conetado, poderá pausar o procedimento enquanto os nós de storage estiverem sendo removidos. O botão **Pausa** é ativado durante o estágio ""Descomissionamento replicado e eliminação de dados codificados"".

  - Se você precisar recuperar qualquer nó depois de iniciar o procedimento de desativação do site, entre em Contato com o suporte.
- 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 pela política ILM ativa. Se for, você deve criar e ativar uma nova política ILM com novas regras ILM.
- Não existe nenhuma política proposta de ILM. Se você tem uma política proposta, você deve excluí-la.

- Nenhuma regra de ILM se refere ao site, mesmo que essas regras não sejam usadas na política ativa ou proposta. Você deve excluir ou editar todas as regras que se referem ao site.

Quando o StorageGRID descompacta o site, ele desativará automaticamente quaisquer perfis de codificação de apagamento não utilizados que se refiram ao site e excluirá automaticamente quaisquer pools de armazenamento não utilizados que se refiram ao site. O pool de storage de todos os nós de storage padrão do sistema é removido porque ele usa todos os sites.

> Antes de remover um site, talvez seja necessário criar novas regras ILM e ativar uma nova política ILM. Essas instruções assumem que você tem um bom entendimento de como o ILM funciona e que você está familiarizado com a criação de pools de armazenamento, perfis de codificação de apagamento, regras do ILM e a simulação e ativação de uma política de ILM. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

"Gerenciar objetos com ILM"

Considerações para os dados do objeto em um local 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 a política de ILM, você deve revisar a capacidade em ambos os sites. Você precisa garantir que o local de Sunnyvale tenha capacidade suficiente para acomodar os dados de objeto do local de Raleigh e que a capacidade adequada permaneça em Sunnyvale para crescimento futuro.

  > Para garantir que a capacidade adequada esteja disponível, talvez seja necessário adicionar volumes de storage ou nós de storage a um local existente ou adicionar um novo local antes de executar este procedimento. Consulte as instruções para expandir um sistema StorageGRID.

- Excluir cópias de objetos do site selecionado.

  Exemplo para excluir dados: Suponha que você use atualmente uma regra ILM de 3 cópias para replicar dados de objetos em três sites. Antes de desativar um site, você pode criar uma regra ILM equivalente a 2 cópias para armazenar dados em apenas dois sites. Quando você ativa uma nova política de ILM que usa a regra de 2 cópias, o StorageGRID exclui as cópias do terceiro site porque elas não atendem mais aos requisitos de ILM. No entanto, os dados do objeto ainda serão protegidos e a capacidade dos dois locais restantes permanecerá a mesma.

  > Nunca crie uma regra ILM de cópia única para acomodar a remoção de um site. Uma regra de ILM que cria apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Requisitos adicionais para uma desativação do local 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 executar um procedimento de expansão para adicionar um novo nó 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 na política ILM ativa. Em alguns casos, talvez seja necessário expandir o sistema StorageGRID adicionando nós de storage, volumes de storage ou novos sites antes de concluir a desativação de um site conectado.
- Você deve permitir tempo adequado para que o procedimento de desativação seja concluído. Os processos de ILM da StorageGRID podem levar dias, semanas ou até meses para mover ou excluir dados de objetos do site antes que o site possa ser desativado.

> A migração ou exclusão de dados de objetos de um local pode levar dias, semanas ou até meses, dependendo da quantidade de dados no local, da carga no sistema, das latências de rede e da natureza das mudanças necessárias no ILM.

- Sempre que possível, você deve completar os passos 1-4 do assistente Decommission Site o mais cedo possível. O procedimento de desativação será concluído mais rapidamente e com menos interrupções e impactos no desempenho se você permitir que os dados sejam movidos do site antes de iniciar o procedimento de desativação real (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.

- Todos os nós no local devem ter um estado de conexão de um dos seguintes:
  - **Desconhecido** (): O nó não está conetado à grade por um motivo desconhecido. Por exemplo, a conexão de rede entre nós foi perdida ou a energia está inativa.
  - **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 para controles de consistência quando você remove um site

O nível de consistência para um bucket do S3 ou contêiner Swift determina se o StorageGRID replica totalmente os metadados de objetos para todos os nós e sites antes de dizer a um cliente que a ingestão de objetos foi bem-sucedida. O nível de consistência faz uma troca entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós e sites de storage.

Quando o StorageGRID remove um site, ele precisa garantir que nenhum dado seja gravado no site que está sendo removido. Como resultado, ele substitui temporariamente o nível de consistência para cada bucket ou contentor. Depois de iniciar o processo de desativação do site, o StorageGRID usa temporariamente a consistência forte do site para impedir que os metadados de objetos sejam gravados no site sejam removidos.

Como resultado dessa substituição temporária, esteja ciente de que qualquer operação de gravação, atualização e exclusão do cliente que ocorrer durante a desativação de um site pode falhar se vários nós ficarem indisponíveis nos locais restantes.

Informações relacionadas

"Como a recuperação do local é realizada pelo suporte técnico"

"Gerenciar objetos com ILM"

"Expanda sua grade"

Recolha de 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.

Item	Notas
`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"

"Transferir o pacote de recuperação"

Passo 1: Selecione Site

Para determinar se um site pode ser desativado, comece acessando o assistente Decommission Site.

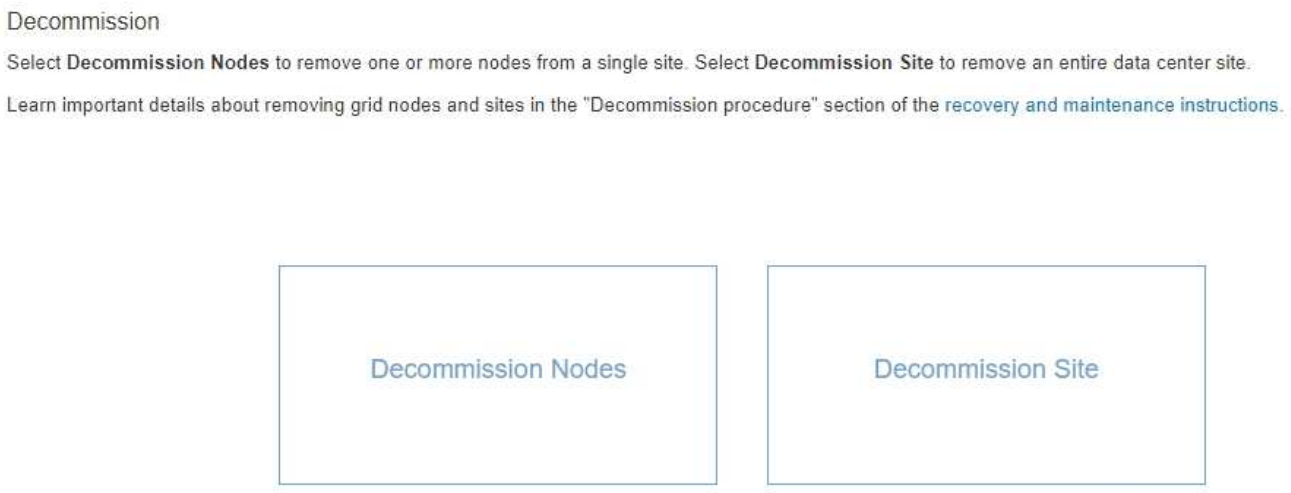
O que você vai precisar

- Você deve ter obtido todos os materiais necessários.
- Você deve ter revisado as considerações para remover um site.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root ou as permissões Manutenção e ILM.

Passos

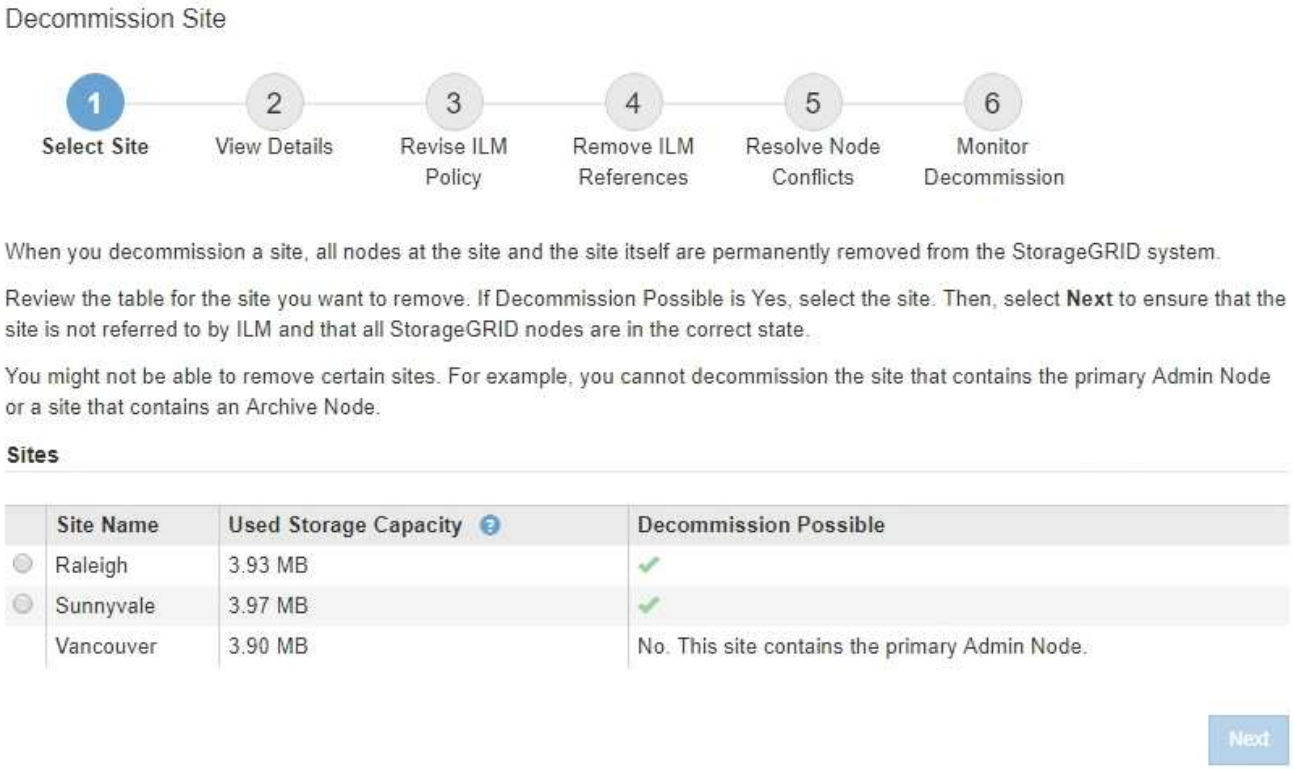
1. Selecione **Manutenção** > **tarefas de Manutenção** > **Desmontagem**.

   A página Decommission é exibida.



2. Selecione o botão **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.
Não. Este site contém o nó de administração principal.	Não é possível desativar um site que contém o nó de administração principal.	Nenhum. Não é possível executar este procedimento.
Não. Este site contém um ou mais nós de arquivo.	Não é possível desativar um site que contém um nó de arquivo.	Nenhum. Não é possível executar este procedimento.
Não. Todos os nós neste local estão desconetados. Contacte o representante da sua conta NetApp.	Não é possível executar uma desativação do site conetado a menos que cada nó no site esteja conetado (✔).	Se você quiser executar uma desativação do site desconetada, entre em Contato com seu representante da conta do NetApp, que revisará seus requisitos e ativará o restante do assistente do site de desintegração. **IMPORTANTE**: Nunca coloque os nós online offline para que você possa remover um site. Você perderá dados.

O exemplo mostra um sistema StorageGRID com três locais. A marca de seleção verde (✔) para os sites Raleigh e Sunnyvale indica que você pode desativar esses sites. No entanto, você não pode desativar o site Vancouver porque ele contém o nó Admin principal.

1. Se for possível desativar, selecione o botão de opção do site.

   O botão **Next** está ativado.

2. Selecione **seguinte**.

   A etapa 2 (Exibir detalhes) é exibida.

Passo 2: Ver detalhes

Na Etapa 2 (Exibir detalhes) do assistente Decommission Site, você pode analisar quais nós estão incluídos no site, ver quanto espaço foi usado em cada nó de armazenamento e avaliar quanto espaço livre está disponível nos outros sites da sua grade.

O que você vai precisar

Antes de desativar um site, você deve rever a quantidade de dados de objeto existentes no site.

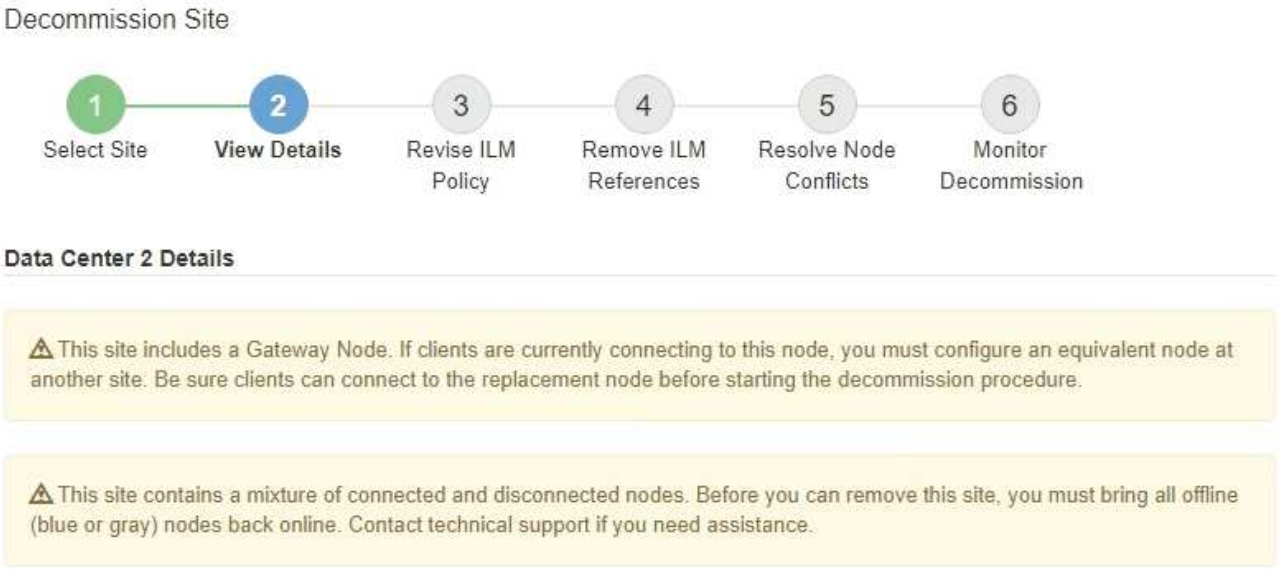
- Se você estiver executando uma desativação de um site conetado, você deve entender a quantidade de dados de objeto atualmente existentes no site antes de atualizar o ILM. Com base nas capacidades do site e nas necessidades de proteção de dados, você pode criar novas regras de ILM para mover dados para outros sites ou excluir dados de objeto do site.
- Execute as expansões necessárias do nó de armazenamento antes de iniciar o procedimento de desativação, se possível.

- Se você estiver executando uma desativação de site desconetada, você deve entender a quantidade de dados de objeto ficarão permanentemente inacessíveis quando você remover o site.

> Se você estiver executando uma desativação de site desconetada, o ILM não poderá mover ou excluir dados de objeto. Quaisquer dados que permaneçam no site serão perdidos. No entanto, se sua política de ILM foi projetada para proteger contra a perda de um único site, cópias de seus dados de objeto ainda existem nos sites restantes.

Passos

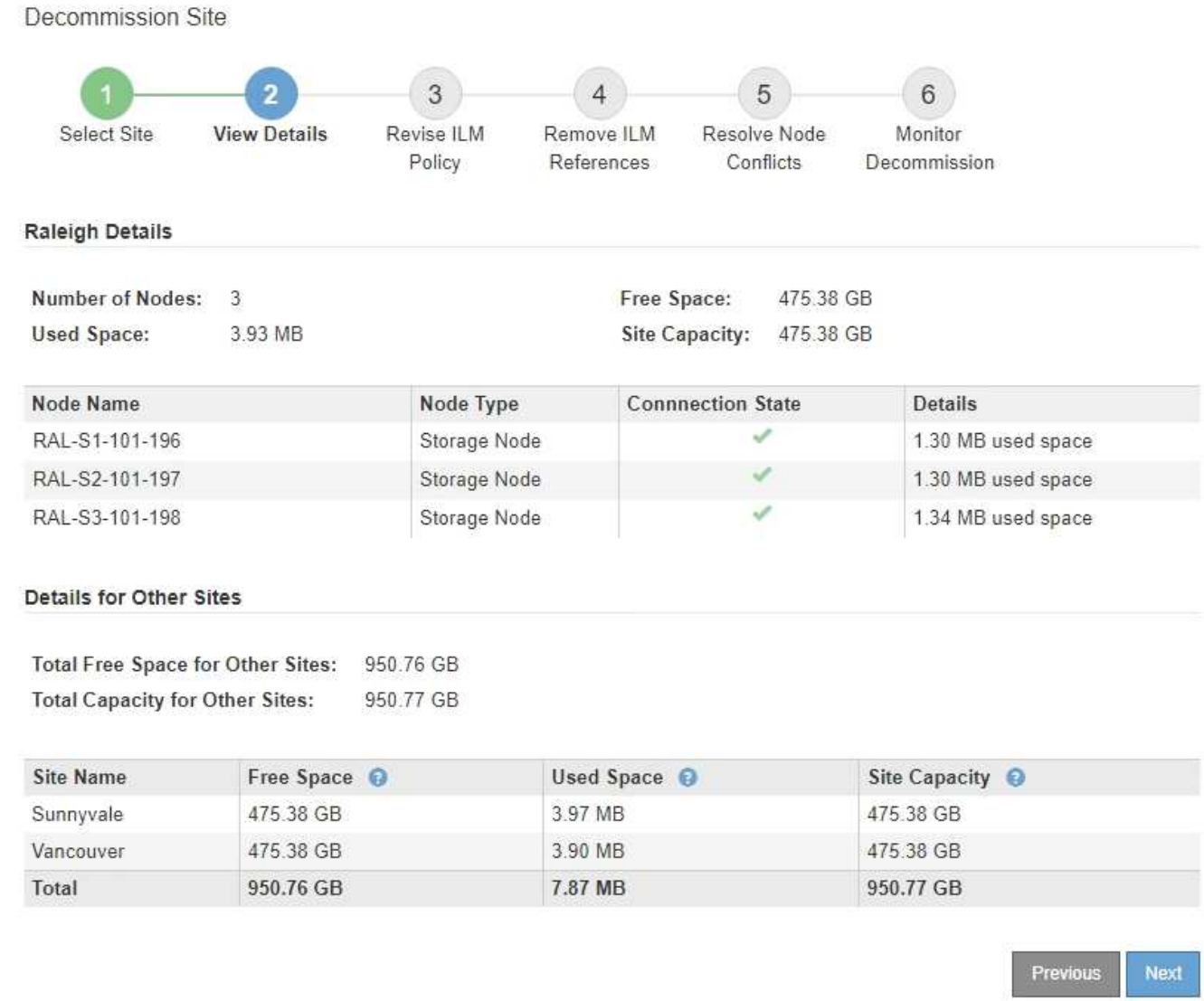
1. No passo 2 (Ver detalhes), reveja quaisquer avisos relacionados com o site que selecionou para remover.



   Nestes casos, aparece um aviso:

   - O site inclui um Gateway Node. Se os clientes S3 e Swift estiverem se conetando atualmente 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, é necessário editar grupos de HA para remover todos os nós do local. Você também pode remover o grupo de HA se ele incluir somente nós deste local.

"Administrar o StorageGRID"

3. Na seção Detalhes para outros sites da página, avalie quanto espaço está disponível nos outros sites da sua grade.

Details for Other Sites

Total Free Space for Other Sites:	950.76 GB
Total Capacity for Other Sites:	950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	**950.76 GB**	**7.87 MB**	**950.77 GB**

Se você estiver executando uma desativação do site 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.

Informações relacionadas

"Gerenciar objetos com ILM"

Passo 3: Revise a Política de ILM

A partir do passo 3 (rever a política ILM) do assistente do site de desintegração, você pode determinar se o site é referido pela política ILM ativa.

O que você vai precisar

Você tem uma boa compreensão de como o ILM funciona e está familiarizado com a criação de pools de armazenamento, perfis de codificação de apagamento, regras ILM e simulação e ativação de uma política ILM.

"Gerenciar objetos com ILM"

Sobre esta tarefa

O StorageGRID não pode desativar um site se esse site for referido por qualquer regra ILM na política ILM ativa.

Se sua política ILM atual se refere ao site que você deseja remover, você deve ativar uma nova política ILM que atenda a certos requisitos. Especificamente, a nova política ILM:

- Não é possível usar um pool de armazenamento que se refere ao site.
- Não é possível usar um perfil de codificação de apagamento que se refere ao site.
- Não é possível usar o pool de armazenamento padrão **todos os nós de armazenamento** ou o site padrão **todos os sites**.
- Não é possível usar a regra de estoque **Make 2 copies**.
- Deve ser projetado para proteger totalmente todos os dados de objetos.

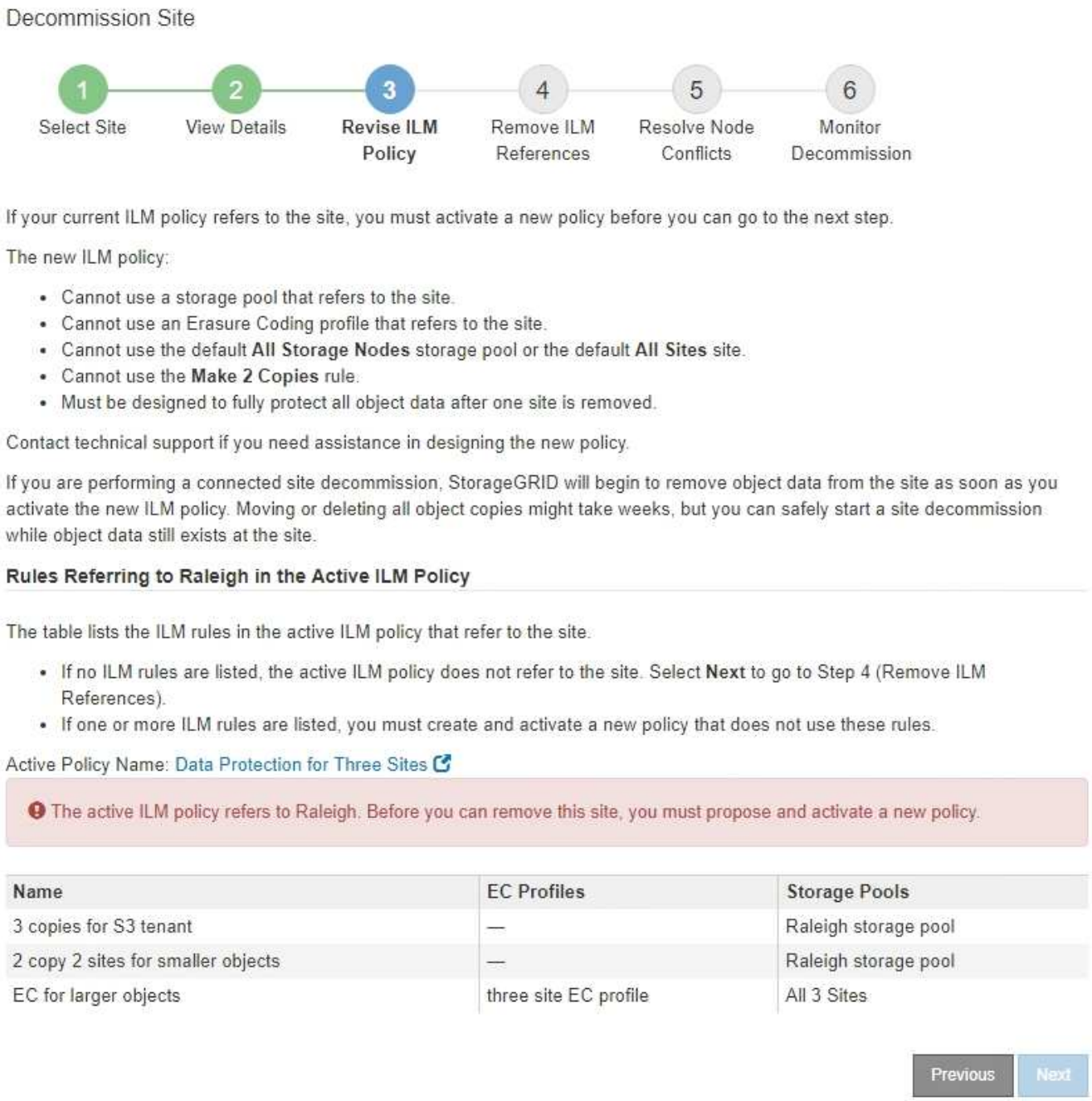
> Nunca crie uma regra ILM de cópia única para acomodar a remoção de um site. Uma regra de ILM que cria apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Se você estiver executando um *Connected site Dedescomissionar*, você deve considerar como o StorageGRID deve gerenciar os dados do objeto atualmente no site que você deseja remover. Dependendo dos requisitos de proteção de dados, as novas regras podem mover os dados de objetos existentes para diferentes locais ou excluir quaisquer cópias de objetos extras que não sejam mais necessárias.

Entre em Contato com o suporte técnico se precisar de assistência para projetar a nova política.

Passos

1. Na Etapa 3 (revisar a Política ILM), determine se alguma regra ILM na política ILM ativa se refere ao site que você selecionou para remover.



2. Se nenhuma regra estiver listada, selecione **Next** para ir para a Etapa 4 (Remover referências ILM)

   "Passo 4: Remover referências ILM"

3. Se uma ou mais regras ILM estiverem listadas na tabela, selecione o link ao lado de **Nome da política ativa**.

   A página de políticas ILM aparece em uma nova guia do navegador. Use esta guia para atualizar o ILM. A página Decommission Site permanecerá aberta na outra guia.

   a. Se necessário, selecione **ILM Storage Pools** para criar um ou mais pools de armazenamento que não se referem ao site.

Para obter detalhes, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

b. Se você planeja usar a codificação de apagamento, selecione **ILM Codificação de apagamento** para criar um ou mais perfis de codificação de apagamento.

   Você deve selecionar pools de armazenamento que não se referem ao site.

   Não use o pool de storage **todos os nós de storage** nos perfis de codificação de apagamento.

4. Selecione **ILM Rules** e clone cada uma das regras listadas na tabela para a Etapa 3 (revisar a Política ILM).

   Para obter detalhes, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

   a. Use nomes que facilitem a seleção dessas regras em uma nova política.
   b. Atualize as instruções de colocação.

      Remova todos os pools de storage ou perfis de codificação de apagamento que se referem ao site e substitua-os por novos pools de armazenamento ou perfis de codificação de apagamento.

      Não use o pool de armazenamento **todos os nós de storage** nas novas regras.

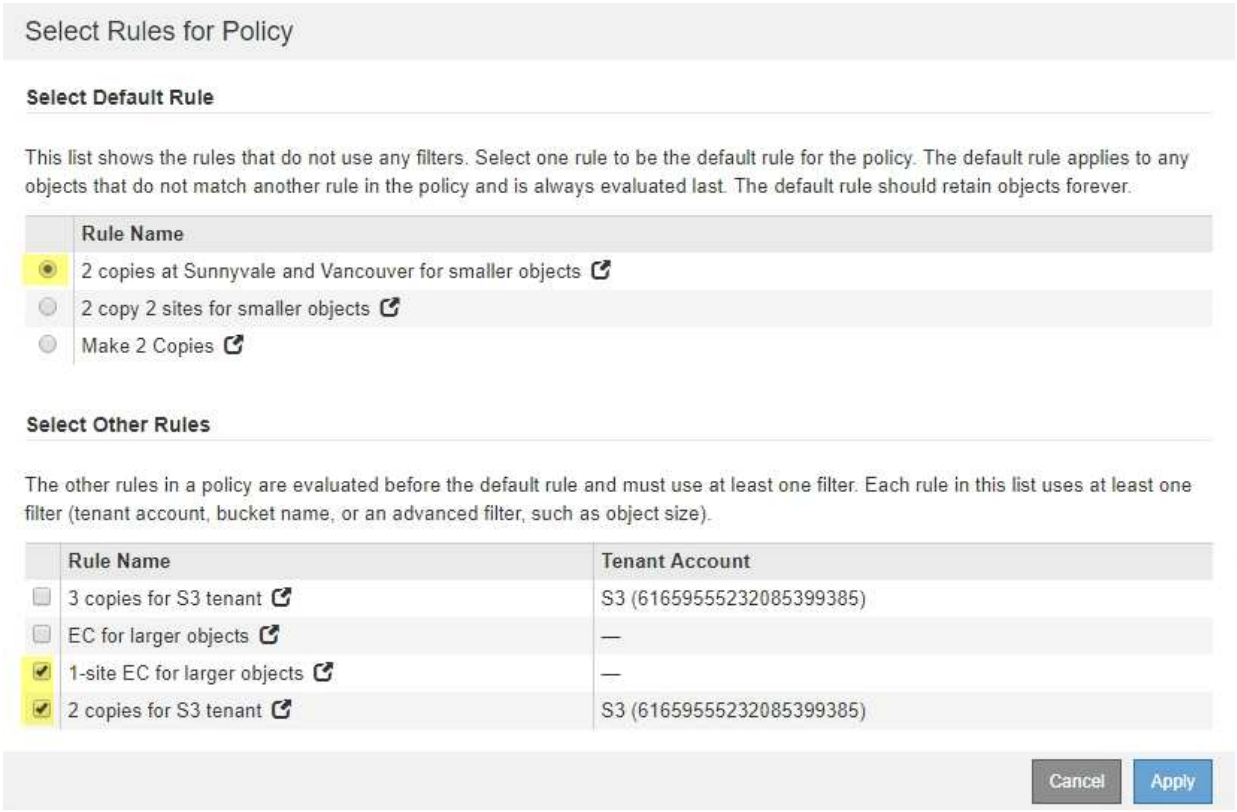
5. Selecione **ILM Policies** e crie uma nova política que use as novas regras.

   Para obter detalhes, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

   a. Selecione a política ativa e selecione **Clone**.
   b. Especifique um nome de política e um motivo para a alteração.
   c. Selecione regras para a política clonada.
      - Desmarque todas as regras listadas para a Etapa 3 (revisar a Política ILM) da página do site de desintegração.
      - Selecione uma regra padrão que não se refira ao site.

        Não selecione a regra **Make 2 Copies** porque essa regra usa o pool de armazenamento **All Storage Nodes**, que não é permitido.

      - Selecione as outras regras de substituição que criou. Essas regras não devem se referir ao site.



d. Selecione **aplicar**.

e. Arraste e solte as linhas para reordenar as regras na política.

Não é possível mover a regra padrão.

Você deve confirmar se as regras ILM estão na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando na parte superior.

a. Salve a política proposta.

6. Ingira objetos de teste e simule a política proposta para garantir que as regras corretas sejam aplicadas.

Erros em uma política ILM podem causar perda de dados 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.

7. Ative a nova política.

Se você estiver executando uma desativação do site conetado, o StorageGRID começará a remover os dados do objeto do site selecionado assim que você ativar a nova política ILM. Mover ou excluir todas as cópias de objetos pode levar semanas. Embora você possa iniciar com segurança uma desativação do site enquanto os dados do objeto ainda existirem no site, o procedimento de desativação será concluído

com mais rapidez e com menos interrupções e impactos no desempenho se você permitir que os dados sejam movidos do site antes de iniciar o procedimento de desativação real (selecionando **Start Decommission** no passo 5 do assistente).

8. Volte para **passo 3 (revisar a política ILM)** para garantir que nenhuma regra ILM na nova política ativa consulte o site e o botão **Next** esteja ativado.

> Se alguma regra estiver listada, você deve criar e ativar uma nova política ILM antes de continuar.

9. Se nenhuma regra estiver listada, selecione **Next**.

   O passo 4 (Remover referências ILM) é exibido.

Passo 4: Remover referências ILM

No passo 4 (Remover referências ILM) do assistente Decommission Site, você pode remover a política proposta se existir e excluir ou editar quaisquer regras ILM não utilizadas que ainda se referem ao site.

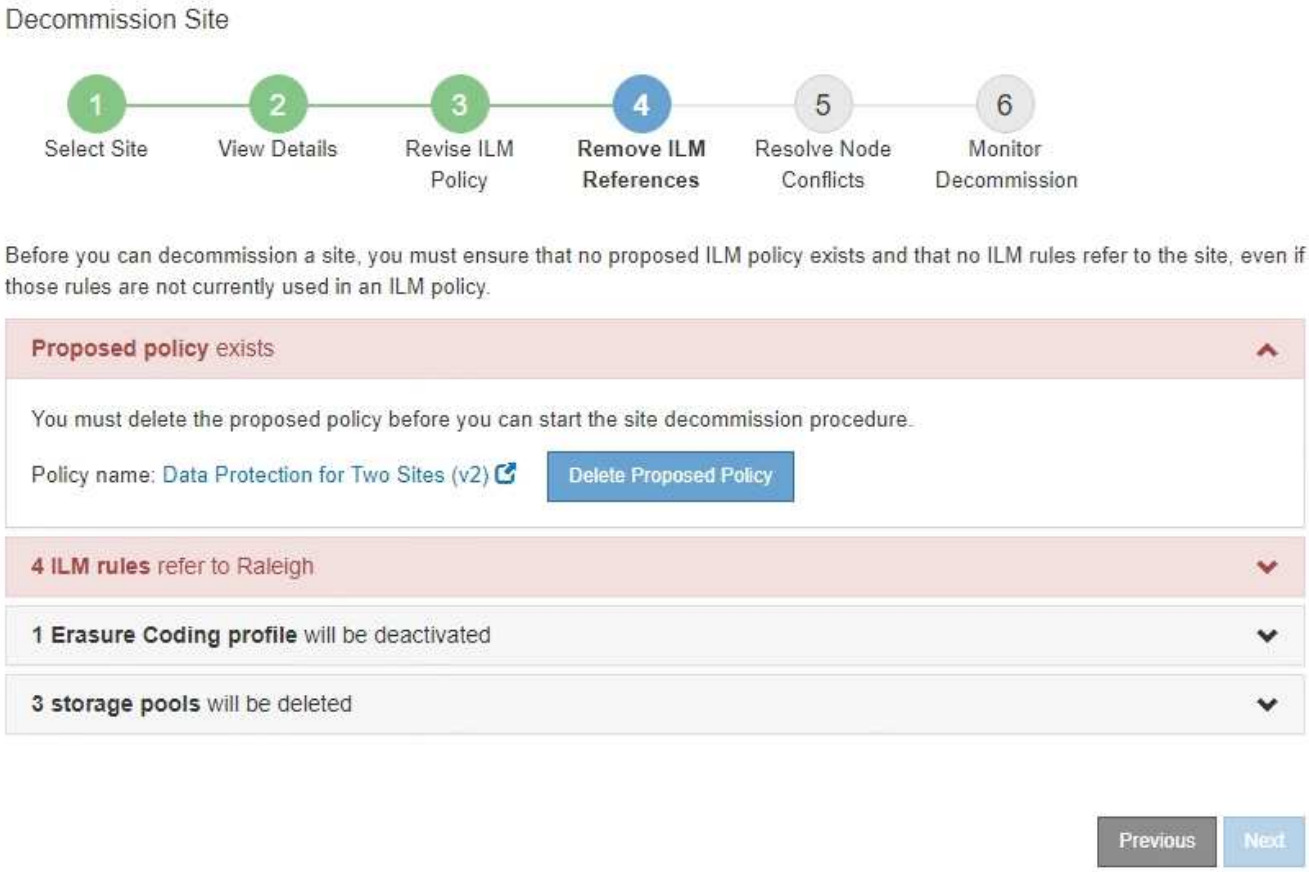
Sobre esta tarefa

Você está impedido de iniciar o procedimento de desativação do site nestes casos:

- Existe uma política proposta de ILM. Se você tem uma política proposta, você deve excluí-la.
- Qualquer regra ILM refere-se ao site, mesmo que essa regra não seja usada em nenhuma política ILM. Você deve excluir ou editar todas as regras que se referem ao site.

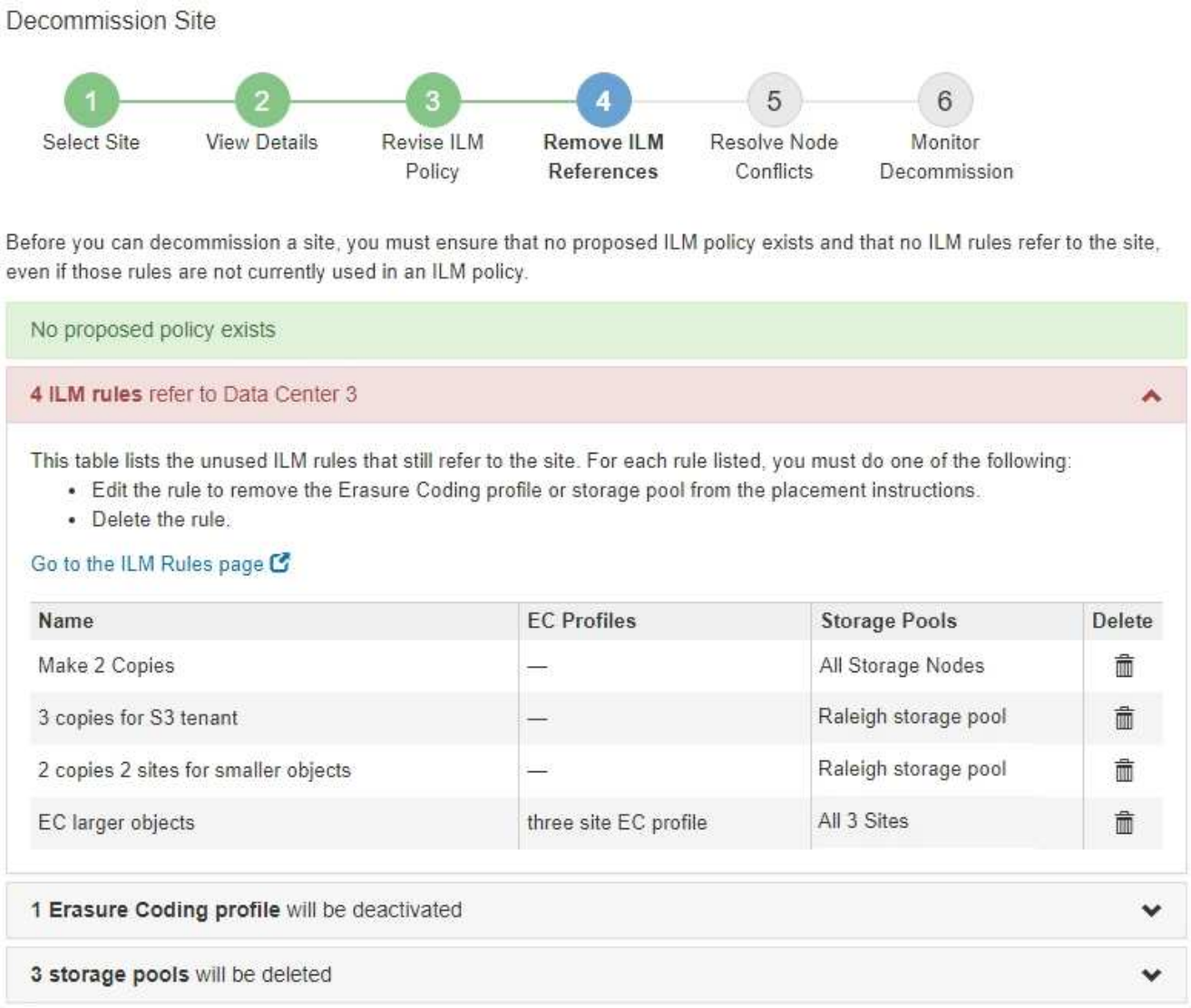
Passos

1. Se uma política proposta for listada, remova-a.



a. Selecione **Excluir Política proposta**.
b. Selecione **OK** na caixa de diálogo de confirmação.

2. Determine se quaisquer regras de ILM não utilizadas se referem ao site.



Todas as regras ILM que estão listadas ainda se referem ao site, mas não são usadas em nenhuma política. No exemplo:

- A regra de estoque **Make 2 Copies** usa o conjunto de armazenamento padrão do sistema **All Storage Nodes**, que usa o site All Sites.
- A regra não utilizada **3 cópias para S3 inquilino** refere-se ao pool de armazenamento **Raleigh**.
- A regra não utilizada **2 copy 2 sites para objetos menores** refere-se ao pool de armazenamento **Raleigh**.
- As regras não utilizadas para **EC Large Objects** usam o site Raleigh no perfil de codificação de apagamento **All 3 Sites**.
- Se nenhuma regra ILM estiver listada, selecione **Next** para ir para **Etapa 5 (resolver conflitos de nó)**.

"Etapa 5: Resolver conflitos de nó (e iniciar a desativação)"

Quando o StorageGRID descompacta o site, ele desativará automaticamente quaisquer perfis de codificação de apagamento não utilizados que se refiram ao site e excluirá automaticamente quaisquer pools de armazenamento não utilizados que se refiram ao site. O pool de storage de todos os nós de storage padrão do sistema é removido porque ele usa o site todos os sites.

- Se uma ou mais regras ILM estiverem listadas, vá para a próxima etapa.

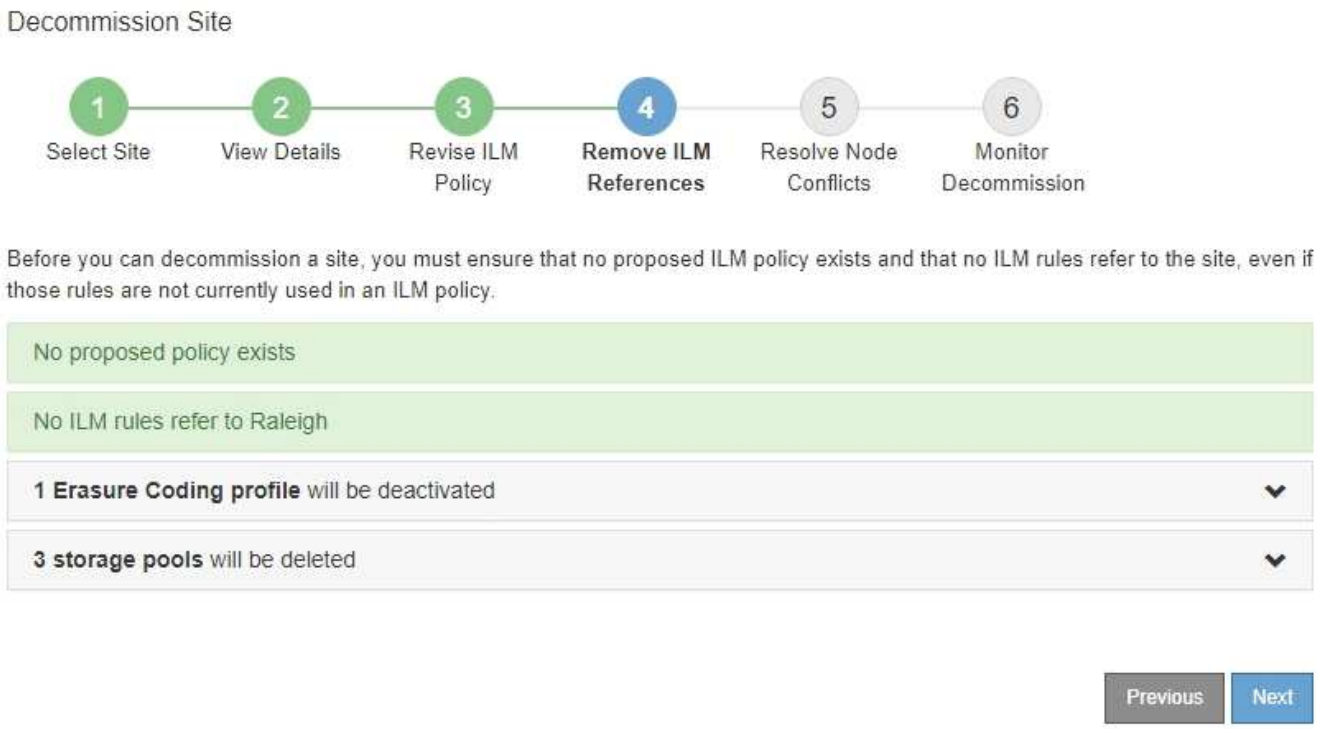
3. Edite ou exclua cada regra não utilizada:
   - Para editar uma regra, acesse a página regras do ILM e atualize todos os canais que usam um perfil de codificação de apagamento ou um pool de armazenamento que se refere ao site. Em seguida, retorne a **Etapa 4 (Remover referências ILM)**.

     Para obter detalhes, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

   - Para excluir uma regra, selecione o ícone de lixeira e selecione **OK**.

     Você deve excluir a regra de estoque **Make 2 Copies** antes de poder desativar um site.

4. Confirme se não existe nenhuma política de ILM proposta, nenhuma regra de ILM não utilizada se refere ao site e o botão **Next** está ativado.



5. Selecione **seguinte**.

   Quaisquer pools de armazenamento restantes e perfis de codificação de apagamento que se refiram ao site tornar-se-ão inválidos quando o site for removido. Quando o StorageGRID descompacta o site, ele desativará automaticamente quaisquer perfis de codificação de apagamento não utilizados que se refiram ao site e excluirá automaticamente quaisquer pools de armazenamento não utilizados que se refiram ao site. O pool de storage de todos os nós de storage padrão do sistema é removido porque ele usa o site todos os sites.

   A etapa 5 (resolver conflitos de nó) é exibida.

Etapa 5: Resolver conflitos de nó (e iniciar a desativação)

Na Etapa 5 (resolver conflitos de nós) do assistente do local de desativação, você pode determinar se algum nó no sistema StorageGRID está 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.

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.

- Nenhum nó no local que você está removendo pode ter uma interface que pertence a um grupo de alta disponibilidade (HA).

Se algum nó estiver listado para a Etapa 5 (resolver conflitos de nó), você deve corrigir o problema antes de iniciar a desativação.

Antes de iniciar o procedimento de desativação do site a partir desta página, reveja as seguintes considerações:

- Você deve permitir tempo adequado para que o procedimento de desativação seja concluído.

> A migração ou exclusão de dados de objetos de um local pode levar dias, semanas ou até meses, dependendo da quantidade de dados no local, da carga no sistema, das latências de rede e da natureza das mudanças necessárias no ILM.

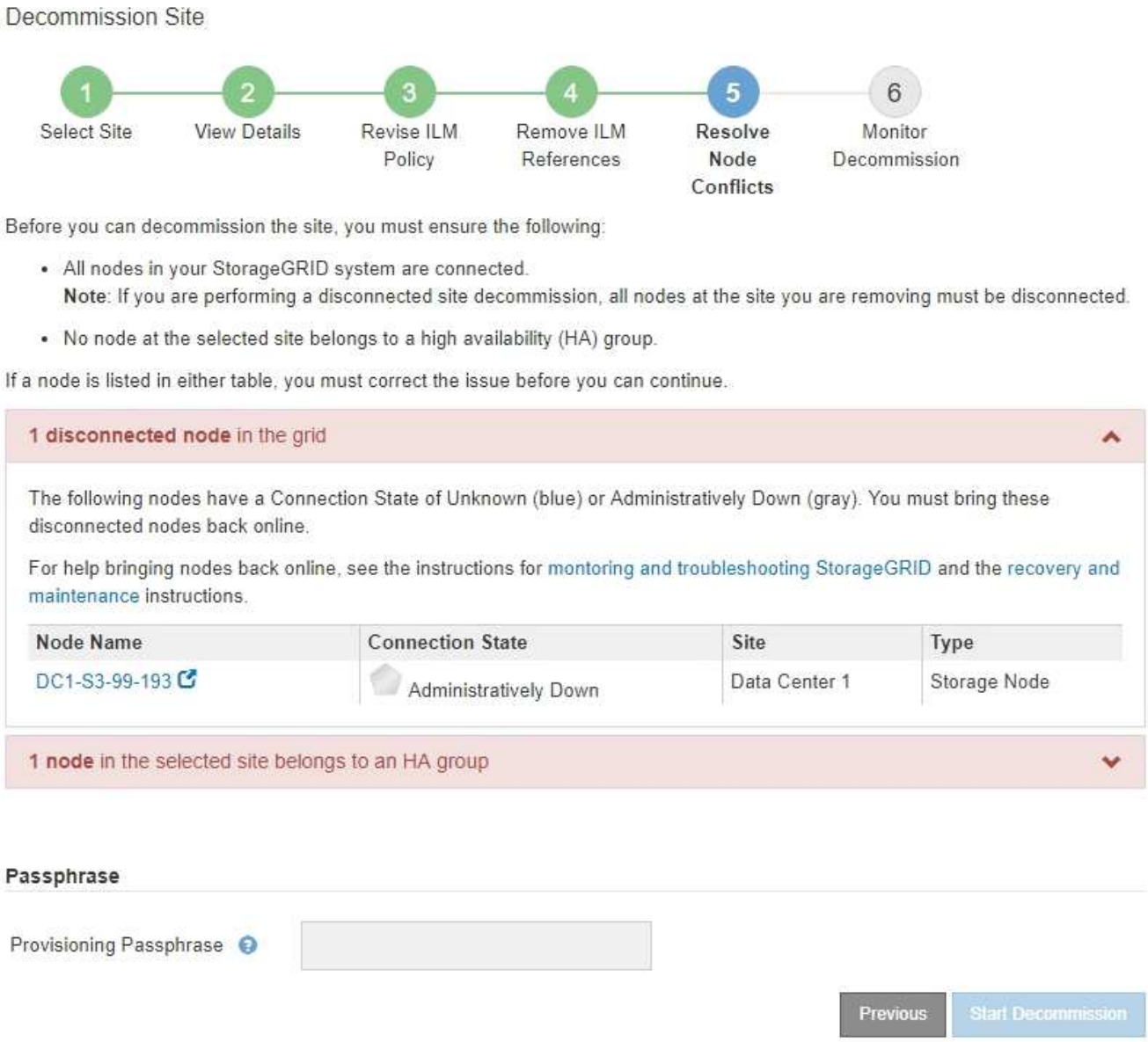
- Enquanto o procedimento de desativação do site está em execução:
  - Você não pode criar regras ILM que se referem ao site que está sendo desativado. Você também não pode editar uma regra ILM existente para se referir ao site.
  - Não é possível executar outros procedimentos de manutenção, como expansão ou atualização.

> Se você precisar executar outro procedimento de manutenção durante a desativação de um site conetado, poderá pausar o procedimento enquanto os nós de storage estiverem sendo removidos. O botão **Pausa** é ativado durante o estágio ""Descomissionamento replicado e eliminação de dados codificados"".

  - Se você precisar recuperar qualquer nó depois de iniciar o procedimento de desativação do site, entre em Contato com o suporte.

Passos

1. Consulte a seção nós 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 ( ).

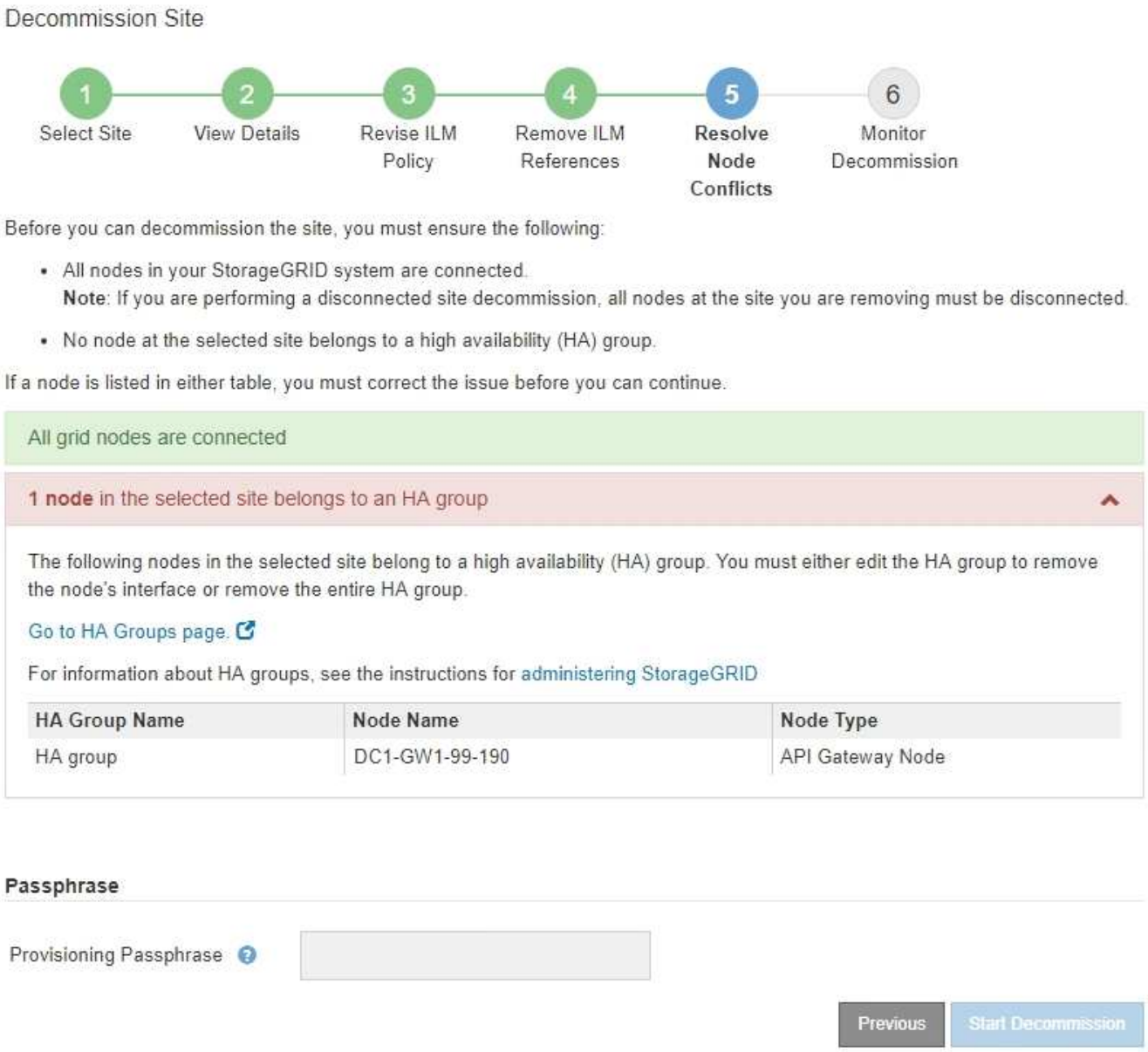


2. Se algum nó estiver desconetado, coloque-o novamente on-line.

   Consulte as instruções para monitoramento e solução de problemas do StorageGRID e os procedimentos do nó de grade. Entre em Contato com o suporte técnico se precisar de assistência.

3. Quando todos os nós desconetados forem colocados novamente on-line, consulte a seção grupos de HA da Etapa 5 (resolver conflitos de nó).

   Esta tabela lista todos os nós do local selecionado que pertencem a um grupo de alta disponibilidade (HA).

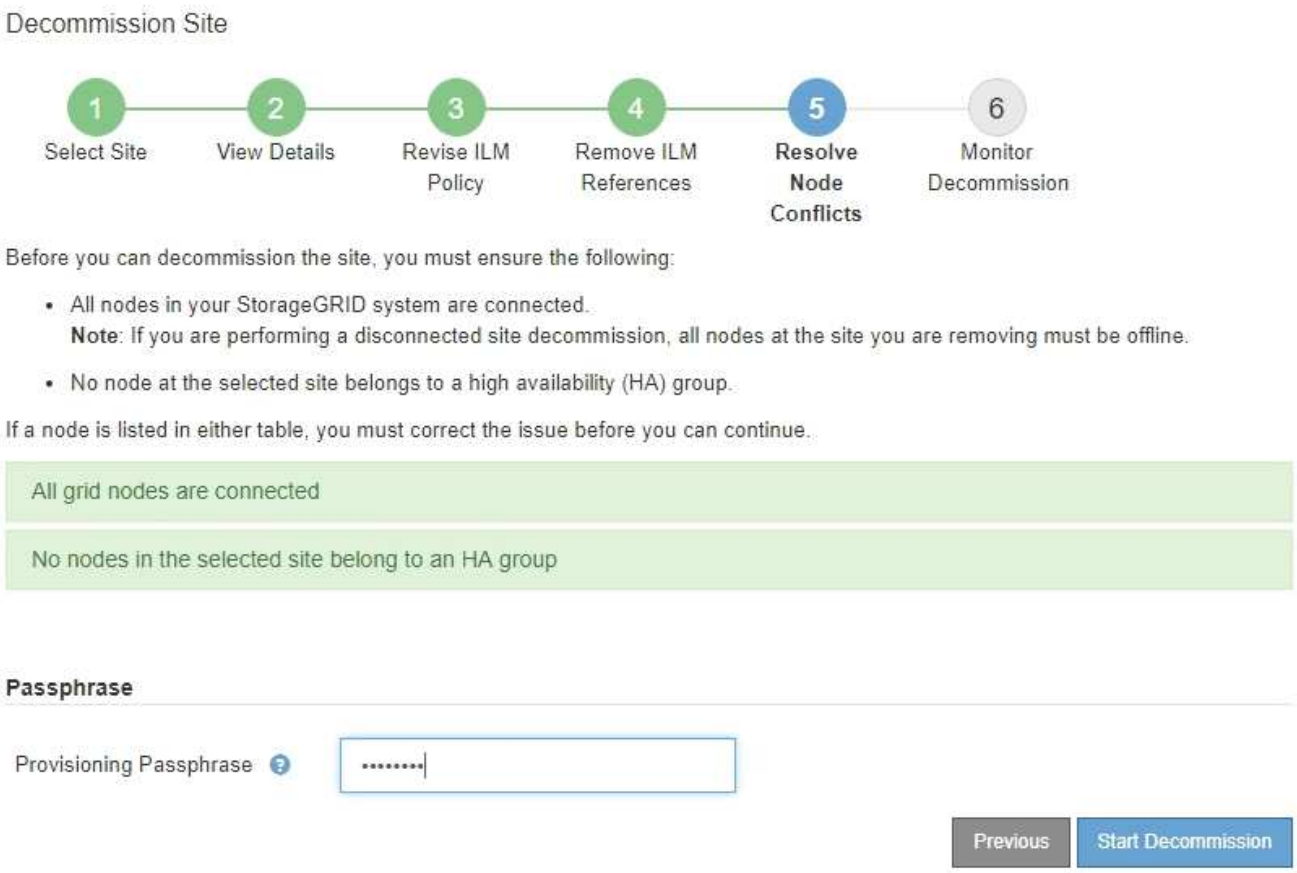


4. Se algum dos nós estiver listado, faça um dos seguintes procedimentos:
   - Edite cada grupo de HA afetado para remover a interface do nó.
   - Remover um grupo de HA que inclua somente nós deste local. Consulte as instruções para administrar o StorageGRID.

   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.

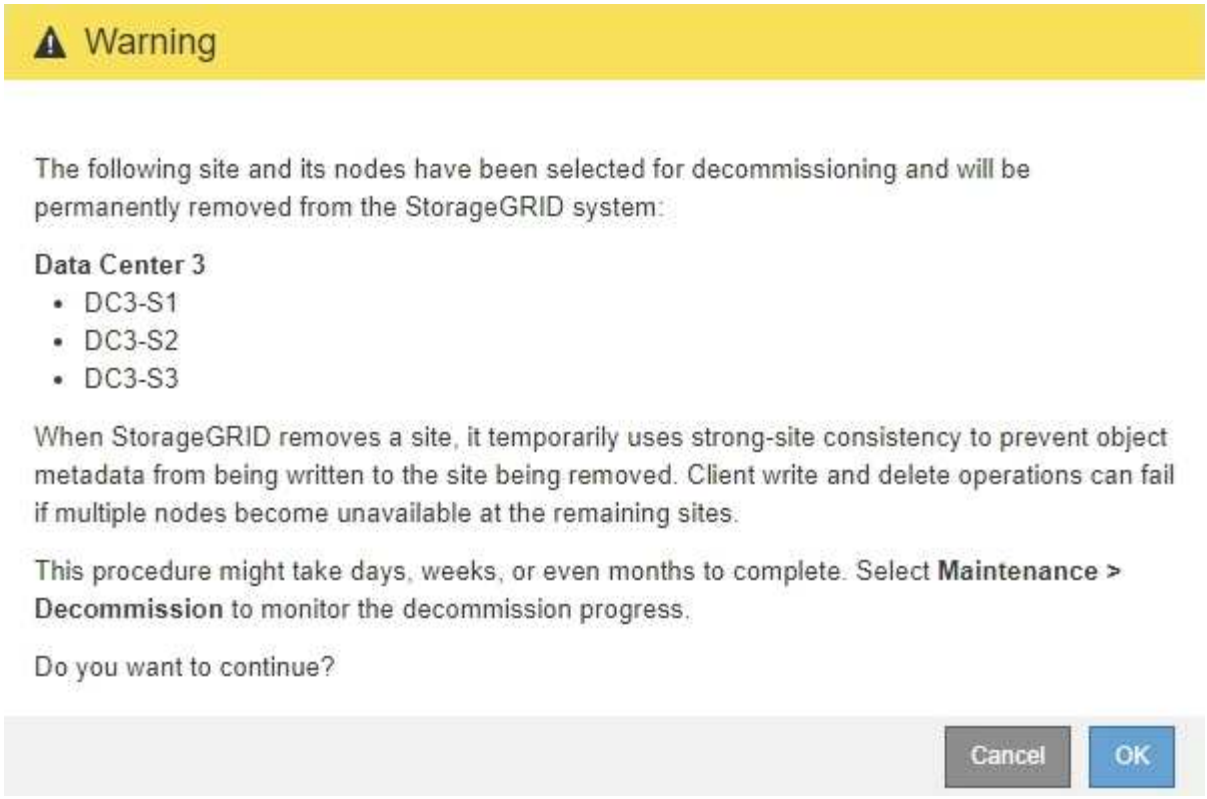
5. Introduza a frase-passe de aprovisionamento.

   O botão **Start Decommission** fica ativado.



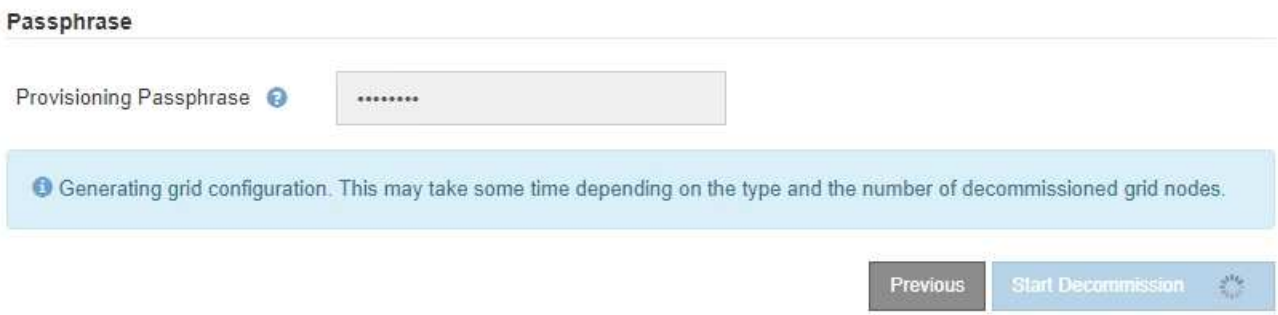
6. Se você estiver pronto para iniciar o procedimento de desativação do site, selecione **Start Decommission**.

   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.

Informações relacionadas

"Monitorizar Resolução de problemas"

"Procedimentos do nó de grade"

"Administrar o StorageGRID"

Passo 6: Monitorar a desintegração

A partir do passo 6 (Monitor Decommission) do assistente de página do site Decommission, você pode monitorar o progresso à medida que o site é removido.

Sobre esta tarefa

Quando o StorageGRID remove um site 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 **Manutenção sistema Pacote de recuperação**.

b. Transfira o `.zip` ficheiro.

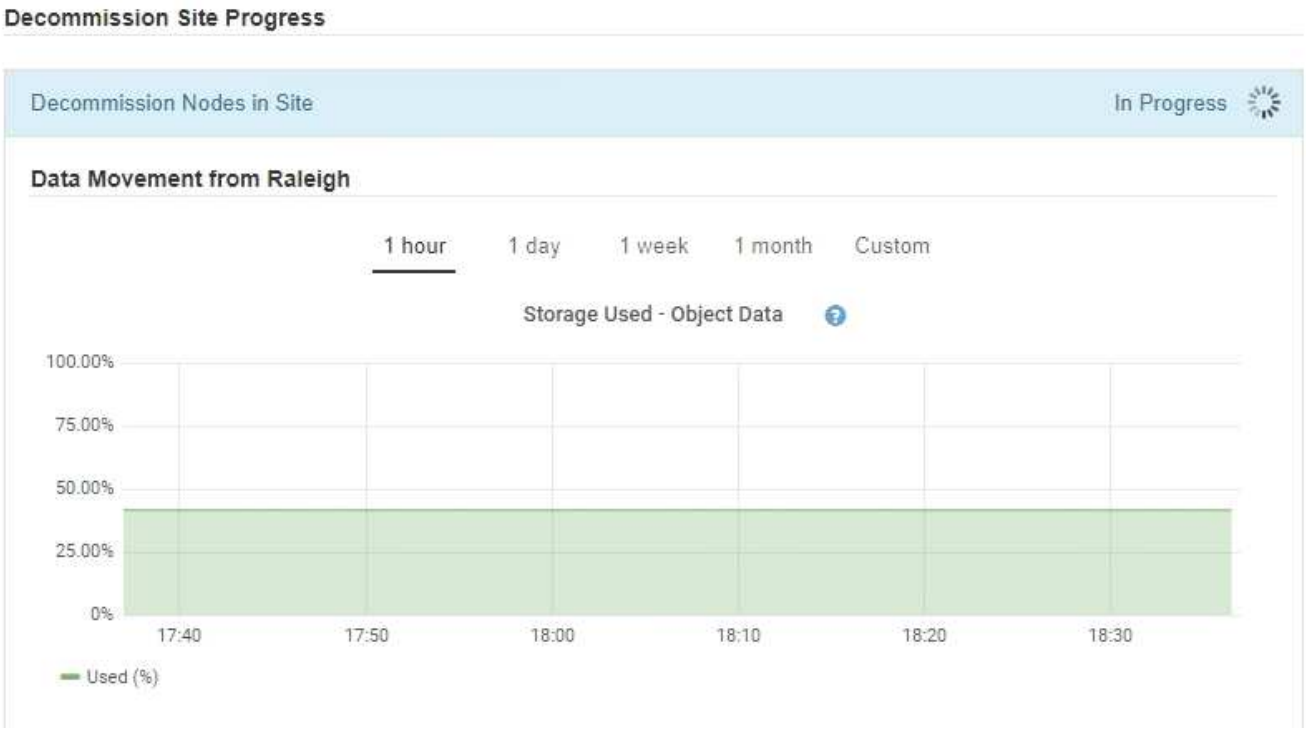
Consulte as instruções para baixar o pacote de recuperação.

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.

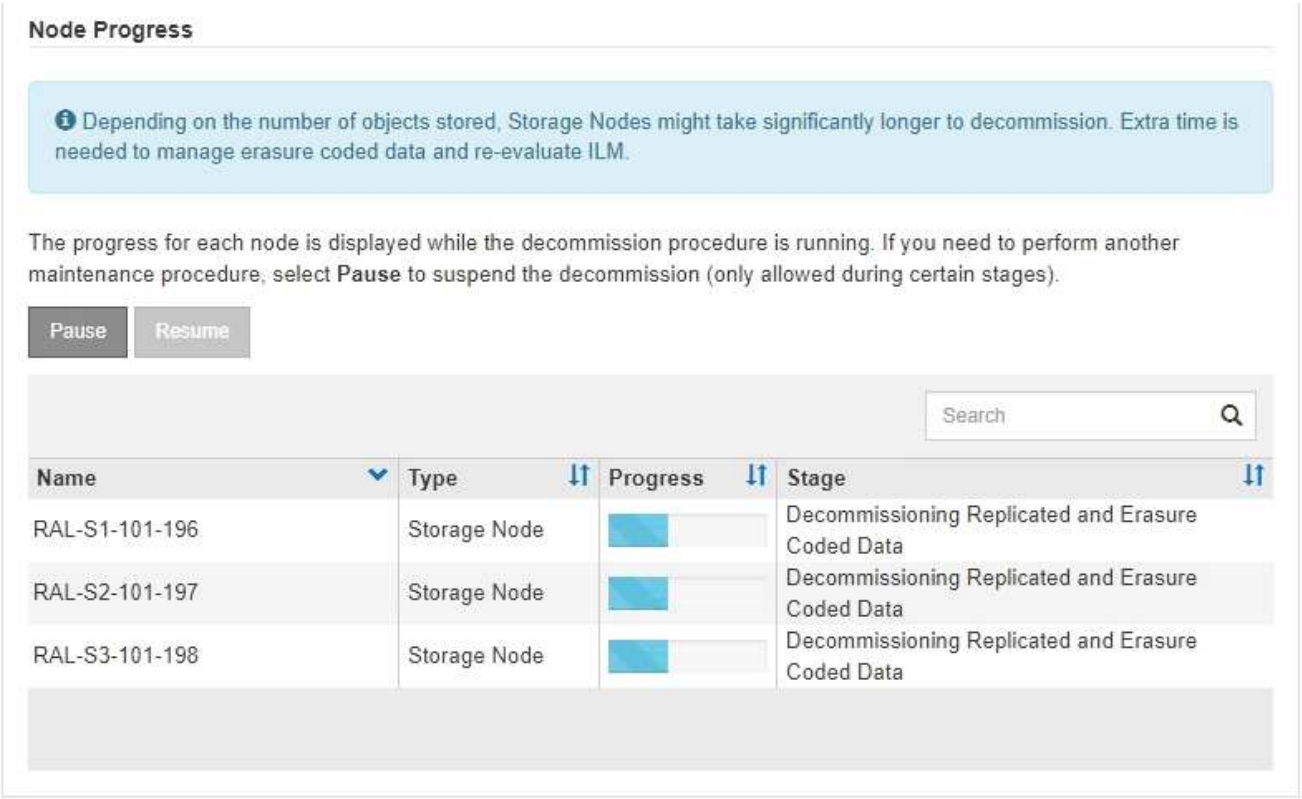
A movimentação de dados começou quando você ativou a nova política de ILM no passo 3 (revisar

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 impercetivelmente, 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.



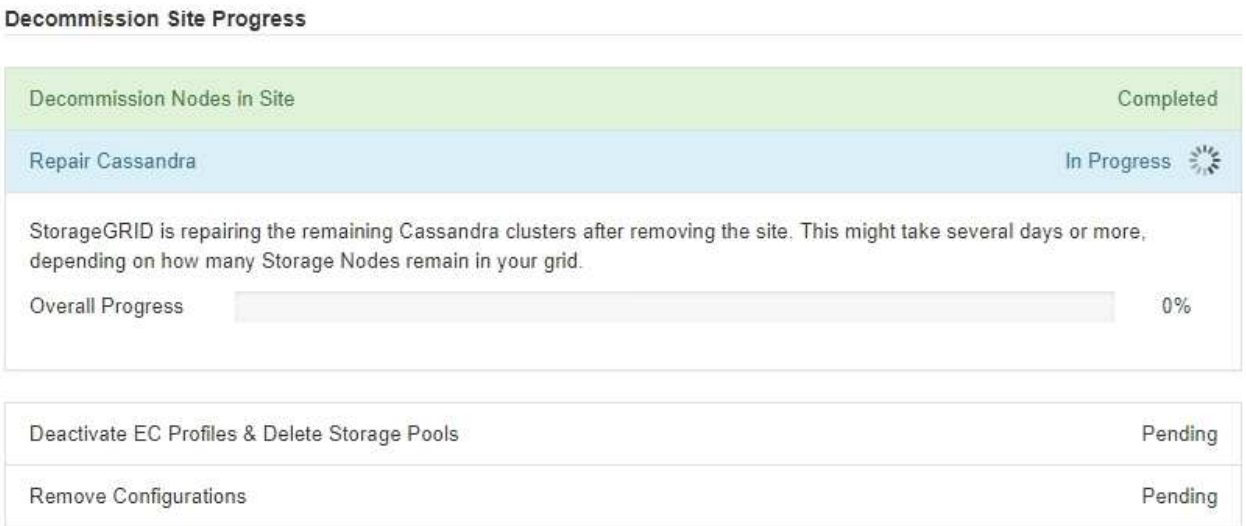
Se você estiver monitorando o progresso de uma desativação de um site conetado, consulte esta tabela para entender os estágios de desativação de um nó de armazenamento:

Fase	Duração estimada
Pendente	Minuto ou menos
Aguarde bloqueios	Minutos
Preparar tarefa	Minuto ou menos
Marcação LDR desativada	Minutos
Desativação de dados duplicados e codificados de apagamento	Horas, dias ou semanas com base na quantidade de dados **Nota**: Se você precisar executar outras atividades de manutenção, você pode pausar a desativação do site durante essa etapa.
Estado definido LDR	Minutos
Lavar filas Auditoria	Minutos a horas, com base no número de mensagens e na latência da rede.
Concluído	Minutos

Se você estiver monitorando o andamento de uma desativação de um local 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
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.

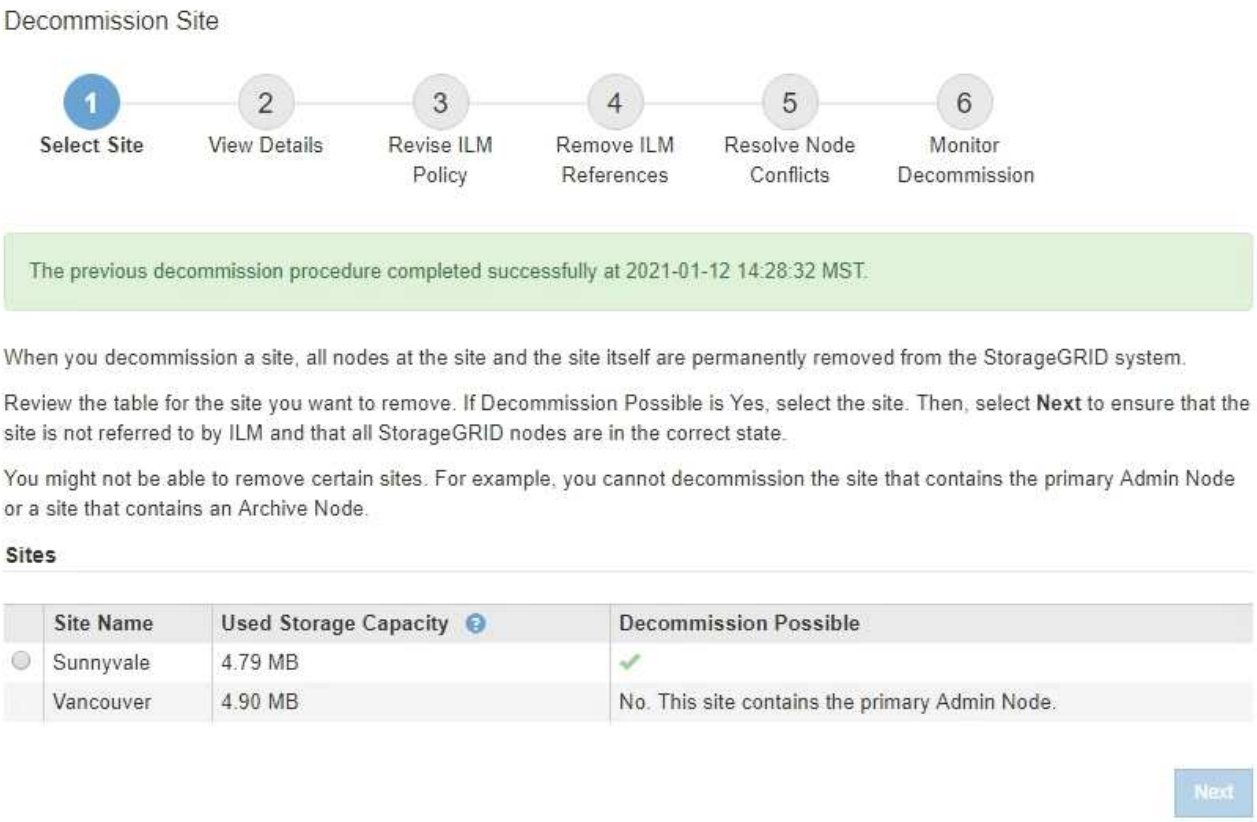


   - Durante a etapa **Deactivate EC Profiles Delete Storage Pools**, as seguintes alterações de ILM são feitas:
     - Todos os perfis de codificação de apagamento que se referem ao site são desativados.
     - Todos os pools de armazenamento que se referem ao site são excluídos.

O pool de storage de todos os nós de storage padrão do sistema também é removido porque ele usa o site todos os sites.

- Finalmente, durante a etapa **Remove Configuration**, quaisquer referências restantes ao site e seus nós são removidas do resto da grade.

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.

Informações relacionadas

"Transferir o pacote de recuperação"

Procedimentos de manutenção da rede

Você pode configurar a lista de sub-redes na rede de Grade ou atualizar endereços IP, servidores DNS ou servidores NTP para o seu sistema StorageGRID.

Opções

- "Atualizando sub-redes para a rede de Grade"
- "Configurando endereços IP"
- "Configurando servidores DNS"
- "Configurando servidores NTP"
- "Restaurar a conetividade de rede para nós isolados"

Atualizando sub-redes para a rede de Grade

O StorageGRID mantém uma lista das sub-redes de rede usadas para se comunicar entre nós de grade na rede de grade (eth0). Essas entradas incluem as sub-redes usadas para a rede de Grade por cada site em seu sistema StorageGRID, bem como quaisquer sub-redes usadas para NTP, DNS, LDAP ou outros servidores externos acessados através do gateway rede de Grade. Quando você adiciona nós de grade ou um novo site em uma expansão, talvez seja necessário atualizar ou adicionar sub-redes à rede de Grade.

O que você vai precisar

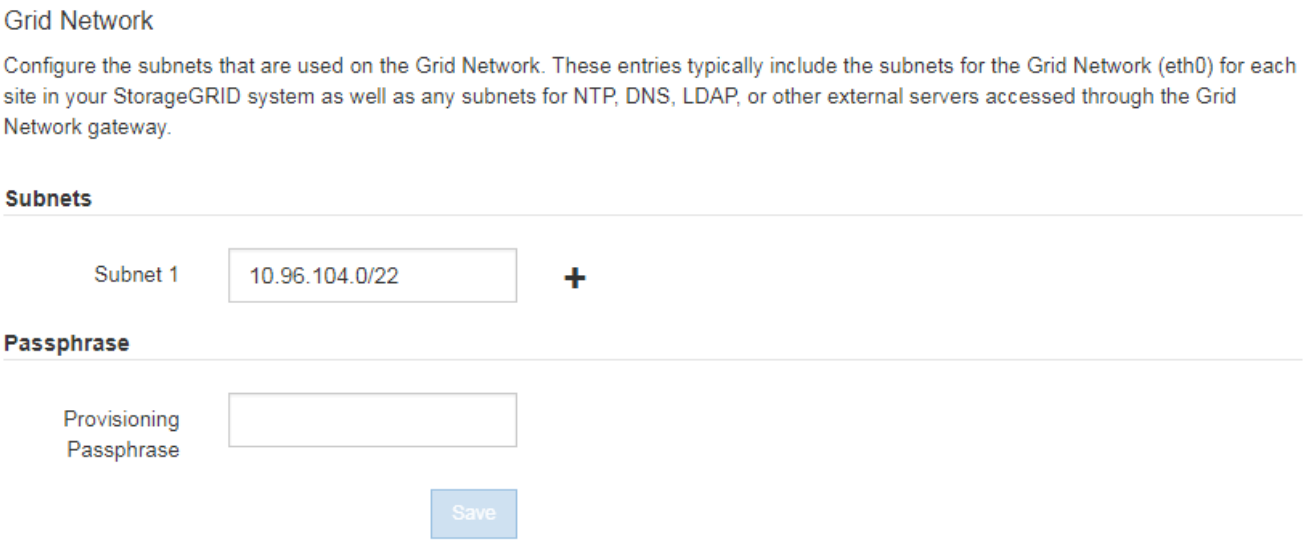
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter os endereços de rede, na notação CIDR, das sub-redes que deseja configurar.

Sobre esta tarefa

Se você estiver executando uma atividade de expansão que inclua a adição de uma nova sub-rede, será necessário adicionar a nova sub-rede da grade antes de iniciar o procedimento de expansão.

Passos

1. Selecione **Manutenção** > **rede** > **rede**.



2. Na lista de sub-redes, clique no sinal de mais para adicionar uma nova sub-rede na notação CIDR.

   Por exemplo, introduza `10.96.104.0/22`.

3. Digite a senha de provisionamento e clique em **Salvar**.

   As sub-redes especificadas são configuradas automaticamente para o sistema StorageGRID.

Configurando endereços IP

Você pode executar a configuração de rede configurando endereços IP para nós de grade usando a ferramenta alterar IP.

Você deve usar a ferramenta alterar IP para fazer a maioria das alterações na configuração de rede que foi inicialmente definida durante a implantação de grade. As alterações manuais usando comandos e arquivos de rede padrão do Linux podem não se propagar para todos os serviços do StorageGRID e podem não persistir em atualizações, reinicializações ou procedimentos de recuperação de nós.

Se você quiser alterar o endereço IP da rede de Grade para todos os nós da grade, use o procedimento especial para alterações em toda a grade.

"Alterar endereços IP para todos os nós na grade"

Se você estiver fazendo alterações somente na Lista de sub-redes de rede de Grade, use o Gerenciador de Grade para adicionar ou alterar a configuração da rede. Caso contrário, use a ferramenta alterar IP se o Gerenciador de Grade estiver inacessível devido a um problema de configuração de rede, ou você estiver executando uma alteração de roteamento de rede de Grade e outras alterações de rede ao mesmo tempo.

O procedimento de mudança de IP pode ser um procedimento disruptivo. Partes da grade podem estar indisponíveis até que a nova configuração seja aplicada.

- Interfaces Ethernet*

O endereço IP atribuído a eth0 é sempre o endereço IP da rede de Grade do nó da grade. O endereço IP

atribuído ao eth1 é sempre o endereço IP da rede Admin do nó da grade. O endereço IP atribuído ao eth2 é sempre o endereço IP da rede do cliente do nó da grade.

Observe que em algumas plataformas, como dispositivos StorageGRID, eth0, eth1 e eth2, podem ser interfaces agregadas compostas por bridges subordinadas ou ligações de interfaces físicas ou VLAN. Nessas plataformas, a guia **SSM** > **Resources** pode mostrar o endereço IP de rede Grid, Admin e Client 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)

- Não é possível alterar o endereço IP da rede do cliente fora da sub-rede de um grupo HA configurado na interface de rede do cliente.
- Não é possível alterar o endereço IP da rede do cliente para o valor de um endereço IP virtual existente atribuído por um grupo HA configurado na interface de rede do cliente.
- Não é possível alterar o endereço IP da rede da grade fora da sub-rede de um grupo HA configurado na interface de rede da grade.
- Não é possível alterar o endereço IP da rede Grid para o valor de um endereço IP virtual existente atribuído por um grupo HA configurado na interface de rede Grid.

Opções

- "Alterar a configuração de rede de um nó"
- "Adicionar ou alterar listas de sub-rede na rede Admin"
- "Adicionar ou alterar listas de sub-rede na rede de Grade"
- "Linux: Adicionando interfaces a um nó existente"
- "Alterar endereços IP para todos os nós na grade"

Alterando a configuração de rede de um nó

Você pode alterar a configuração de rede de um ou mais nós usando a ferramenta alterar IP. Você pode alterar a configuração da rede de Grade ou adicionar, alterar ou remover as redes Admin ou Client.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

- Linux:* se você estiver adicionando um nó de grade à rede Admin ou rede de cliente pela primeira vez, e você não tiver configurado anteriormente ADMIN_network_TARGET ou CLIENT_network_TARGET no arquivo de configuração do nó, você deve fazê-lo agora.

Consulte as instruções de instalação do StorageGRID para seu sistema operacional Linux.

Appliances: em appliances StorageGRID, se o cliente ou a rede de administração não tiver sido configurada

no Instalador de appliance StorageGRID durante a instalação inicial, a rede não poderá ser adicionada usando apenas a ferramenta Change IP (alterar IP). Primeiro, você deve colocar o aparelho no modo de manutenção, configurar os links, retornar o aparelho ao modo de operação normal e, em seguida, usar a ferramenta alterar IP para modificar a configuração de rede. Consulte o procedimento para configurar links de rede nas instruções de instalação e manutenção do seu aparelho.

Você pode alterar o endereço IP, a máscara de sub-rede, o gateway ou o valor MTU para um ou mais nós em qualquer rede.

Você também pode adicionar ou remover um nó de uma rede de cliente ou de uma rede de administração:

- Você pode adicionar um nó a uma rede cliente ou a uma rede Admin adicionando um endereço IP/máscara de sub-rede nessa rede ao nó.
- Você pode remover um nó de uma rede de cliente ou de uma rede de administrador excluindo o endereço IP/máscara de sub-rede do nó nessa rede.

  Os nós não podem ser removidos da rede de Grade.

> Swaps de endereço IP não são permitidos. Se for necessário trocar endereços IP entre nós de grade, você deverá usar um endereço IP intermediário temporário.

> Se o logon único (SSO) estiver ativado para o sistema StorageGRID e você estiver alterando o endereço IP de um nó Admin, esteja ciente de que qualquer confiança de parte confiável que foi configurada usando o endereço IP do nó Admin (em vez de seu nome de domínio totalmente qualificado, conforme recomendado) se tornará inválida. Você não poderá mais entrar no nó. Imediatamente após alterar o endereço IP, você deve atualizar ou reconfigurar a confiança de parte confiável do nó nos Serviços de Federação do ative Directory (AD FS) com o novo endereço IP. Consulte as instruções para administrar o StorageGRID.

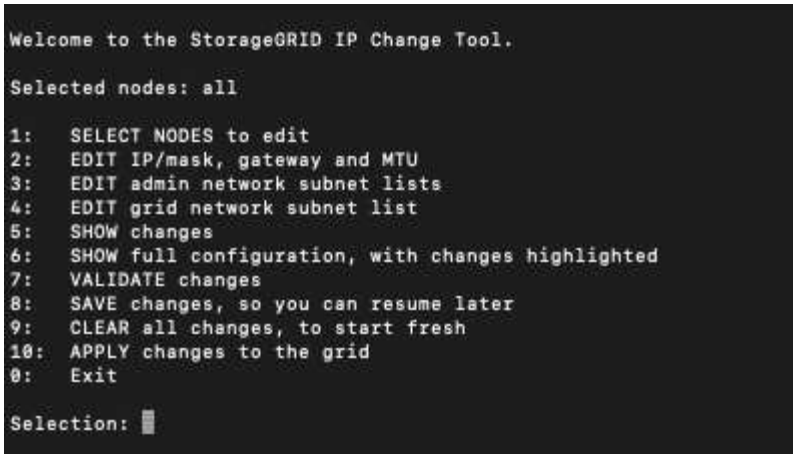
> Todas as alterações feitas na rede usando a ferramenta Change IP são propagadas para o firmware do instalador dos dispositivos StorageGRID. Dessa forma, se o software StorageGRID for reinstalado em um dispositivo ou se um dispositivo for colocado no modo de manutenção, a configuração de rede estará correta.

Passos

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

      Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
2. Inicie a ferramenta Change IP inserindo o seguinte comando: `change-ip`
3. Insira a senha de provisionamento no prompt.

   É apresentado o menu principal.



4. Opcionalmente, selecione **1** para escolher quais nós atualizar. Em seguida, selecione uma das seguintes opções:

   - **1**: Nó único — selecione pelo nome
   - **2**: Nó único — selecione por site e, em seguida, por nome
   - **3**: Nó único — selecione por IP atual
   - **4**: Todos os nós em um local
   - **5**: Todos os nós na grade

   Observação: se você quiser atualizar todos os nós, permita que "todos" permaneçam selecionados.

   Depois de fazer sua seleção, o menu principal é exibido, com o campo **Selected Nodes** atualizado para refletir sua escolha. Todas as ações subsequentes são realizadas apenas nos nós exibidos.

5. No menu principal, selecione a opção **2** para editar informações de IP/máscara, gateway e MTU para os nós selecionados.
   a. Selecione a rede onde deseja fazer alterações:

      - **1**: Rede de rede
      - **2**: Rede de administração
      - **3**: Rede de clientes
      - **4**: Todas as redes depois de selecionar, o prompt mostra o nome do nó, o nome da rede (Grade, Admin ou Cliente), o tipo de dados (IP/máscara, Gateway ou MTU) e o valor atual.

        Editar o endereço IP, o comprimento do prefixo, o gateway ou MTU de uma interface configurada por DHCP alterará a interface para estática. Quando você seleciona alterar uma interface configurada pelo DHCP, um aviso é exibido para informá-lo de que a interface mudará para estática.

      As interfaces configuradas como `fixed` não podem ser editadas.

   b. Para definir um novo valor, introduza-o no formato apresentado para o valor atual.
   c. Para deixar o valor atual inalterado, pressione **Enter**.
   d. Se o tipo de dados for `IP/mask`, você poderá excluir o Admin ou a rede do cliente do nó inserindo **d** ou **0,0.0,0/0**.

e. Depois de editar todos os nós que você deseja alterar, digite **q** para retornar ao menu principal.

   Suas alterações são mantidas até serem limpas ou aplicadas.

6. Reveja as alterações selecionando uma das seguintes opções:
   - **5**: Mostra edições na saída que são isoladas para mostrar apenas o item alterado. As alterações são realçadas em verde (adições) ou vermelho (exclusões), como mostrado na saída do exemplo:

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x 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.

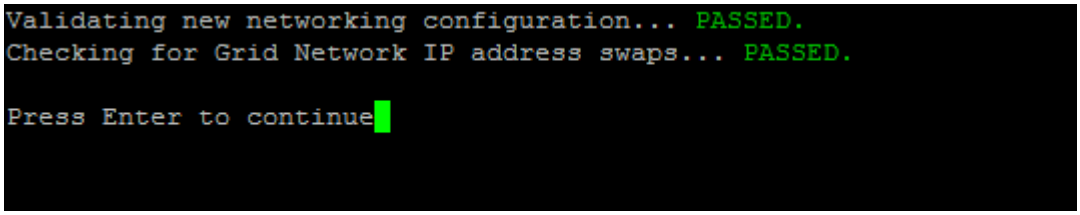
```
Validating new networking configuration... FAILED.

  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. Depois que a validação passar, escolha uma das seguintes opções:
   - **8**: Salve as alterações não aplicadas.

     Essa opção permite que você saia da ferramenta Change IP e inicie-a novamente mais tarde, sem perder nenhuma alteração não aplicada.

   - **10**: Aplicar a nova configuração de rede.
9. Se você selecionou a opção **10**, escolha uma das seguintes opções:
   - **Apply**: Aplique as alterações imediatamente e reinicie automaticamente cada nó, se necessário.

     Se a nova configuração de rede não exigir alterações físicas de rede, você pode selecionar **Apply** para aplicar as alterações imediatamente. Os nós serão reiniciados automaticamente, se necessário. Os nós que precisam ser reiniciados serão exibidos.

   - **Stage**: Aplique as alterações na próxima vez que os nós forem reiniciados manualmente.

     Se você precisar fazer alterações na configuração de rede física ou virtual para que a nova configuração de rede funcione, use a opção **stage**, encerre os nós afetados, faça as alterações de rede física necessárias e reinicie os nós afetados. Se você selecionar **Apply** sem primeiro fazer essas alterações de rede, as alterações geralmente falharão.

     > ⓘ Se você usar a opção **stage**, será necessário reiniciar o nó o mais rápido possível após o preparo para minimizar as interrupções.

   - **Cancelar**: Não faça alterações na rede neste momento.

     Se você não sabia que as alterações propostas exigem que os nós sejam reiniciados, você pode adiar as alterações para minimizar o 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 preparar alterações, um novo pacote de recuperação é gerado como resultado da

alteração da configuração da grade.

10. Se você selecionou **stage**, siga estas etapas após a conclusão do provisionamento:
    a. Faça as alterações de rede física ou virtual necessárias.
        - Alterações físicas de rede*: Faça as alterações físicas necessárias de rede, desligando o nó com segurança, se necessário.
        - Linux*: Se você estiver adicionando o nó a uma rede Admin ou rede de cliente pela primeira vez, certifique-se de que você adicionou a interface conforme descrito em ""adicionando interfaces a um nó existente".
    b. Reinicie os nós afetados.
11. Selecione **0** para sair da ferramenta Change IP após a conclusão das alterações.
12. Faça o download de um novo Pacote de recuperação do Gerenciador de Grade.
    a. Selecione **Manutenção** > **sistema** > **Pacote de recuperação**.
    b. Introduza a frase-passe de aprovisionamento.

Informações relacionadas

"Linux: Adicionando interfaces a um nó existente"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"Administrar o StorageGRID"

"Configurando endereços IP"

Adicionar ou alterar listas de sub-rede na rede Admin

Você pode adicionar, excluir ou alterar as sub-redes na Lista de sub-redes de rede Admin de um ou mais nós.

O que você vai precisar

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

Você pode adicionar, excluir ou alterar sub-redes para todos os nós na Lista de sub-redes de rede Admin.

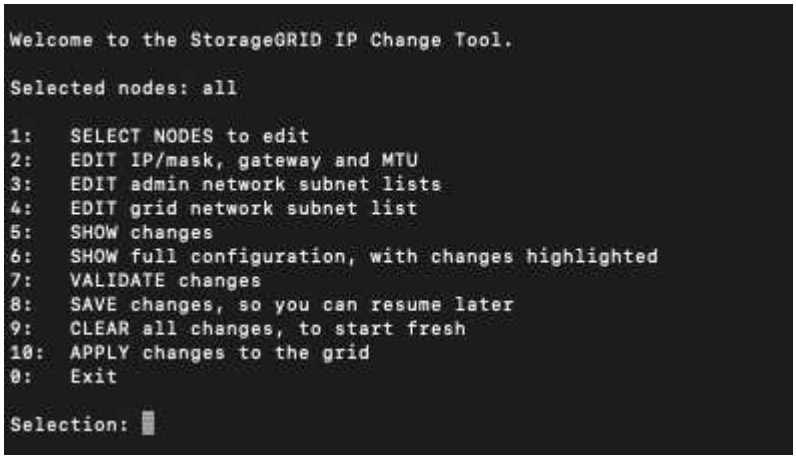
Passos

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

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

2. Inicie a ferramenta Change IP inserindo o seguinte comando: `change-ip`
3. Insira a senha de provisionamento no prompt.

   É apresentado o menu principal.



4. Opcionalmente, limite as redes/nós nos quais as operações são executadas. Escolha uma das seguintes opções:
   - Selecione os nós a editar escolhendo **1**, se você quiser filtrar em nós específicos nos quais executar a operação. Selecione uma das seguintes opções:
     - **1**: Nó único (selecionar pelo nome)
     - **2**: Nó único (selecione por site, depois pelo nome)
     - **3**: Nó único (selecionar por IP atual)
     - **4**: Todos os nós em um local
     - **5**: Todos os nós na grade
     - **0**: Volte
   - Permitir que "'all'" permaneça selecionado. Após a seleção ser feita, é apresentado o ecrã do menu principal. O campo nós selecionados reflete sua nova seleção e agora todas as operações selecionadas serão executadas somente neste item.
5. No menu principal, selecione a opção para editar sub-redes para a rede Admin (opção **3**).
6. Escolha uma das seguintes opções:
   - Adicione uma sub-rede inserindo este comando: `add CIDR`
   - Exclua uma sub-rede inserindo este comando: `del CIDR`
   - Defina a lista de sub-redes inserindo este comando: `set CIDR`

     Para todos os comandos, você pode inserir vários endereços usando este formato: `add CIDR, CIDR`

     Exemplo: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

Você pode reduzir a quantidade de digitação necessária usando "'seta para cima'" para recuperar valores digitados anteriormente para o prompt de entrada atual e, em seguida, editá-los, se necessário.

A entrada de exemplo abaixo mostra a adição de sub-redes à Lista de sub-redes de Admin Network:

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. Quando estiver pronto, digite **q** para voltar à tela do menu principal. Suas alterações são mantidas até serem limpas ou aplicadas.

Se você selecionou qualquer um dos modos de seleção de nó "todos" na etapa 2, você deve pressionar **Enter** (sem **q**) para chegar ao próximo nó na lista.

8. Escolha uma das seguintes opções:

   - Selecione a opção **5** para mostrar as edições na saída que estão isoladas para mostrar apenas o item alterado. As alterações são realçadas em verde (adições) ou vermelho (exclusões), como mostrado na saída de exemplo abaixo:

```
================================================================================
Site: Data Center 1
================================================================================
DC1-ADM1-105-154 Admin  Subnets                          add 172.17.0.0/16
                                                         del 172.16.0.0/16
                                [       172.14.0.0/16 ]
                                [       172.15.0.0/16 ]
                                [       172.17.0.0/16 ]
                                [       172.19.0.0/16 ]
                                [       172.20.0.0/16 ]
                                [       172.21.0.0/16 ]
Press Enter to continue
```

   - Selecione a opção **6** para mostrar as edições na saída que exibem a configuração completa. As alterações são realçadas em verde (adições) ou vermelho (exclusões). **Nota:** alguns emuladores de terminal podem mostrar adições e exclusões usando a formatação strikethrough.

     Quando você tenta alterar a lista de sub-redes, a seguinte mensagem é exibida:

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that are not
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
are not reachable using default StorageGRID routing, but are
reachable using a different interface and gateway. Making and
applying changes to the subnet list will make all automatically
applied subnets persistent. If you do not want that to happen, delete
the unwanted subnets before applying changes. If you know that all
/32 subnets in the list were added intentionally, you can ignore this
caution.
```

Se você não atribuiu especificamente as sub-redes de servidor NTP e DNS a uma rede, o StorageGRID cria uma rota de host (/32) para a conexão automaticamente. Se, por exemplo, você preferir ter uma rota /16 ou /24 para conexão de saída a um servidor DNS ou NTP, você deve excluir a rota /32 criada automaticamente e adicionar as rotas que deseja. Se você não excluir a rota de host criada automaticamente, ela será persistida depois de aplicar quaisquer alterações à lista de sub-redes.

Embora você possa usar essas rotas de host descobertas automaticamente, em geral, você deve configurar manualmente as rotas DNS e NTP para garantir a 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 seguinte saída de amostra:

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

12. Faça o download de um novo Pacote de recuperação do Gerenciador de Grade.

a. Selecione **Manutenção** > **sistema** > **Pacote de recuperação**.

b. Introduza a frase-passe de aprovisionamento.

Informações relacionadas

"Configurando endereços IP"

Adicionar ou alterar listas de sub-rede na rede de Grade

Você pode usar a ferramenta alterar IP para adicionar ou alterar sub-redes na rede de Grade.

O que você vai precisar

- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

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.

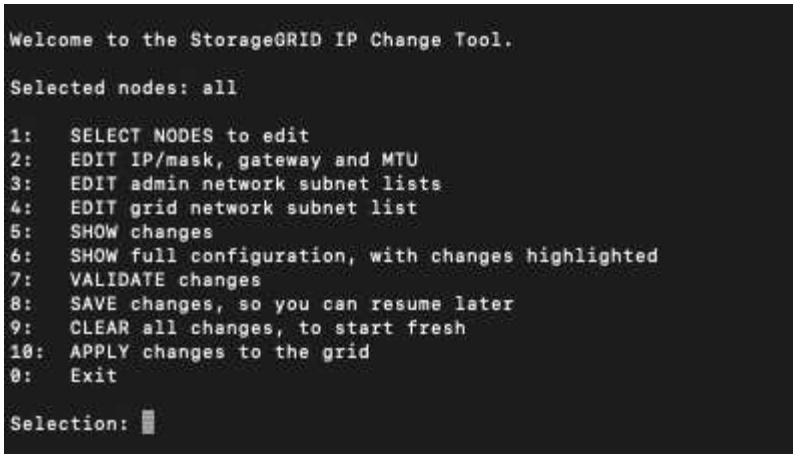
> Se você estiver fazendo alterações somente na Lista de sub-redes de rede de Grade, use o Gerenciador de Grade para adicionar ou alterar a configuração da rede. Caso contrário, use a ferramenta alterar IP se o Gerenciador de Grade estiver inacessível devido a um problema de configuração de rede, ou 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.



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:

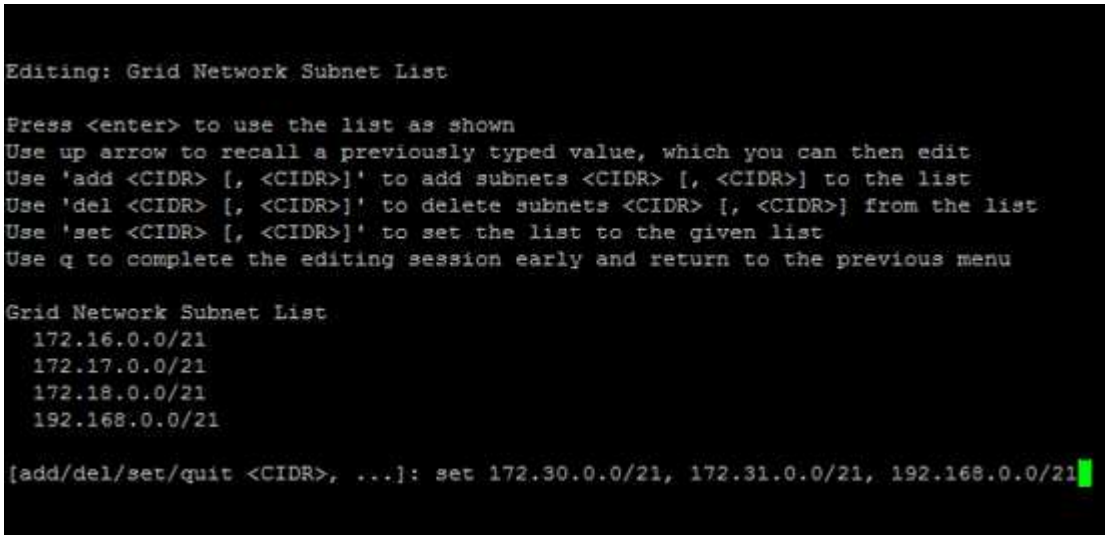
   - Adicione uma sub-rede inserindo este comando: `add CIDR`
   - Exclua uma sub-rede inserindo este comando: `del CIDR`
   - Defina a lista de sub-redes inserindo este comando: `set CIDR`

> Para todos os comandos, você pode inserir vários endereços usando este formato: `add CIDR, CIDR`

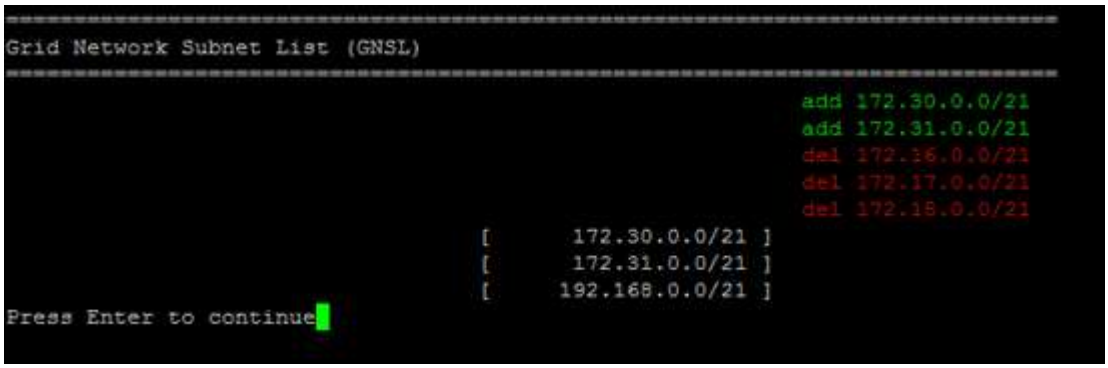
   Exemplo: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

> 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:



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 seguinte saída de amostra:

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

11. Se você selecionou a opção **10** ao fazer alterações na rede de Grade, selecione uma das seguintes opções:

- **Apply**: Aplique as alterações imediatamente e reinicie automaticamente cada nó, se necessário.

  Se a nova configuração de rede funcionar simultaneamente com a configuração de rede antiga sem alterações externas, você pode usar a opção **Apply** para uma alteração de configuração totalmente automatizada.

- **Stage**: Aplique as alterações na próxima vez que os nós forem reiniciados.

  Se você precisar fazer alterações na configuração de rede física ou virtual para que a nova configuração de rede funcione, use a opção **stage**, encerre os nós afetados, faça as alterações de rede física necessárias e reinicie os nós afetados.

  > Se você usar a opção **stage**, será necessário reiniciar o nó o mais rápido possível após o preparo para minimizar as interrupções.

- **Cancelar**: Não faça alterações na rede neste momento.

  Se você não sabia que as alterações propostas exigem que os nós sejam reiniciados, você pode adiar as alterações para minimizar o impactos do usuário. Selecionar **CANCEL** retorna ao menu principal e preserva as alterações para que você possa aplicá-las mais tarde.

Depois de aplicar ou preparar alterações, um novo pacote de recuperação é gerado como resultado da alteração da configuração da grade.

12. Se a configuração for interrompida devido a erros, as seguintes opções estarão disponíveis:
    - Para cancelar o procedimento de alteração de IP e regressar ao menu principal, introduza **a**.
    - Para tentar novamente a operação que falhou, digite **r**.
    - Para continuar para a próxima operação, digite **c**.

      A operação com falha pode ser tentada mais tarde selecionando a opção **10** (aplicar alterações) no menu principal. O procedimento de alteração de IP não será concluído até que todas as operações tenham sido concluídas com êxito.

    - Se você teve que intervir manualmente (para reinicializar um nó, por exemplo) e está confiante de que a ação que a ferramenta acha que falhou foi realmente concluída com sucesso, digite **f** para marcá-lo como bem-sucedido e passar para a próxima operação.
13. Faça o download de um novo Pacote de recuperação do Gerenciador de Grade.
    a. Selecione **Manutenção** > **sistema** > **Pacote de recuperação**.
    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.

Informações relacionadas

"Configurando endereços IP"

Linux: Adicionando interfaces a um nó existente

Se você quiser adicionar uma interface a um nó baseado em Linux que você não instalou inicialmente, você deve usar este procedimento.

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 de instalação do StorageGRID para seu sistema operacional Linux.

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Você executa este procedimento no servidor Linux que hospeda o nó que precisa da nova atribuição de rede, não dentro do nó. Este procedimento adiciona apenas a interface ao nó; ocorre um erro de validação se tentar especificar quaisquer outros parâmetros de rede.

Para fornecer informações de endereçamento, você deve usar a ferramenta alterar IP. Consulte as informações sobre como alterar a configuração de rede de um nó.

"Alterar a configuração de rede de um nó"

Passos

1. Faça login no servidor Linux que hospeda o nó que precisa da nova atribuição de rede.
2. Edite o arquivo de configuração do nó em `/etc/storagegrid/nodes/node-name.conf`.

   Não especifique quaisquer outros parâmetros de rede, ou um erro de validação resultará.

   a. Adicione o novo destino de rede.

   ```
   CLIENT_NETWORK_TARGET = bond0.3206
   ```

   b. Opcional: Adicione um endereço MAC.

   ```
   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`

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

"Alterar a configuração de rede de um nó"

Alterar endereços IP para todos os nós na grade

Se você precisar alterar o endereço IP da rede de Grade para todos os nós da grade, siga este procedimento especial. Você não pode fazer uma alteração de IP de rede de grade em toda a grade usando o procedimento para alterar nós individuais.

O que você vai precisar

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

Sobre esta tarefa

Para garantir que a grade seja iniciada com sucesso, você deve fazer todas as alterações de uma vez.

> Este procedimento aplica-se apenas à rede de grelha. Não é possível usar este procedimento para alterar endereços IP nas redes Admin ou Client.

Se você quiser alterar os endereços IP e MTU para os nós apenas em um local, siga as instruções para alterar a configuração de rede de um nó.

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. Consulte as instruções para administrar o StorageGRID.

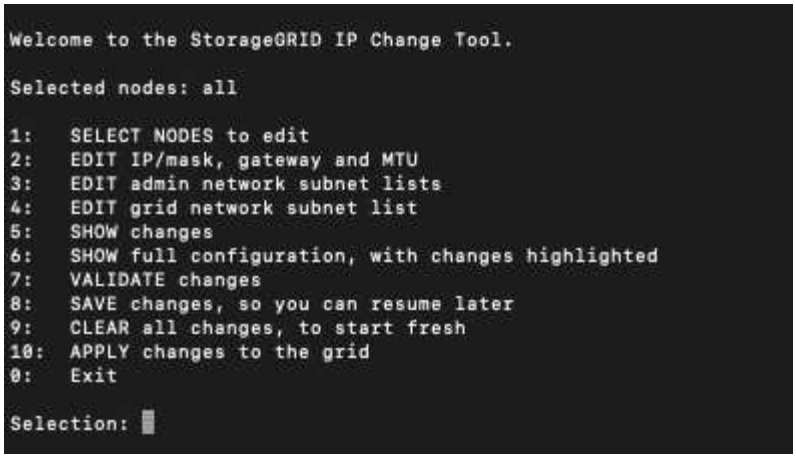
   > Se necessário, adicione a nova sub-rede para os novos endereços IP.

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

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

3. Inicie a ferramenta Change IP inserindo o seguinte comando: `change-ip`
4. Insira a senha de provisionamento no prompt.

É apresentado o menu principal. Por padrão, o `Selected nodes` campo é definido como `all`.



5. No menu principal, selecione **2** para editar informações sobre máscara de IP/sub-rede, gateway e MTU para todos os nós.

   a. Selecione **1** para fazer alterações na rede de Grade.

      Depois de fazer a seleção, o prompt mostra os nomes dos nós, o nome da rede da grade, o tipo de dados (IP/máscara, Gateway ou MTU) e os valores atuais.

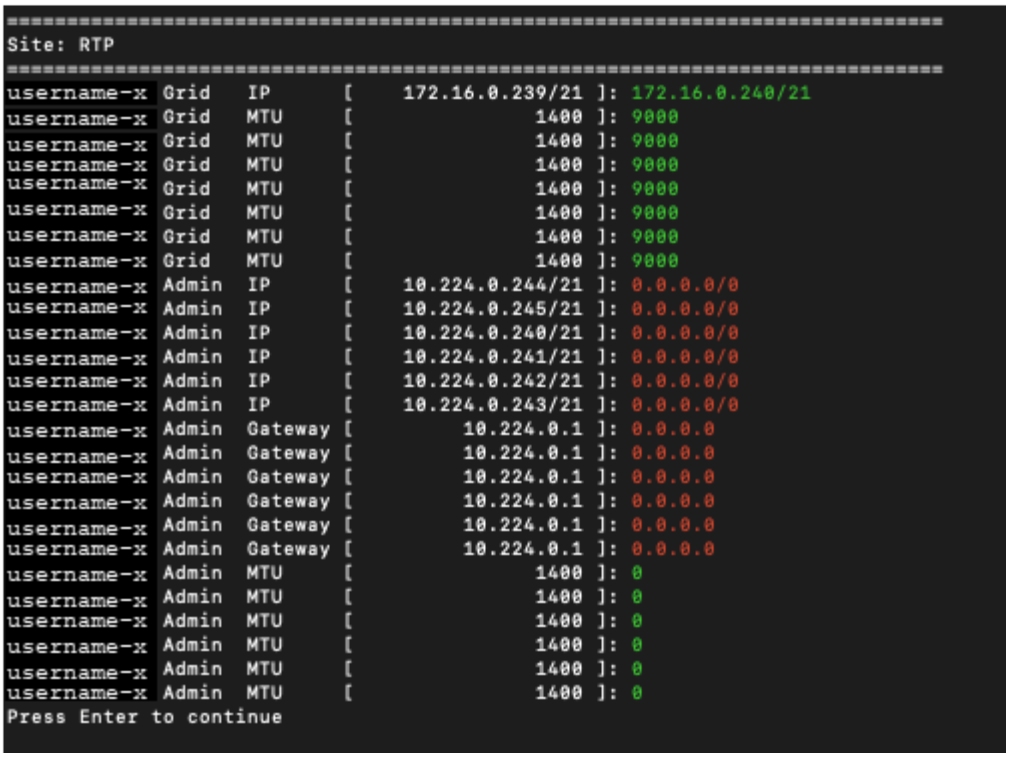
      Editar o endereço IP, o comprimento do prefixo, o gateway ou MTU de uma interface configurada por DHCP alterará a interface para estática. É apresentado um aviso antes de cada interface configurada pelo DHCP.

   As interfaces configuradas como `fixed` não podem ser editadas.

   a. Para definir um novo valor, introduza-o no formato apresentado para o valor atual.
   b. Depois de editar todos os nós que você deseja alterar, digite **q** para retornar ao menu principal.

      Suas alterações são mantidas até serem limpas ou aplicadas.

6. Reveja as alterações selecionando uma das seguintes opções:
   - **5**: Mostra edições na saída que são isoladas para mostrar apenas o item alterado. As alterações são realçadas em verde (adições) ou vermelho (exclusões), como mostrado na saída do exemplo:



- **6**: Mostra edições na saída que exibe a configuração completa. As alterações são realçadas em verde (adições) ou vermelho (exclusões).

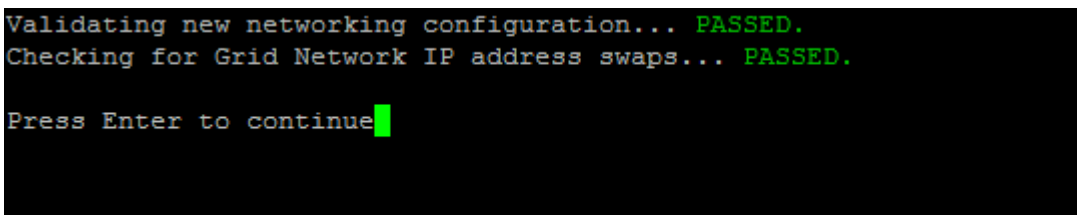
> Certas interfaces de linha de comando podem mostrar adições e exclusões usando a formatação strikethrough. A exibição adequada depende do cliente terminal que suporta as sequências de escape VT100 necessárias.

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. Quando a validação passar, 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 um reinício contínuo, 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 uma só vez, 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. Assim 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 **Manutenção** > **sistema** > **Pacote de recuperação**.
    b. Introduza a frase-passe de aprovisionamento.

Informações relacionadas

"Administrar o StorageGRID"

"Alterar a configuração de rede de um nó"

"Adicionar ou alterar listas de sub-rede na rede de Grade"

"Fechando um nó de grade"

Configurando servidores DNS

Você pode adicionar, remover e atualizar servidores DNS (sistema de nomes de domínio), para que você possa usar nomes de host FQDN (nome de domínio totalmente qualificado) em vez de endereços IP.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter os endereços IP dos servidores DNS para configurar.

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 ou SNMP e AutoSupport. É recomendável especificar pelo menos dois servidores DNS.

Forneça entre dois a seis endereços IP para servidores DNS. Em geral, selecione servidores DNS que cada site pode acessar localmente no caso de a rede ser aterrissada. Isso é para garantir que um site islanded continua a ter acesso ao serviço DNS. Depois de configurar a lista de servidores DNS em toda a grade, você pode personalizar ainda mais a lista de servidores DNS para cada nó.

"Modificação da configuração DNS para um único nó de grade"

Se as informações do servidor DNS forem omitidas ou configuradas incorretamente, um alarme DNST será acionado no serviço SSM de cada nó da grade. O alarme é apagado quando o DNS está configurado corretamente e as novas informações do servidor atingiram todos os nós da grade.

Passos

1. Selecione **Manutenção** > **rede** > **servidores DNS**.
2. Na seção servidores, adicione atualizações ou remova entradas do servidor DNS, conforme necessário.

   A prática recomendada é especificar pelo menos dois servidores DNS por site. Você pode especificar até seis servidores DNS.

3. Clique em **Salvar**.

Modificação da configuração DNS para um único nó de grade

Em vez de configurar o DNS (Domain Name System) globalmente para toda a implantação, você pode executar um script para configurar o DNS de forma diferente para cada nó de grade.

Em geral, você deve usar a opção **Manutenção rede servidores DNS** no Gerenciador de Grade para configurar servidores DNS. Use o script a seguir somente se você precisar usar servidores DNS diferentes para diferentes nós de grade.

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

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

   e. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`
   f. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
2. Faça login no nó que deseja atualizar com uma configuração DNS personalizada: `ssh node_IP_address`
3. Execute o script de configuração DNS: `setup_resolv.rb`.

   O script responde com a lista de comandos suportados.

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. Adicione o endereço IPv4 de um servidor que fornece serviço de nome de domínio para sua rede: `add <nameserver IP_address>`
5. Repita o `add nameserver` comando para adicionar servidores de nomes.
6. Siga as instruções conforme solicitado para outros comandos.
7. Salve suas alterações e saia do aplicativo: `save`
8. feche o shell de comando no servidor: `exit`
9. Para cada nó de grade, repita as etapas de iniciar sessão no nó até fechando o shell de comando.
10. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do

agente SSH. Introduza: `ssh-add -D`

Configurando servidores NTP

Você pode adicionar, atualizar ou remover servidores NTP (Network Time Protocol) para garantir que os dados sejam sincronizados com precisão entre nós de grade em seu sistema StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter os endereços IPv4 dos servidores NTP para configurar.

Sobre esta tarefa

O sistema StorageGRID usa o protocolo de tempo de rede (NTP) para sincronizar o tempo entre todos os nós de grade na grade.

Em cada local, pelo menos dois nós no sistema StorageGRID recebem a função NTP principal. Eles sincronizam com um mínimo sugerido de quatro, e um máximo de seis, fontes de tempo externas e entre si. Cada nó no sistema StorageGRID que não é um nó NTP primário atua como um cliente NTP e sincroniza com esses nós NTP primários.

Os servidores NTP externos 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, como o StorageGRID.

"Limite de suporte para configurar o serviço de tempo do Windows para ambientes de alta precisão"

Se você encontrar problemas com a estabilidade ou disponibilidade dos servidores NTP originalmente especificados durante a instalação, você pode atualizar a lista de fontes NTP externas que o sistema StorageGRID usa adicionando servidores adicionais ou atualizando ou removendo servidores existentes.

Passos

1. Selecione **Manutenção** > **rede** > **servidores NTP**.
2. Na seção servidores, adicione atualizações ou remova entradas do servidor NTP, conforme necessário.

   Você deve incluir pelo menos 4 servidores NTP e pode especificar até 6 servidores.

3. Na caixa de texto **frase-passe de aprovisionamento**, introduza a frase-passe de aprovisionamento do sistema StorageGRID e clique em **Guardar**.

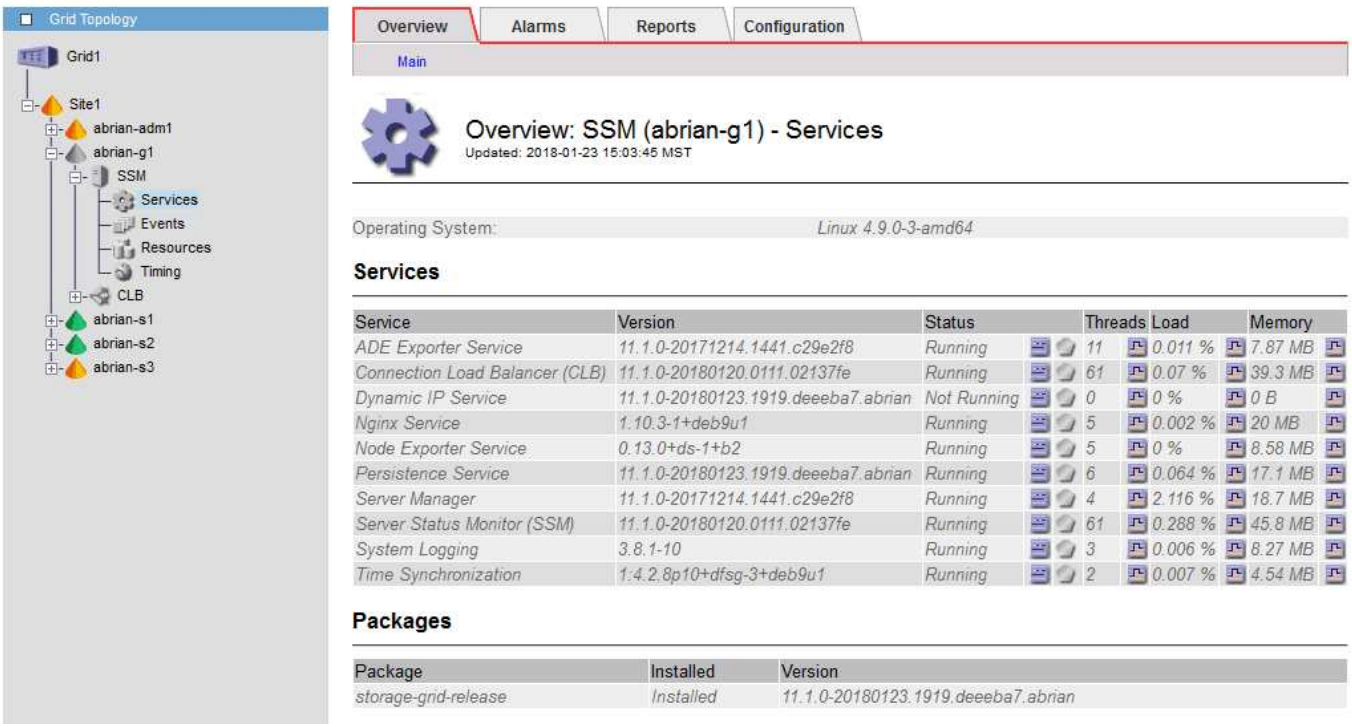
   O estado do procedimento é apresentado na parte superior da página. A página é desativada até que as atualizações de configuração estejam concluídas.

> Se todos os seus servidores NTP falharem no teste de conexão depois de salvar os novos servidores NTP, não prossiga. Entre em Contato com o suporte técnico.

Restaurar a conetividade de rede para nós isolados

Em certas circunstâncias, como alterações de endereço IP em todo o site ou grade, um ou mais grupos de nós podem não ser capazes de entrar em Contato com o resto da grade.

No Gerenciador de Grade (**suporte Ferramentas topologia de Grade**), se um nó estiver cinza ou se um nó estiver azul com muitos de seus serviços mostrando um status diferente de execução, você deve verificar o isolamento do nó.



Algumas das consequências de ter nós isolados incluem o seguinte:

- Se vários nós estiverem isolados, talvez você não consiga entrar ou acessar o Gerenciador de Grade.
- Se vários nós estiverem isolados, o uso do storage e os valores de cota mostrados no Dashboard do Tenant Manager podem estar desatualizados. Os totais serão atualizados quando a 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, o utilitário de linha de comando pode ter de ser executado em cada nó isolado.

Passos

1. Acesse o nó e `/var/local/log/dynip.log` verifique se há mensagens de isolamento.

   Por exemplo:

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action may be required.
   ```

   Se você estiver usando o console VMware, ele conterá uma mensagem informando que o nó pode estar isolado.

   Nas implantações Linux, as mensagens de isolamento aparecerão nos `/var/log/storagegrid/node/<nodename>.log` arquivos.

2. Se as mensagens de isolamento forem recorrentes e persistentes, execute o seguinte comando:

   `add_node_ip.py <address\>`

   `<address\>`Onde está o endereço IP de um nó remoto que está conetado à grade.

   ```
   # /usr/sbin/add_node_ip.py  10.224.4.210

   Retrieving local host information
   Validating remote node at address 10.224.4.210
   Sending node IP hint for 10.224.4.210 to local node
   Local node found on remote node. Update complete.
   ```

3. Verifique o seguinte para cada nó que foi isolado anteriormente:
   - Os serviços do nó foram iniciados.
   - O status do serviço IP dinâmico é "em execução" depois de executar o `storagegrid-status` comando.
   - Na árvore topologia de Grade, o nó não aparece mais desconetado do resto da grade.

Se a execução do `add_node_ip.py` comando não resolver o problema, pode haver outros problemas de rede que precisam ser resolvidos.

Procedimentos de nível de host e middleware

Alguns procedimentos de manutenção são específicos para implantações Linux ou

VMware do StorageGRID, ou são específicos para outros componentes da solução StorageGRID.

Linux: Migrando um nó de grade para um novo host

Você pode migrar os nós do StorageGRID de um host Linux para outro para executar a manutenção do host (como patches e reinicialização do sistema operacional) sem afetar a funcionalidade ou a disponibilidade da sua grade.

Você migra um ou mais nós de um host Linux (o "host de origem") para outro host Linux (o "host de destino"). O host de destino deve ter sido preparado anteriormente para uso no StorageGRID.

> Você pode usar este procedimento somente se você planejou sua implantação do StorageGRID para incluir suporte à migração.

Para migrar um nó de grade para um novo host, ambas as condições a seguir devem ser verdadeiras:

- O storage compartilhado é usado para todos os volumes de storage por nó
- As interfaces de rede têm nomes consistentes entre os hosts

> Em uma implantação de produção, não execute mais de um nó de storage em um único host. O uso de um host dedicado para cada nó de storage fornece um domínio de falha isolado.

Outros tipos de nós, como nós de administração ou nós de gateway, podem ser implantados no mesmo host. No entanto, se você tiver vários nós do mesmo tipo (dois nós de Gateway, por exemplo), não instale todas as instâncias no mesmo host.

Para obter mais informações, consulte "requisitos de migração de nós" nas instruções de instalação do StorageGRID para o seu sistema operacional Linux.

Informações relacionadas

"Implantando novos hosts Linux"

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Linux: Exportando o nó do host de origem

Encerre o nó da grade e exporte-o do host Linux de origem.

Execute o seguinte comando no host Linux de origem.

1. Obtenha o status de todos os nós atualmente em execução no host de origem.

```
sudo storagegrid node status all
```

```
Name Config-State Run-State

DC1-ADM1 Configured Running
```

```
DC1-ARC1 Configured Running

DC1-GW1 Configured Running

DC1-S1 Configured Running

DC1-S2 Configured Running

DC1-S3 Configured Running
```

2. Identifique o nome do nó que deseja migrar e pare-o se o estado de execução for `Running`.

```
sudo storagegrid node stop DC1-S3
```

```
Stopping node DC1-S3

Waiting up to 630 seconds for node shutdown
```

3. Exporte o nó do host de origem.

```
sudo storagegrid node export DC1-S3
```

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.

Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you

want to import it again.
```

4. Tome nota `import command suggested in the output of the `export` do comando.

   Você executará esse comando no host de destino na próxima etapa.

Linux: Importando o nó no host de destino

Depois de exportar o nó do host de origem, você importa e valida o nó no host Linux de destino. A validação confirma que o nó tem acesso aos mesmos dispositivos de interface de rede e armazenamento de bloco que tinha no host de origem.

Execute o seguinte comando no host Linux de destino.

1. Importe o nó no host de destino.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.

You should run 'storagegrid node validate DC1-S3'
```

2. Valide a configuração do nó no novo host.

```
sudo storagegrid node validate DC1-S3
```

```
Confirming existence of node DC1-S3... PASSED

Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node DC1-
S3... PASSED

Checking for duplication of unique values... PASSED
```

3. Se ocorrerem erros de validação, solucione-os antes de iniciar o nó migrado.

   Para obter informações sobre solução de problemas, consulte as instruções de instalação do StorageGRID para seu sistema operacional Linux.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale Ubuntu ou Debian"

Linux: Iniciando o nó migrado

Depois de validar o nó migrado, você inicia o nó executando um comando no host Linux de destino.

Passos

1. Inicie o nó no novo host.

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. No Gerenciador de Grade, verifique se o status do nó está verde sem alarmes levantados contra ele.

   Verificar se o status do nó está verde garante que o nó migrado tenha reiniciado e se juntado novamente à grade. Se o status não estiver verde, não migre nenhum nó adicional para que você não tenha mais de um nó fora de serviço.

   Se você não conseguir acessar o Gerenciador de Grade, aguarde 10 minutos e execute o seguinte comando:

   ```
   sudo storagegrid node status node-name
   ```

   Confirme se o nó migrado tem um Estado de execução de `Running`.

Manutenção do Archive Node para middleware TSM

Os nós de arquivamento podem ser configurados para direcionar a fita por meio de um

servidor middleware TSM ou a nuvem por meio da API S3. Uma vez configurado, o destino de um nó de arquivo não pode ser alterado.

Se o servidor que hospeda o nó de arquivo falhar, substitua o servidor e siga o procedimento de recuperação apropriado.

Falha com dispositivos de armazenamento de arquivo

Se você determinar que há uma falha no dispositivo de armazenamento de arquivos que o nó de arquivamento está acessando por meio do Gerenciador de armazenamento Tivoli (TSM), coloque o nó de arquivamento off-line para limitar o número de alarmes exibidos no sistema StorageGRID. Em seguida, você pode usar as ferramentas administrativas do servidor TSM ou do dispositivo de armazenamento, ou ambos, para diagnosticar e resolver o problema.

Colocar o componente alvo offline

Antes de realizar qualquer manutenção do servidor de middleware TSM que possa resultar na indisponibilidade do Archive Node, coloque o componente Target offline para limitar o número de alarmes que são acionados se o servidor de middleware TSM ficar indisponível.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione **Archive Node** > **ARC** > **Target** > **Configuration** > **Main**.
3. Altere o valor do Tivoli Storage Manager State para **Offline** e clique em **Apply Changes**.
4. Após a conclusão da manutenção, altere o valor do Tivoli Storage Manager State para **Online** e clique em **Apply Changes**.

Ferramentas administrativas do Tivoli Storage Manager

A ferramenta dsmadmc é o console administrativo do servidor de middleware TSM que está instalado no nó de Arquivo. Você pode acessar a ferramenta digitando `dsmadmc` na linha de comando do servidor. Faça login no console administrativo usando o mesmo nome de usuário administrativo e senha configurados para o serviço ARC.

O `tsmquery.rb` script foi criado para gerar informações de status do dsmadmc de forma mais legível. Você pode executar este script inserindo o seguinte comando na linha de comando do nó de Arquivo: `/usr/local/arc/tsmquery.rb status`

Para obter mais informações sobre o console administrativo do TSM dsmadmc, consulte *Tivoli Storage Manager for Linux: Administrators Reference*.

Objeto permanentemente indisponível

Quando o Archive Node solicita um objeto do servidor Tivoli Storage Manager (TSM) e a recuperação falha, o Archive Node tenta novamente a solicitação após um intervalo de 10 segundos. Se o objeto estiver permanentemente indisponível (por exemplo, porque o objeto está corrompido na fita), a API TSM não tem como indicar isso para o nó de arquivo, portanto, o nó de arquivo continua a tentar novamente a solicitação.

Quando esta situação ocorre, um alarme é acionado e o valor continua a aumentar. Para ver o alarme, selecione **Support** > **Tools** > **Grid Topology**. Em seguida, selecione **Archive Node** > **ARC** > **Retrieve** >

Request Failures.

Se o objeto estiver permanentemente indisponível, você deverá identificar o objeto e cancelar manualmente a solicitação do nó de arquivo conforme descrito no procedimento, Determinar se os objetos estão permanentemente indisponíveis.

Uma recuperação também pode falhar se o objeto estiver temporariamente indisponível. Neste caso, as solicitações de recuperação subsequentes devem eventualmente ser bem-sucedidas.

Se o sistema StorageGRID estiver configurado para usar uma regra ILM que cria uma cópia de objeto único e essa cópia não puder ser recuperada, o objeto será perdido e não poderá ser recuperado. No entanto, você ainda deve seguir o procedimento para determinar se o objeto está permanentemente indisponível para "limpar" o sistema StorageGRID, para cancelar a solicitação do nó de Arquivo e para purgar metadados para o objeto perdido.

Determinar se os objetos estão permanentemente indisponíveis

Você pode determinar se os objetos estão permanentemente indisponíveis fazendo uma solicitação usando o console administrativo do TSM.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Sobre esta tarefa

Este exemplo é fornecido apenas para suas informações; este procedimento não pode ajudá-lo a identificar todas as condições de falha que podem resultar em objetos indisponíveis ou volumes de fita. Para obter informações sobre a administração do TSM, consulte a documentação do TSM Server.

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Identifique o objeto ou objetos que não puderam ser recuperados pelo nó de arquivo:
   a. Vá para o diretório que contém os arquivos de log de auditoria: `cd /var/local/audit/export`

      O arquivo de log de auditoria ativo é chamado audit.log. Uma vez por dia, o arquivo ativo `audit.log` é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato `yyyy-mm-dd.txt`. Após um dia, o arquivo salvo é compactado e renomeado, no formato `yyyy-mm-dd.txt.gz`, que preserva a data original.

   b. Procure no ficheiro de registo de auditoria relevante mensagens que indiquem que não foi possível obter um objeto arquivado. Por exemplo, digite: `grep ARCE audit.log | less -n`

      Quando um objeto não pode ser recuperado de um nó de arquivo, a mensagem de AUDITORIA ARCE (Archive Object Retrieve End) exibe ARUN (archive middleware unavailable) ou GERR (erro geral) no campo de resultados. A linha de exemplo a seguir do log de auditoria mostra que a mensagem ARCE terminou com a EXECUÇÃO de resultado para CBID 498D8A1F681F05B3.

```
[AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
):ARUN][AVER(UI32):7]
[ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
MID(FC32):ARCI]
[ATID(UI64):4560349751312520631]]
```

Para obter mais informações, consulte as instruções para entender as mensagens de auditoria.

c. Registre o CBID de cada objeto que teve uma falha de solicitação.

Você também pode querer gravar as seguintes informações adicionais usadas pelo TSM para identificar objetos salvos pelo nó de arquivo:

- **Nome do espaço de arquivo**: Equivalente ao ID do nó de arquivo. Para encontrar a ID do nó de arquivo, selecione **suporte** > **Ferramentas** > **topologia de grade**. Em seguida, selecione **Archive Node** > **ARC** > **Target** > **Overview**.
- **Nome de alto nível**: Equivalente ao ID de volume atribuído ao objeto pelo nó de arquivo. O ID do volume assume a forma de uma data (por exemplo, `20091127`) e é gravado como o VLID do objeto em mensagens de auditoria de arquivo.
- **Nome de nível baixo**: Equivalente ao CBID atribuído a um objeto pelo sistema StorageGRID.

d. Faça logout do shell de comando: `exit`

3. Verifique o servidor TSM para ver se os objetos identificados na etapa 2 estão permanentemente indisponíveis:

a. Faça login no console administrativo do servidor TSM: `dsmadmc`

Use o nome de usuário administrativo e a senha configurados para o serviço ARC. Introduza o nome de utilizador e a palavra-passe no Gestor de grelha. (Para ver o nome de utilizador, selecione **Support** > **Tools** > **Grid Topology**. Em seguida, selecione **Archive Node** > **ARC** > **Target** > **Configuration**.)

b. Determine se o objeto está permanentemente indisponível.

Por exemplo, você pode pesquisar no log de atividade do TSM um erro de integridade de dados para esse objeto. O exemplo a seguir mostra uma pesquisa do log de atividades para o dia passado para um objeto com CBID . `498D8A1F681F05B3`

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

Dependendo da natureza do erro, o CBID pode não ser registrado no log de atividades do TSM. Talvez seja necessário pesquisar no log outros erros do TSM no momento da falha da solicitação.

c. Se uma fita inteira estiver permanentemente indisponível, identifique os CBIDs para todos os objetos armazenados nesse volume: `query content TSM_Volume_Name`

`TSM_Volume_Name`Onde está o nome TSM para a fita indisponível. O seguinte é um exemplo da saída para este comando:

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- ----------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

O `Client's Name for File Name` é o mesmo que o ID do volume do nó de arquivo (ou TSM ""nome de alto nível"") seguido pelo CBID do objeto (ou TSM ""nome de baixo nível""). Ou seja, o `Client's Name for File Name` toma a forma `/Archive Node volume ID /CBID`. Na primeira linha da saída de exemplo, o `Client's Name for File Name` é `/20081201/ C1D172940E6C7E12`.

Lembre-se também de que o `Filespace` é o ID do nó do nó de arquivo.

Você precisará do CBID de cada objeto armazenado no volume e do ID do nó do nó de arquivo para cancelar a solicitação de recuperação.

4. Para cada objeto que está permanentemente indisponível, cancele a solicitação de recuperação e emita um comando para informar o sistema StorageGRID de que a cópia do objeto foi perdida:

> Use o console ADE com cuidado. Se o console for usado incorretamente, é possível interromper as operações do sistema e corromper os dados. Introduza os comandos cuidadosamente e utilize apenas os comandos documentados neste procedimento.

a. Se você ainda não estiver conetado ao nó de arquivamento, faça login da seguinte forma:
   i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   iii. Digite o seguinte comando para mudar para root: `su -`
   iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
b. Aceda à consola ADE do serviço ARC: `telnet localhost 1409`
c. Cancelar a solicitação para o objeto: `/proc/BRTR/cancel -c CBID`

`CBID`Onde está o identificador do objeto que não pode ser recuperado do TSM.

Se as únicas cópias do objeto estiverem em fita, a solicitação de "recuperação em massa" será cancelada com uma mensagem "'1 solicitações canceladas". Se houver cópias do objeto em outro

lugar do sistema, a recuperação do objeto é processada por um módulo diferente, de modo que a resposta à mensagem seja "'0 solicitações canceladas".

d. Emita um comando para notificar o sistema StorageGRID de que uma cópia de objeto foi perdida e que uma cópia adicional deve ser feita: `/proc/CMSI/Object_Lost CBID node_ID`

```
`CBID`Onde está o identificador do objeto que não pode ser recuperado do servidor TSM `node_ID` e é o ID do nó do nó de arquivo onde a recuperação falhou.
```

Você deve inserir um comando separado para cada cópia de objeto perdido: Inserir um intervalo de CBIDs não é suportado.

Na maioria dos casos, o sistema StorageGRID começa imediatamente a fazer cópias adicionais de dados de objeto para garantir que a política de ILM do sistema seja seguida.

No entanto, se a regra ILM para o objeto especificar que apenas uma cópia será feita e essa cópia agora foi perdida, o objeto não pode ser recuperado. Nesse caso, executar o `Object_Lost` comando limpa os metadados do objeto perdido do sistema StorageGRID.

Quando o `Object_Lost` comando for concluído com êxito, a seguinte mensagem é retornada:

```
CLOC_LOST_ANS returned result 'SUCS'
```

+

> O `/proc/CMSI/Object_Lost` comando só é válido para objetos perdidos que são armazenados em nós de arquivo.

a. Saia da consola ADE: `exit`

b. Terminar sessão no nó de arquivo: `exit`

5. Repor o valor de falhas de pedido no sistema StorageGRID:

a. Aceda a **Archive Node** > **ARC** > **Retrieve** > **Configuration** e selecione **Reset Request Failure Count**.

b. Clique em **aplicar alterações**.

Informações relacionadas

"Administrar o StorageGRID"

"Rever registos de auditoria"

VMware: Configurando uma máquina virtual para reinicialização automática

Se a máquina virtual não reiniciar depois que o VMware vSphere Hypervisor for reiniciado, talvez seja necessário configurar a máquina virtual para reinicialização automática.

Você deve executar este procedimento se notar que uma máquina virtual não reinicia enquanto estiver recuperando um nó de grade ou executando outro procedimento de manutenção.

Passos

1. Na árvore Cliente do VMware vSphere, selecione a máquina virtual que não foi iniciada.
2. Clique com o botão direito do rato na máquina virtual e selecione **ligar**.
3. Configure o VMware vSphere Hypervisor para reiniciar a máquina virtual automaticamente no futuro.

Procedimentos do nó de grade

Talvez seja necessário executar procedimentos em um nó de grade específico. Embora você possa executar alguns desses procedimentos no Gerenciador de Grade, a maioria dos procedimentos exige que você acesse o Gerenciador de servidor a partir da linha de comando do nó.

O Gerenciador de servidores é executado em cada nó de grade para supervisionar o início e a parada dos serviços e garantir que os serviços se juntem e saiam do sistema StorageGRID. O Gerenciador de servidores também monitora os serviços em cada nó de grade e tentará reiniciar automaticamente quaisquer serviços que relatem falhas.

Você deve acessar o Server Manager somente se o suporte técnico o tiver direcionado para isso.

Você deve fechar a sessão de shell de comando atual e fazer logout depois de terminar com o Gerenciador de servidor. Introduza: `exit`

Opções

- "Exibindo o status e a versão do Server Manager"
- "Exibindo o status atual de todos os serviços"
- "Iniciando o Server Manager e todos os serviços"
- "Reiniciando o Gerenciador de servidores e todos os serviços"
- "Parar o Gerenciador de servidores e todos os serviços"
- "Exibindo o status atual de um serviço"
- "Parar um serviço"
- "Colocar um aparelho no modo de manutenção"
- "Forçar a cessação de um serviço"
- "Iniciar ou reiniciar um serviço"
- "Removendo remapas de portas"
- "Remoção de remapas de portas em hosts bare metal"
- "Reinicializando um nó de grade"
- "Fechando um nó de grade"
- "Desligar um host"
- "Desligar e ligar todos os nós na grade"

- "Usando um arquivo DoNotStart"
- "Solução de problemas do Server Manager"

Exibindo o status e a versão do Server Manager

Para cada nó de grade, você pode exibir o status atual e a versão do Server Manager em execução nesse nó de grade. Você também pode obter o status atual de todos os serviços executados nesse nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Veja o status atual do Server Manager em execução no nó da grade: **`service servermanager status`**

   O status atual do Server Manager em execução no nó da grade é relatado (em execução ou não). Se o status do Gerenciador de servidor for `running`, a hora em que ele foi executado desde a última vez em que foi iniciado é listada. Por exemplo:

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

   Este estado é o equivalente ao estado apresentado no cabeçalho do visor da consola local.

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`**

Exibindo o status atual de todos os serviços

Você pode visualizar o status atual de todos os serviços executados em um nó de grade a qualquer momento.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:

   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Veja o status de todos os serviços em execução no nó da grade: `storagegrid-status`

   Por exemplo, a saída para o nó de administração principal mostra o status atual dos serviços AMS, CMN e NMS como em execução. Essa saída é atualizada imediatamente se o status de um serviço mudar.

```
Host Name                      190-ADM1
IP Address
Operating System Kernel        4.9.0          Verified
Operating System Environment   Debian 9.4     Verified
StorageGRID Webscale Release   11.1.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.1.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.1.0         Running
cmn                            11.1.0         Running
nms                            11.1.0         Running
ssm                            11.1.0         Running
mi                             11.1.0         Running
dynip                          11.1.0         Running
nginx                          1.10.3         Running
tomcat                         8.5.14         Running
grafana                        4.2.0          Running
mgmt api                       11.1.0         Running
prometheus                     1.5.2+ds       Running
persistence                    11.1.0         Running
ade exporter                   11.1.0         Running
attrDownPurge                  11.1.0         Running
attrDownSamp1                  11.1.0         Running
attrDownSamp2                  11.1.0         Running
node exporter                  0.13.0+ds      Running
```

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`

Iniciando o Server Manager e todos os serviços

Talvez seja necessário iniciar o Server Manager, que também inicia todos os serviços no nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Iniciar o Server Manager em um nó de grade onde ele já está sendo executado resulta em uma reinicialização do Server Manager e de todos os serviços no nó de grade.

Passos

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`

Reiniciando o Gerenciador de servidores e todos os serviços

Talvez seja necessário reiniciar o gerenciador de servidor e todos os serviços em execução em um nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
2. Reinicie o Server Manager e todos os serviços no nó de grade: `service servermanager restart`

   O Gerenciador de servidores e todos os serviços no nó de grade são interrompidos e reiniciados.

Utilizar o `restart` comando é o mesmo que utilizar o `stop` comando seguido do `start` comando.

3. Faça logout do shell de comando: `exit`

Parar o Gerenciador de servidores e todos os serviços

O Server Manager destina-se a ser executado em todos os momentos, mas pode ser necessário parar o Server Manager e todos os serviços executados em um nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

O único cenário que exige que você pare o Gerenciador de servidor enquanto mantém o sistema operacional em execução é quando você precisa integrar o Gerenciador de servidor a outros serviços. Se houver um requisito para parar o Gerenciador de servidores para manutenção do hardware ou reconfiguração do servidor, todo o servidor deve ser interrompido.

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`

Exibindo o status atual de um serviço

Você pode visualizar o status atual de um serviço em execução em um nó de grade a qualquer momento.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Exibir o status atual de um serviço em execução em um nó de grade: "**Service *servicename* status** o status atual do serviço solicitado em execução no nó de grade é relatado (em execução ou não). Por exemplo:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Faça logout do shell de comando: **`exit`**

Parar um serviço

Alguns procedimentos de manutenção exigem que você pare um único serviço enquanto mantém outros serviços no nó da grade em execução. Apenas pare os serviços individuais quando for direcionado para o fazer através de um procedimento de manutenção.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Quando você usa essas etapas para "parar administrativamente" um serviço, o Gerenciador de servidor não reiniciará automaticamente o serviço. Você deve iniciar o único serviço manualmente ou reiniciar o Server Manager.

Se necessitar de parar o serviço LDR num nó de armazenamento, tenha em atenção que poderá demorar algum tempo a parar o serviço se existirem ligações ativas.

Passos

1. Faça login no nó da grade:

   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Parar um serviço individual: `service servicename stop`

   Por exemplo:

```
service ldr stop
```

Os serviços podem levar até 11 minutos para parar.

3. Faça logout do shell de comando: `exit`

Informações relacionadas

"Forçar a cessação de um serviço"

Colocar um aparelho no modo de manutenção

Deve colocar o aparelho no modo de manutenção antes de efetuar procedimentos de manutenção específicos.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

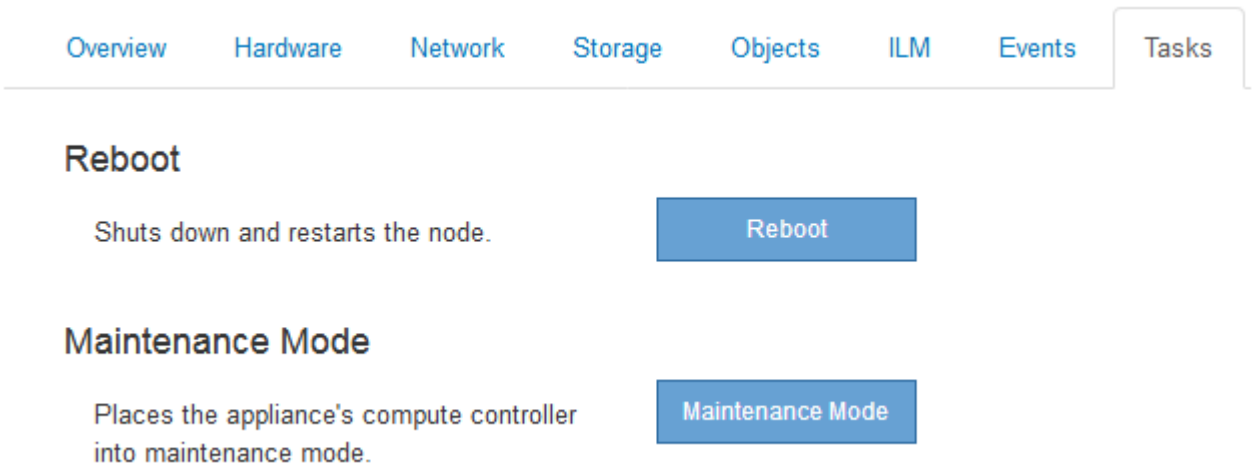
Sobre esta tarefa

Colocar um dispositivo StorageGRID no modo de manutenção pode tornar o aparelho indisponível para acesso remoto.

A senha e a chave de host de um dispositivo StorageGRID no modo de manutenção permanecem as mesmas que eram quando o aparelho estava em serviço.

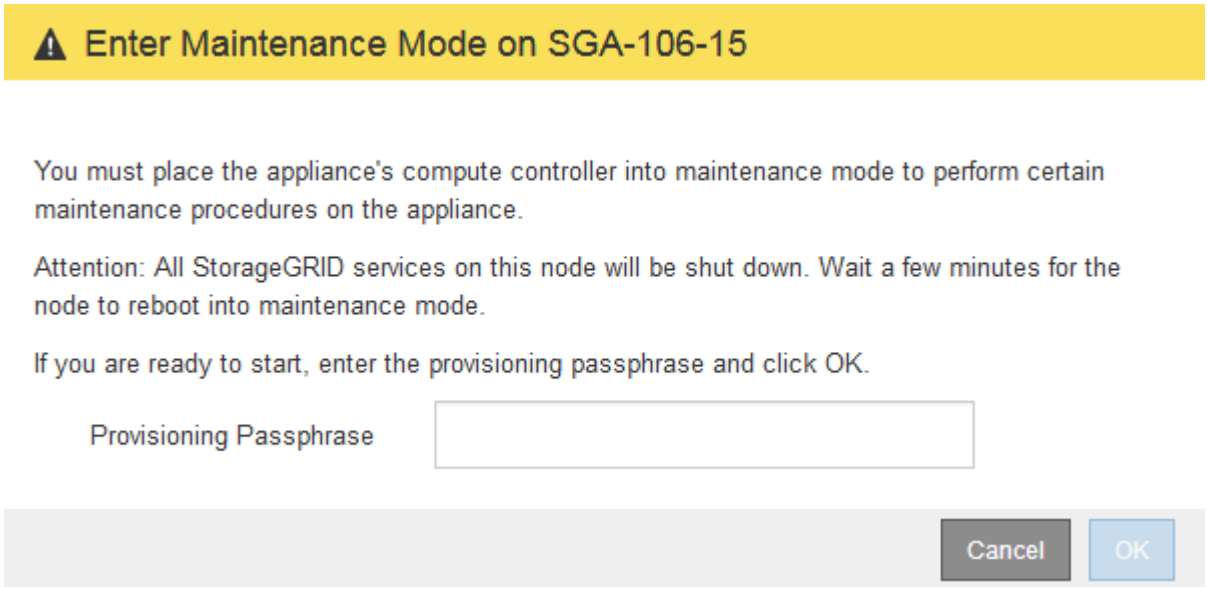
Passos

1. No Gerenciador de Grade, selecione **nós**.
2. Na exibição em árvore da página nós, selecione o nó de storage do dispositivo.
3. Selecione **tarefas**.



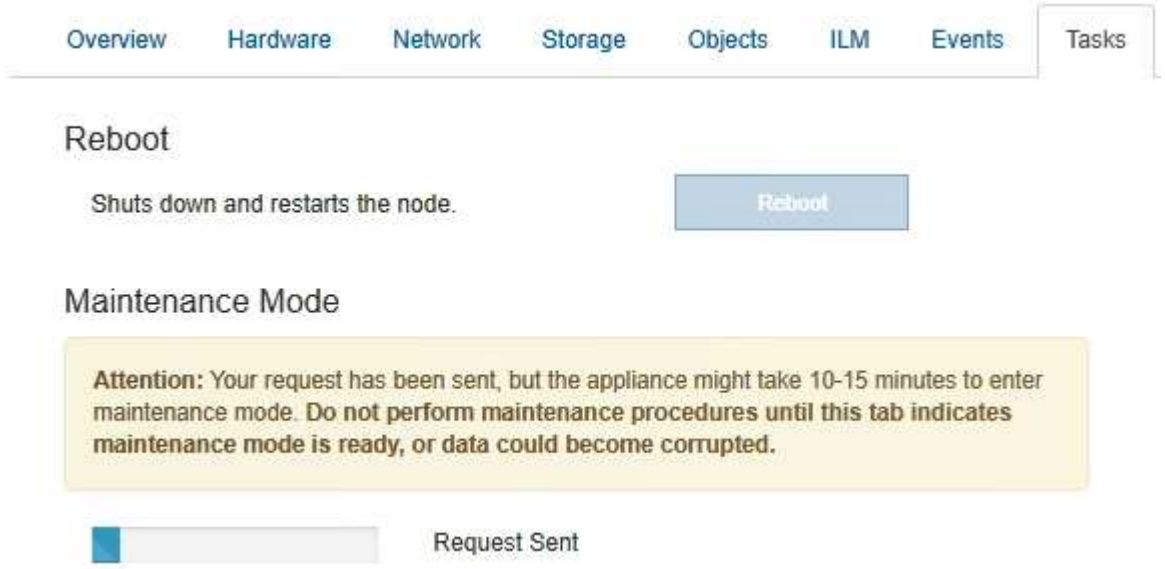
4. Selecione **Maintenance Mode** (modo de manutenção).

É apresentada uma caixa de diálogo de confirmação.

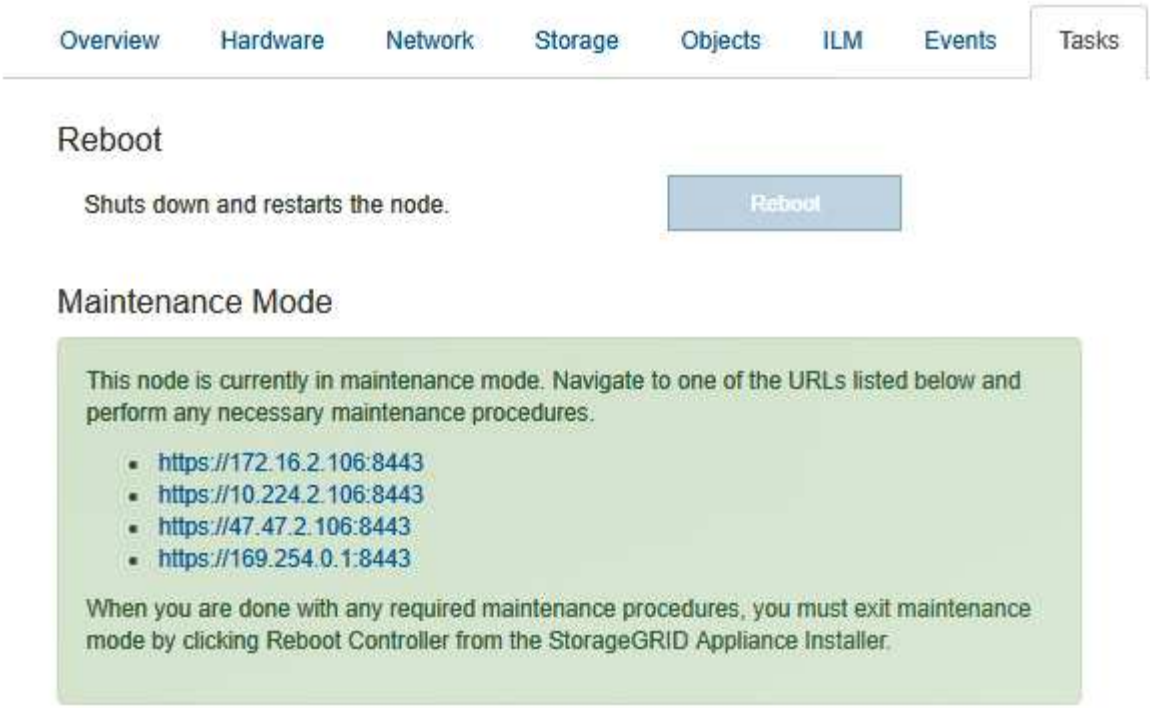


5. Introduza a frase-passe de aprovisionamento e selecione **OK**.

Uma barra de progresso e uma série de mensagens, incluindo "Request Sent" (pedido enviado), "Stop StorageGRID" (Paragem) e "Reboot" (reinício), indicam que o aparelho está a concluir os passos para entrar no modo de manutenção.



Quando o dispositivo está no modo de manutenção, uma mensagem de confirmação lista os URLs que você pode usar para acessar o Instalador do StorageGRID Appliance.



6. Para acessar o Instalador do StorageGRID Appliance, navegue até qualquer um dos URLs exibidos.

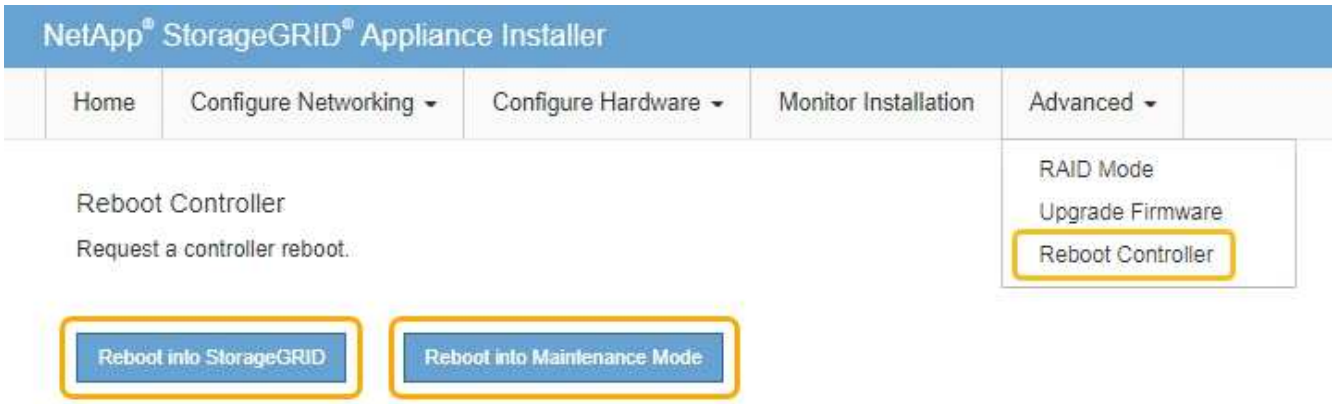
   Se possível, use o URL que contém o endereço IP da porta Admin Network do dispositivo.

   > O acesso `https://169.254.0.1:8443` requer uma conexão direta com a porta de gerenciamento local.

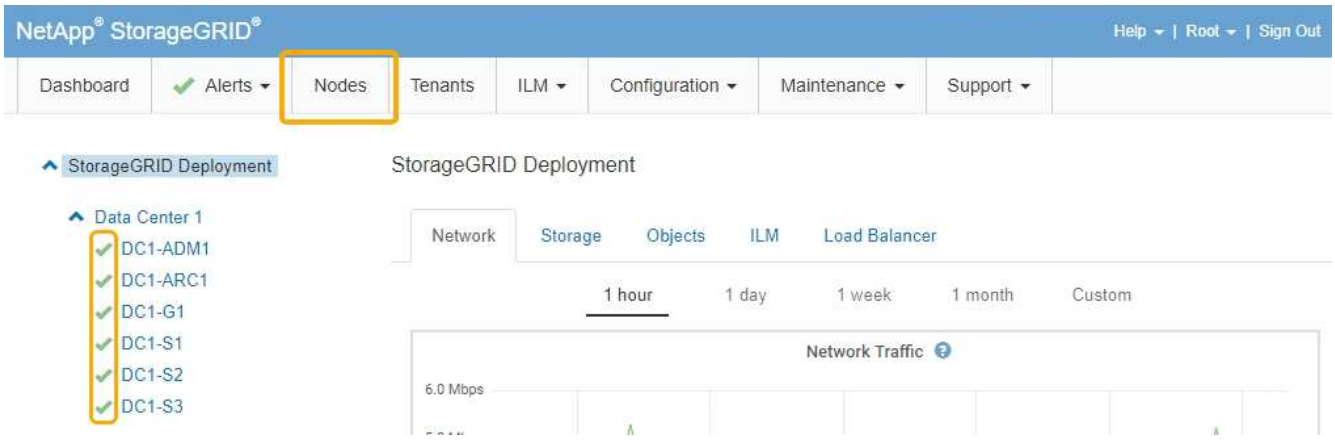
7. A partir do instalador do dispositivo StorageGRID, confirme se o aparelho está no modo de manutenção.

8. Execute todas as tarefas de manutenção necessárias.
9. Depois de concluir as tarefas de manutenção, saia do modo de manutenção e retome a operação normal do nó. No Instalador de dispositivos StorageGRID, selecione **Avançado controlador de reinicialização** e, em seguida, selecione **Reiniciar no StorageGRID**.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A guia **nós** deve exibir um status normal ✔para o nó do dispositivo, indicando que não há alertas ativos e o nó está conetado à grade.



Forçar a cessação de um serviço

Se você precisar parar um serviço imediatamente, você pode usar o `force-stop` comando.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Forçar manualmente o serviço a terminar: `service servicename force-stop`

   Por exemplo:

   ```
   service ldr force-stop
   ```

   O sistema aguarda 30 segundos antes de terminar o serviço.

3. Faça logout do shell de comando: `exit`

Iniciar ou reiniciar um serviço

Talvez seja necessário iniciar um serviço que tenha sido interrompido ou talvez seja necessário parar e reiniciar um serviço.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:

   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Decida qual comando emitir, com base se o serviço está em execução ou parado no momento.

   - Se o serviço estiver parado no momento, use o `start` comando para iniciar o serviço manualmente: `service servicename start`

     Por exemplo:

     ```
     service ldr start
     ```

   - Se o serviço estiver atualmente em execução, use o `restart` comando para parar o serviço e, em seguida, reinicie-o: `service servicename restart`

     Por exemplo:

     ```
     service ldr restart
     ```

     +

Utilizar o `restart` comando é o mesmo que utilizar o `stop` comando seguido do `start` comando. Você pode emitir `restart` mesmo se o serviço estiver parado no momento.

3. Faça logout do shell de comando: `exit`

Removendo 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.

Este procedimento remove todos os remapas de portas. Se você precisar manter alguns dos remapas, entre em Contato com o suporte técnico.

Para obter informações sobre como configurar pontos de extremidade do balanceador de carga, consulte as instruções para administrar o StorageGRID.

Se o remapeamento de portas fornecer acesso ao cliente, o cliente deve ser reconfigurado para usar uma porta diferente configurada como um endpoint de balanceador de carga, se possível, para evitar a perda de serviço, caso contrário, remover o mapeamento de portas resultará na perda de acesso ao cliente e deve ser programado adequadamente.

Este procedimento não funciona para um sistema StorageGRID implantado como um contentor em hosts de metal nu. Consulte as instruções para remover os 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 contentor Docker que executa o StorageGRID.

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Execute o seguinte script: `remove-port-remap.sh`
3. Reinicie o nó.

   Siga as instruções para reiniciar um nó de grade.

4. Repita estas etapas em cada nó de administração e nó de gateway que tenha portas remapeadas

conflitantes.

Informações relacionadas

"Administrar o StorageGRID"

"Reinicializando um nó de grade"

"Remoção de remapas de portas em hosts bare metal"

Remoção de remapas de portas em hosts bare metal

Se você quiser configurar um ponto de extremidade para o serviço Load Balancer e quiser usar uma porta que já tenha sido configurada como a porta mapeada de um remapeamento de porta, primeiro remova o remapeamento de porta existente ou o ponto de extremidade não será efetivo. Se você estiver executando o StorageGRID em hosts bare metal, siga este procedimento em vez do procedimento geral para remover os remapas de portas. Você deve editar o arquivo de configuração de nó para cada nó Admin e nó Gateway que tenha portas remapeadas conflitantes para remover todos os remapas de portas do nó e reiniciar o nó.

> 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
<strong>PORT_REMAP = client/tcp/8082/443</strong>
<strong>PORT_REMAP_INBOUND = client/tcp/8082/443</strong>
```

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.

Reinicializando um nó de grade

Você pode reinicializar um nó de grade a partir do Gerenciador de Grade ou do shell de comando do nó.

Sobre esta tarefa

Quando você reinicializa um nó de grade, o nó desliga e reinicia. Todos os serviços são reiniciados automaticamente.

Se você planeja reinicializar os nós de storage, observe o seguinte:

- Se uma regra ILM especificar um comportamento de ingestão de confirmação dupla ou a regra especificar balanceado e não for possível criar imediatamente todas as cópias necessárias, o StorageGRID enviará imediatamente quaisquer objetos recém-ingeridos a dois nós de armazenamento no mesmo local e avaliará o ILM posteriormente. Se você quiser reinicializar dois ou mais nós de storage em um determinado site, talvez não seja possível acessar esses objetos durante a reinicialização.
- Para garantir que você possa acessar todos os objetos enquanto um nó de armazenamento estiver reiniciando, pare de ingerir objetos em um site por aproximadamente uma hora antes de reiniciar o nó.

Informações relacionadas

"Administrar o StorageGRID"

Opções

- "Reiniciar um nó de grade a partir do Gerenciador de Grade"
- "Reinicializando um nó de grade a partir do shell de comando"

Reiniciar um nó de grade a partir do Gerenciador de Grade

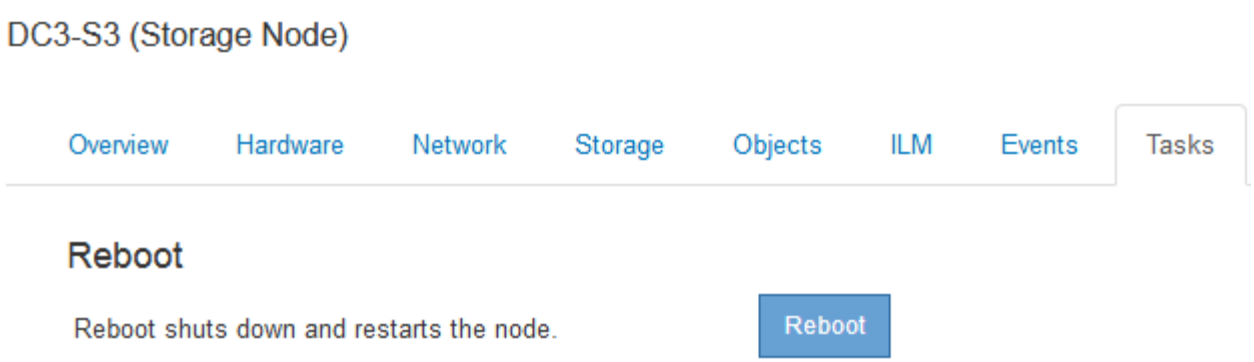
Reiniciar um nó de grade a partir do Gerenciador de Grade emite o `reboot` comando no nó de destino.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.

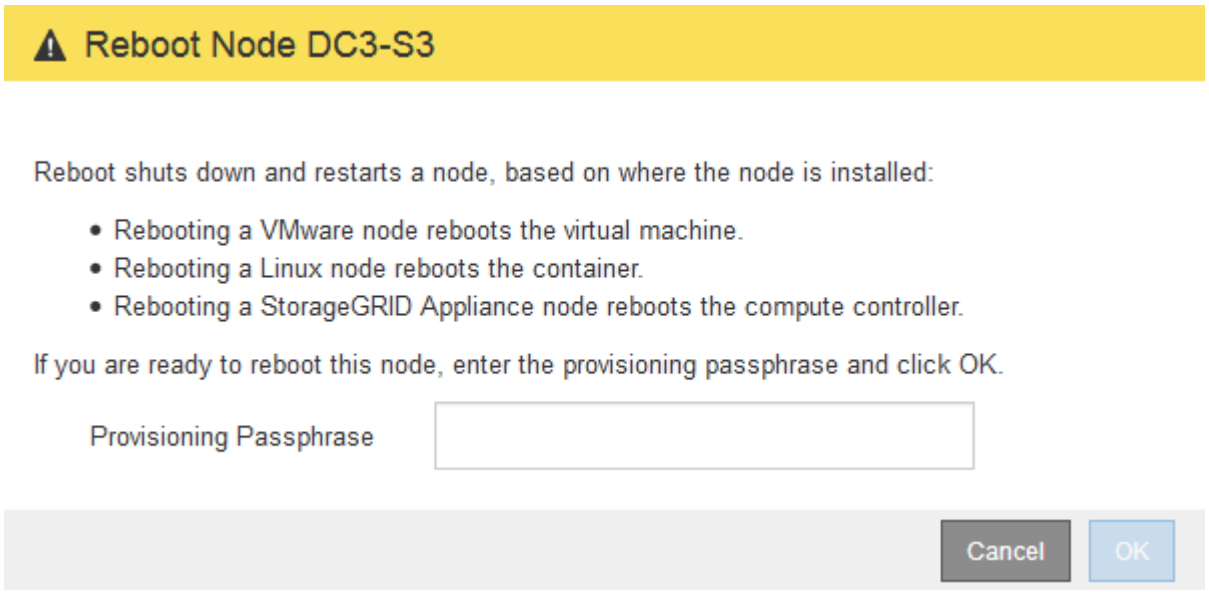
Passos

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



4. Clique em **Reboot**.

   É apresentada uma caixa de diálogo de confirmação.



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

5. Digite a senha de provisionamento e clique em **OK**.
6. Aguarde até que o nó seja reiniciado.

   Pode levar algum tempo para que os serviços sejam desativados.

   Quando o nó é reinicializado, o ícone cinza (administrativamente para baixo) aparece no lado esquerdo da página nós. Quando todos os serviços tiverem sido iniciados novamente, o ícone muda novamente para a cor original.

Reinicializando um 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.

O que você vai precisar

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

Passos

1. Faça login no nó da grade:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
2. 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`

Fechando um nó de grade

Você pode encerrar um nó de grade a partir do shell de comando do nó.

O que você vai precisar

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

Sobre esta tarefa

Antes de executar este procedimento, reveja estas considerações:

- Em geral, você não deve encerrar mais de um nó de cada vez para evitar interrupções.
- Não encerre um nó durante um procedimento de manutenção, a menos que seja explicitamente instruído a fazê-lo pela documentação ou pelo suporte técnico.
- O processo de desligamento é baseado em onde o nó é instalado, como segue:
  - Desligar um nó da VMware desliga a máquina virtual.
  - Desligar um nó Linux desliga o contentor.
  - Desligar um nó de dispositivo StorageGRID desliga o controlador de computação.
- Se você planeja encerrar os nós de storage, observe o seguinte:
  - Se uma regra ILM especificar um comportamento de ingestão de confirmação dupla ou a regra especificar balanceado e não for possível criar imediatamente todas as cópias necessárias, o StorageGRID enviará imediatamente quaisquer objetos recém-ingeridos a dois nós de armazenamento no mesmo local e avaliará o ILM posteriormente. Se você quiser encerrar dois ou mais nós de storage em um determinado local, talvez não consiga acessar esses objetos durante o encerramento.

- Para garantir que você possa acessar todos os objetos quando um nó de armazenamento for desligado, pare de ingerir objetos em um local por aproximadamente uma hora antes de desligar o nó.

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. Faça logout do shell de comando: `exit`

Depois de ser desligado, você pode desligar o nó da grade.

"Desligar um host"

Informações relacionadas

"Administrar o StorageGRID"

Desligar um host

Antes de desligar um host, você deve interromper os serviços em todos os nós da grade nesse host.

Passos

1. Faça login no nó da grade:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Parar todos os serviços em execução no nó: `service servermanager stop`

   Os serviços podem levar até 15 minutos para serem encerrados, e você pode querer fazer login no sistema remotamente para monitorar o processo de desligamento.

3. Repita as etapas 1 e 2 para cada nó no host.
4. Se você tiver um host Linux:

a. Faça login no sistema operacional host.
b. Pare o nó: `storagegrid node stop`
c. Encerre o sistema operacional do host.

5. Se o nó estiver sendo executado em uma máquina virtual VMware ou se for um nó de dispositivo, execute o comando shutdown: `shutdown -h now`

   Execute esta etapa independentemente do resultado do `service servermanager stop` comando.

   > Depois de emitir o `shutdown -h now` comando em um nó de dispositivo, você deve desligar o dispositivo para reiniciar o nó.

   Para o aparelho, este comando desliga o controlador, mas o aparelho ainda está ligado. Você deve concluir o próximo passo.

6. Se você estiver desativando um nó de dispositivo:
   - Para o dispositivo de serviços SG100 ou SG1000
     i. Desligue a alimentação do aparelho.
     ii. Aguarde até que o LED azul de alimentação se desligue.
   - Para o aparelho SG6000
     i. Aguarde que o LED verde Cache ative na parte de trás do controlador de armazenamento seja desligado.

        Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

     ii. Desligue o aparelho e aguarde até que o LED azul de alimentação se desligue.
   - Para o aparelho SG5700
     i. Aguarde que o LED verde Cache ative na parte de trás do controlador de armazenamento seja desligado.

        Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

     ii. Desligue a alimentação do aparelho e aguarde que todas as atividades de exibição de LED e de sete segmentos parem.

7. Faça logout do shell de comando: `exit`

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

Desligar e ligar todos os nós na grade

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.

Interrompendo serviços e desligando nós de 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, contentores Docker e dispositivos StorageGRID.

Sobre esta tarefa

Se possível, você deve parar os serviços nos nós da grade nesta ordem:

- Pare primeiro os serviços nos nós do Gateway.
- Parar os serviços no nó de administração principal por último.

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 migrar nós de um host Linux para outro para executar a manutenção do host sem afetar a funcionalidade ou a disponibilidade de sua grade.

"Linux: Migrando um nó de grade para um novo host"

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, nós de arquivamento e nós de administração não primários.

   Você pode parar os serviços nesses nós em qualquer ordem.

Se você emitir o `service servermanager stop` comando para parar os serviços em um nó de armazenamento de dispositivo, será necessário desligar o dispositivo para reiniciar o nó.

5. Para o nó de administração principal, repita as etapas para iniciar sessão no nó e parando todos os serviços no nó.
6. Para nós que estão sendo executados em hosts Linux:
   a. Faça login no sistema operacional host.
   b. Pare o nó: `storagegrid node stop`
   c. Encerre o sistema operacional do host.
7. Para nós que estão sendo executados em máquinas virtuais VMware e para nós de storage do dispositivo, execute o comando shutdown: `shutdown -h now`

   Execute esta etapa independentemente do resultado do `service servermanager stop` comando.

   Para o dispositivo, esse comando desliga o controlador de computação, mas o dispositivo ainda está ligado. Você deve concluir o próximo passo.

8. Se você tiver nós do dispositivo:
   - Para o dispositivo de serviços SG100 ou SG1000
     i. Desligue a alimentação do aparelho.
     ii. Aguarde até que o LED azul de alimentação se desligue.
   - Para o aparelho SG6000
     i. Aguarde que o LED verde Cache ative na parte de trás do controlador de armazenamento seja desligado.

        Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

     ii. Desligue o aparelho e aguarde até que o LED azul de alimentação se desligue.
   - Para o aparelho SG5700
     i. Aguarde que o LED verde Cache ative na parte de trás do controlador de armazenamento seja desligado.

        Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

     ii. Desligue a alimentação do aparelho e aguarde que todas as atividades de exibição de LED e de sete segmentos parem.
9. Se necessário, faça logout do shell de comando: `exit`

   A grelha StorageGRID foi agora desligada.

Informações relacionadas

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

Iniciando os nós da grade

Siga esta sequência para iniciar os nós da grelha após um encerramento completo.

> 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.

Sobre esta tarefa

Se possível, você deve ligar os nós da grade nesta ordem:

- Aplique o poder aos nós de administração primeiro.
- Aplique energia aos nós do Gateway por último.

> Se um host incluir vários nós de grade, os nós retornarão online automaticamente quando você ligar o host.

Passos

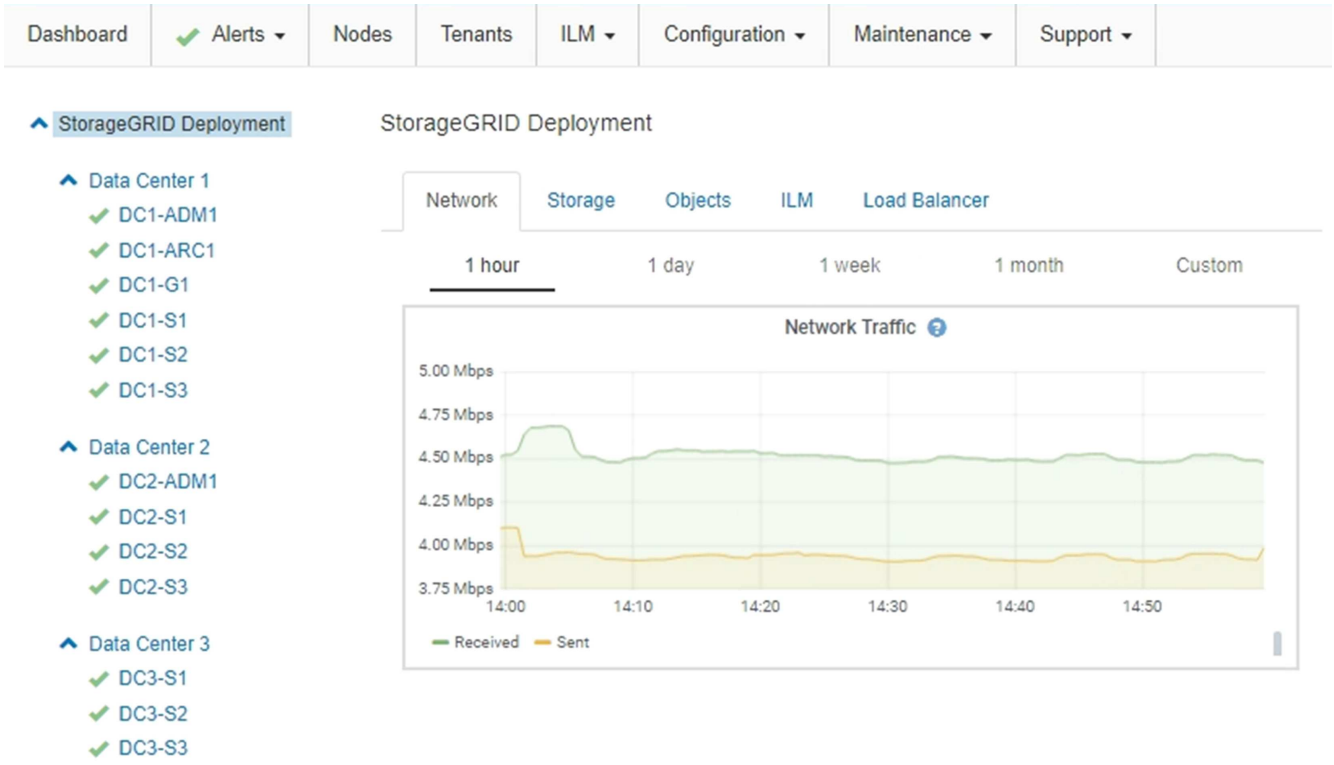
1. Ligue os hosts para o nó de administração principal e quaisquer nós de administração não primários.

   > Você não poderá fazer login nos nós de administração até que os nós de storage tenham sido reiniciados.

2. Ligue os hosts para todos os nós de arquivamento e nós de storage.

   Você pode ativar esses nós em qualquer ordem.

3. Ligue os hosts para todos os nós do Gateway.
4. Entre no Gerenciador de Grade.
5. Clique em **nós** e monitore o status dos nós da grade. Verifique se todos os nós retornam ao status "'verde'".



Usando 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.

Adicionando um arquivo DoNotStart para um serviço

Você pode impedir que um serviço individual comece adicionando um arquivo DoNotStart ao diretório desse serviço em um nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:

   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Adicione um arquivo DoNotStart: `touch /etc/sv/service/DoNotStart`

   ```
   `service`onde está o nome do serviço a ser impedido de iniciar. Por
   exemplo,
   ```

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   É criado um ficheiro DoNotStart. Nenhum conteúdo de arquivo é necessário.

   Quando o Gerenciador de servidor ou o nó de grade é reiniciado, o Gerenciador de servidor será reiniciado, mas o serviço não será reiniciado.

3. Faça logout do shell de comando: `exit`

Removendo um arquivo DoNotStart para um serviço

Quando você remove um arquivo DoNotStart que está impedindo que um serviço seja iniciado, você deve iniciar esse serviço.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:

   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   c. Digite o seguinte comando para mudar para root: `su -`

   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Remova o arquivo DoNotStart do diretório de serviços: `rm /etc/sv/service/DoNotStart`

`service`onde está o nome do serviço. Por exemplo,

```
rm /etc/sv/ldr/DoNotStart
```

3. Inicie o serviço: `service servicename start`
4. Faça logout do shell de comando: `exit`

Solução de problemas do Server Manager

O suporte técnico pode direcioná-lo para tarefas de solução de problemas para determinar a origem dos problemas relacionados ao Gerenciador de servidores.

Aceder ao ficheiro de registo do Gestor de servidor

Se surgir um problema ao utilizar o Gestor de servidor, verifique o respetivo ficheiro de registo.

As mensagens de erro relacionadas ao Gestor de servidor são capturadas no ficheiro de registo do Gestor de servidor, que se encontra em: `/var/local/log/servermanager.log`

Verifique este arquivo para ver se há mensagens de erro relacionadas a falhas. Encaminhe o problema para o suporte técnico, se necessário. Poderá ser-lhe pedido que encaminhe ficheiros de registo para o suporte técnico.

Serviço com um estado de erro

Se detetar que um serviço introduziu um estado de erro, tente reiniciar o serviço.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

O Server Manager monitora os serviços e reinicia qualquer um que tenha parado inesperadamente. Se um serviço falhar, o Gerenciador do servidor tentará reiniciá-lo. Se houver três tentativas falhadas de iniciar um serviço dentro de cinco minutos, o serviço entrará em um estado de erro. O Gerenciador de servidores não tenta outra reinicialização.

Passos

1. Faça login no nó da grade:
   a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Confirme o estado de erro do serviço: `service servicename status`

   Por exemplo:

   ```
   service ldr status
   ```

   Se o serviço estiver em um estado de erro, a seguinte mensagem será retornada: `servicename in error state`. Por exemplo:

   ```
   ldr in error state
   ```

   > Se o status do serviço for `disabled`, consulte as instruções para remover 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`

Informações relacionadas

"Removendo um arquivo DoNotStart para um serviço"

Clonagem do nó do dispositivo

Você pode clonar um nó de dispositivo no StorageGRID para usar um dispositivo de design mais recente ou recursos aprimorados. A clonagem transfere todas as informações do nó existente para o novo dispositivo, fornece um processo de atualização de hardware fácil de executar e fornece uma alternativa à desativação e expansão para a substituição de dispositivos.

Como funciona a clonagem de nós do dispositivo

A clonagem do nó do dispositivo permite substituir facilmente um nó do dispositivo (origem) existente na grade por um dispositivo compatível (destino) que faz parte do mesmo local lógico da StorageGRID. O processo transfere todos os dados para o novo dispositivo, colocando-os em serviço para substituir o nó antigo do dispositivo e deixando o dispositivo antigo em um estado de pré-instalação.

Por que clonar um nó de dispositivo?

Você pode clonar um nó de dispositivo se precisar:

- Substitua os aparelhos que estão chegando ao fim da vida útil.
- Atualize os nós existentes para aproveitar a tecnologia aprimorada do dispositivo.
- Aumente a capacidade de storage em grade sem alterar o número de nós de storage no sistema

StorageGRID.

- Aumentar a eficiência de storage, como alterar o modo RAID de DDP-8 para DDP-16 ou RAID-6.
- Implemente com eficiência a criptografia de nó para permitir o uso de servidores de gerenciamento de chaves externas (KMS).

Que rede StorageGRID é utilizada?

A clonagem transfere dados do nó de origem diretamente para o dispositivo de destino em qualquer uma das três redes StorageGRID. Normalmente, a rede de Grade é utilizada, mas também pode utilizar a rede Admin ou a rede Cliente se o utilitário de origem estiver ligado a estas redes. Escolha a rede a ser usada para clonagem de tráfego que forneça a melhor performance de transferência de dados sem prejudicar a performance da rede StorageGRID ou a disponibilidade de dados.

Ao instalar o dispositivo de substituição, você deve especificar endereços IP temporários para conexão StorageGRID e transferência de dados. Como o dispositivo de substituição fará parte das mesmas redes que o nó do dispositivo que ele substitui, você deve especificar endereços IP temporários para cada uma dessas redes no dispositivo de substituição.

Compatibilidade do dispositivo alvo

Os dispositivos de substituição devem ser do mesmo tipo que o nó de origem que estão substituindo e ambos devem fazer parte do mesmo local lógico do StorageGRID.

- Um dispositivo de serviços de substituição pode ser diferente do nó de administração ou do nó de gateway que está substituindo.
  - Você pode clonar um dispositivo de nó de origem SG100 para um dispositivo de destino de serviços SG1000 para oferecer maior capacidade ao nó de administrador ou nó de gateway.
  - Você pode clonar um dispositivo de nós de origem SG1000 para um dispositivo de destino de serviços SG100 para reimplantar o SG1000 para uma aplicação mais exigente.

    Por exemplo, se um dispositivo de nó de origem SG1000 estiver sendo usado como nó Admin e você quiser usá-lo como um nó de balanceamento de carga dedicado.

  - A substituição de um dispositivo de nó de origem SG1000 por um dispositivo de destino de serviços SG100 reduz a velocidade máxima das portas de rede de 100 GbE para 25 GbE.
  - Os aparelhos SG100 e SG1000 têm conetores de rede diferentes. Mudar o tipo de aparelho pode exigir a substituição dos cabos ou módulos SFP.
- Um dispositivo de storage de substituição deve ter capacidade igual ou superior ao nó de storage que está substituindo.
  - Se o dispositivo de armazenamento de destino tiver o mesmo número de unidades que o nó de origem, as unidades no dispositivo de destino devem ter a mesma capacidade (em TB) ou maior.
  - Se o número de unidades padrão instaladas em um dispositivo de armazenamento de destino for menor que o número de unidades no nó de origem, devido à instalação de unidades de estado sólido (SSDs), a capacidade geral de armazenamento das unidades padrão no dispositivo de destino (em TB) deve atender ou exceder a capacidade total da unidade funcional de todas as unidades no nó de armazenamento de origem.

    Por exemplo, ao clonar um dispositivo de nó de storage de SG5660 fontes com 60 unidades para um dispositivo de destino de SG6060 U com 58 unidades padrão, unidades maiores devem ser instaladas no dispositivo de destino SG6060 antes da clonagem para manter a capacidade de storage. (Os dois slots de unidade que contêm SSDs no dispositivo de destino não estão incluídos na capacidade total

de armazenamento do dispositivo.)

No entanto, se um dispositivo de nó de origem de SG5660 unidades de 60 unidades estiver configurado com DDP-8 SANtricity Dynamic Disk Pools, configurar um dispositivo de destino de SG6060 unidades com mesmo tamanho de 58 unidades com DDP-16 pode tornar o dispositivo SG6060 um destino de clone válido devido à sua eficiência de storage aprimorada.

Você pode exibir informações sobre o modo RAID atual do nó do dispositivo de origem na página **nós** no Gerenciador de Grade. Selecione o separador **Storage** (armazenamento) para o aparelho.

Que informação não é clonada?

As configurações do dispositivo a seguir não são transferidas para o dispositivo de substituição durante a clonagem. Deve configurá-los durante a configuração inicial do aparelho de substituição.

- Interface BMC
- Ligações de rede
- Status da criptografia do nó
- Gerenciador de sistema do SANtricity (para nós de storage)
- Modo RAID (para nós de storage)

Que problemas impedem a clonagem?

Se algum dos seguintes problemas for encontrado durante a clonagem, o processo de clonagem será interrompido e uma mensagem de erro será gerada:

- Configuração de rede incorreta
- Falta de conetividade entre os dispositivos de origem e destino
- Incompatibilidade de dispositivos de origem e destino
- Para nós de storage, um dispositivo de substituição de capacidade insuficiente

Para continuar, é necessário resolver cada problema de clonagem.

Considerações e requisitos para clonagem de nós do dispositivo

Antes de clonar um nó do dispositivo, você precisa entender as considerações e os requisitos.

Requisitos de hardware para o dispositivo de substituição

Certifique-se de que o aparelho de substituição cumpre os seguintes critérios:

- O nó de origem (dispositivo sendo substituído) e o dispositivo de destino (novo) devem ser do mesmo tipo de dispositivo:
  - Você só pode clonar um dispositivo Admin Node ou um dispositivo Gateway Node para um novo dispositivo de serviços.
  - Você só pode clonar um dispositivo nó de storage para um novo dispositivo de storage.
- Para os dispositivos Admin Node ou Gateway Node, o dispositivo de nó de origem e o dispositivo de destino não precisam ser do mesmo tipo de dispositivo; no entanto, alterar o tipo de dispositivo pode exigir a substituição dos cabos ou módulos SFP.

Por exemplo, você pode substituir um dispositivo de SG1000 nós por um SG100 ou substituir um dispositivo SG100 por um dispositivo SG1000.

- Para dispositivos de nó de storage, o dispositivo de nó de origem e o dispositivo de destino não precisam ser do mesmo tipo de dispositivo. No entanto, o dispositivo de destino deve ter a mesma capacidade de storage ou maior que o dispositivo de origem.

  Por exemplo, você pode substituir um dispositivo de SG5600 nós por um dispositivo SG5700 ou SG6000.

Entre em Contato com seu representante de vendas da StorageGRID para obter ajuda na escolha de dispositivos de substituição compatíveis para clonar nós de dispositivos específicos em sua instalação do StorageGRID.

Preparando-se para clonar um nó de dispositivo

Você precisa ter as seguintes informações antes de clonar um nó de dispositivo:

- Obtenha um endereço IP temporário para a rede de Grade do administrador da rede para uso com o utilitário de destino durante a instalação inicial. Se o nó de origem pertencer a uma rede de administração ou a uma rede de cliente, obtenha endereços IP temporários para essas redes.

  Os endereços IP temporários estão normalmente na mesma sub-rede que o dispositivo de nó de origem que está sendo clonado e não são necessários após a conclusão da clonagem. Os dispositivos de origem e destino devem se conectar ao nó de administrador principal do StorageGRID para estabelecer uma conexão de clonagem.

- Determinar qual rede usar para clonar o tráfego de transferência de dados que forneça a melhor performance de transferência de dados sem prejudicar a performance da rede StorageGRID ou a disponibilidade de dados.

  > O uso da rede de administração de 1 GbE para clonar a transferência de dados resulta em clonagem mais lenta.

- Determine se a criptografia de nó usando um servidor de gerenciamento de chaves (KMS) será usada no dispositivo de destino, de modo que você possa habilitar a criptografia de nó durante a instalação inicial do dispositivo de destino antes da clonagem. Você pode verificar se a criptografia de nó está ativada no nó do dispositivo de origem, conforme descrito na instalação do dispositivo.

  O nó de origem e o dispositivo de destino podem ter configurações diferentes de criptografia de nó. A descriptografia e a criptografia de dados são executadas automaticamente durante a transferência de dados e quando o nó de destino é reiniciado e se junta à grade.

  - "Aparelhos de serviços SG100 SG1000"
  - "SG5600 dispositivos de armazenamento"
  - "SG5700 dispositivos de armazenamento"
  - "SG6000 dispositivos de armazenamento"
- Determine se o modo RAID no dispositivo de destino deve ser alterado de sua configuração padrão, para que você possa especificar essas informações durante a instalação inicial do dispositivo de destino antes da clonagem. Você pode exibir informações sobre o modo RAID atual do nó do dispositivo de origem na página **nós** no Gerenciador de Grade. Selecione o separador **Storage** (armazenamento) para o aparelho.

  O nó de origem e o dispositivo de destino podem ter configurações RAID diferentes.

- Planeje por tempo suficiente para concluir o processo de clonagem de nós. Vários dias podem ser necessários para transferir dados de um nó de armazenamento operacional para um dispositivo de destino. Agende a clonagem em um momento que minimize o impacto nos negócios.
- Você só deve clonar um nó de dispositivo de cada vez. A clonagem pode impedir que você execute outras funções de manutenção do StorageGRID ao mesmo tempo.
- Depois de clonar um nó de dispositivo, você pode usar o dispositivo de origem que foi retornado a um estado de pré-instalação como destino para clonar outro dispositivo de nó compatível.

Procedimento de clonagem do nó do dispositivo

O processo de clonagem pode levar vários dias para transferir dados entre o nó de origem (o dispositivo está sendo substituído) e o dispositivo de destino (novo).

O que você vai precisar

- Você instalou o dispositivo de destino compatível em um gabinete ou rack, conetou todos os cabos e aplicou energia.
- Você verificou que a versão do Instalador de dispositivos StorageGRID no dispositivo de substituição corresponde à versão de software do seu sistema StorageGRID, atualizando o firmware do Instalador de dispositivos StorageGRID, se necessário.
- Você configurou o dispositivo de destino, incluindo a configuração de conexões StorageGRID, o Gerenciador de sistema do SANtricity (somente dispositivos de storage) e a interface do BMC.
  - Ao configurar conexões StorageGRID, use os endereços IP temporários.
  - Ao configurar links de rede, use a configuração final do link.

> Deixe o Instalador do StorageGRID Appliance aberto depois de concluir a configuração inicial do dispositivo de destino. Você retornará à página do instalador do dispositivo de destino depois de iniciar o processo de clonagem do nó.

- Você ativou opcionalmente a criptografia de nó para o dispositivo de destino.
- Opcionalmente, você definiu o modo RAID para o dispositivo de destino (somente dispositivos de armazenamento).
- "Considerações e requisitos para clonagem de nós do dispositivo"

  "Aparelhos de serviços SG100 SG1000"

  "SG5600 dispositivos de armazenamento"

  "SG5700 dispositivos de armazenamento"

  "SG6000 dispositivos de armazenamento"

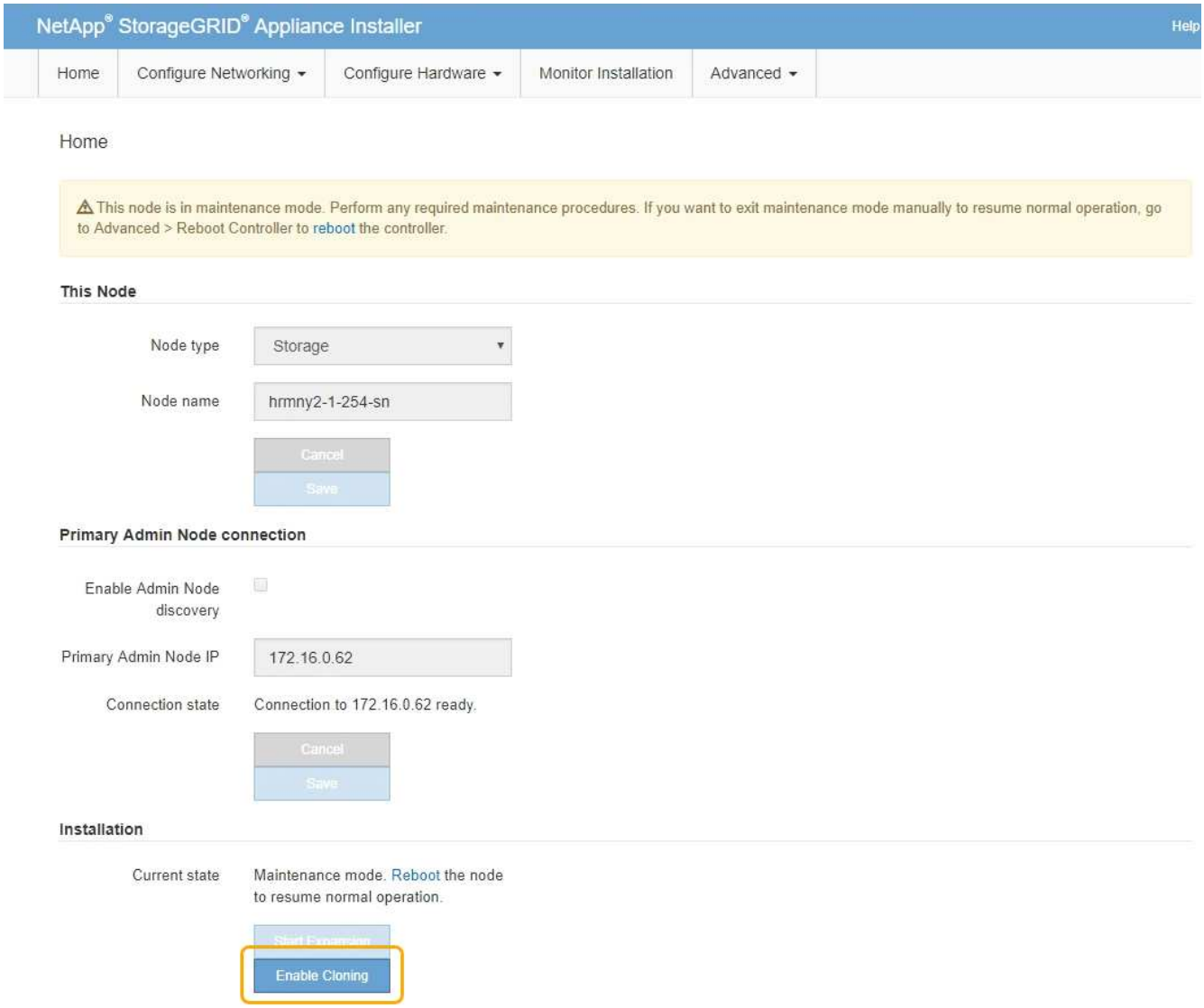
Você deve clonar apenas um nó do dispositivo de cada vez para manter o desempenho da rede StorageGRID e a disponibilidade de dados.

Passos

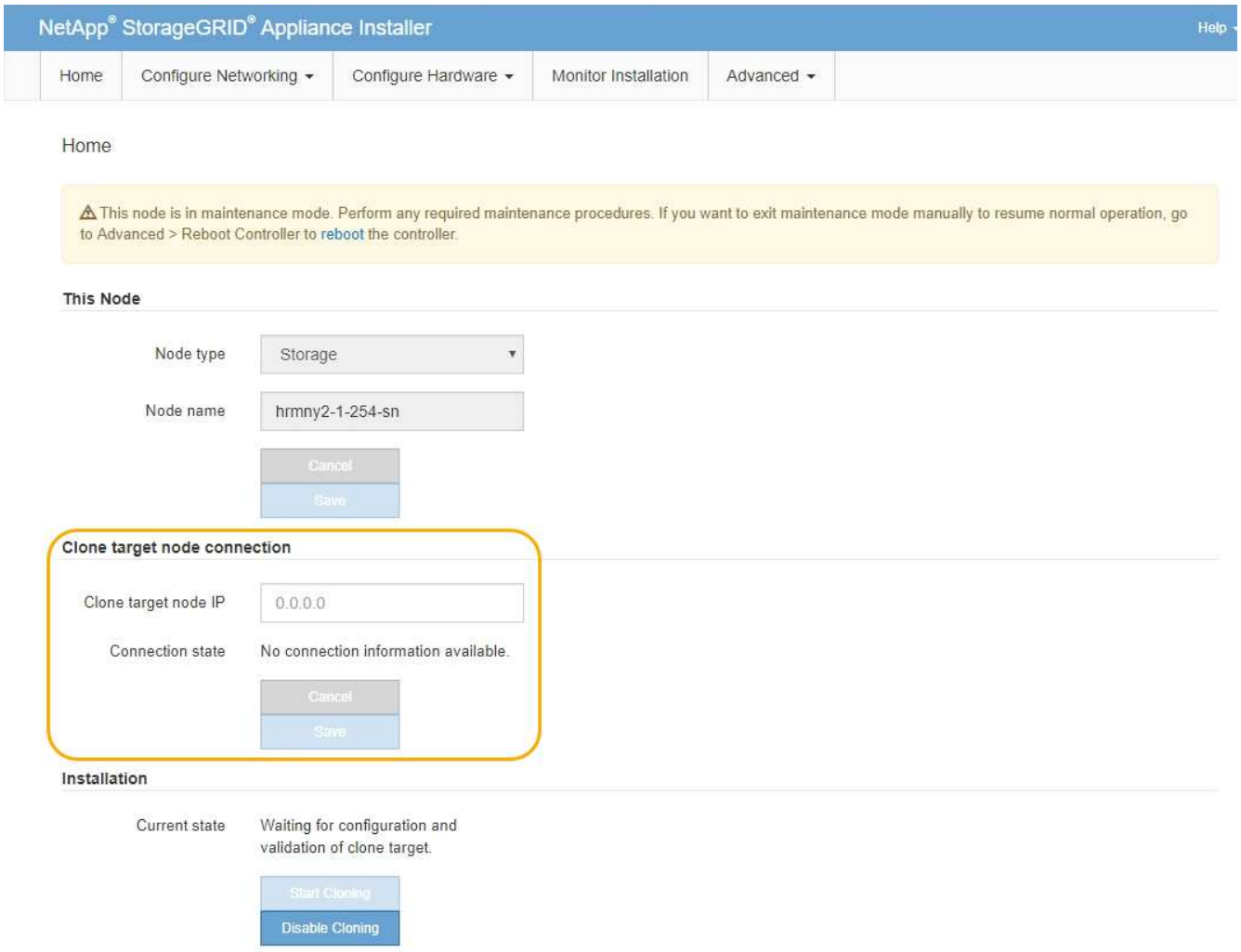
1. Coloque o nó de origem que você está clonando no modo de manutenção.

   "Colocar um aparelho no modo de manutenção"

2. No Instalador de dispositivos StorageGRID no nó de origem, na seção Instalação da página inicial, selecione **Ativar clonagem**.



A seção de conexão do nó de administração principal é substituída pela seção de conexão do nó de destino Clone.

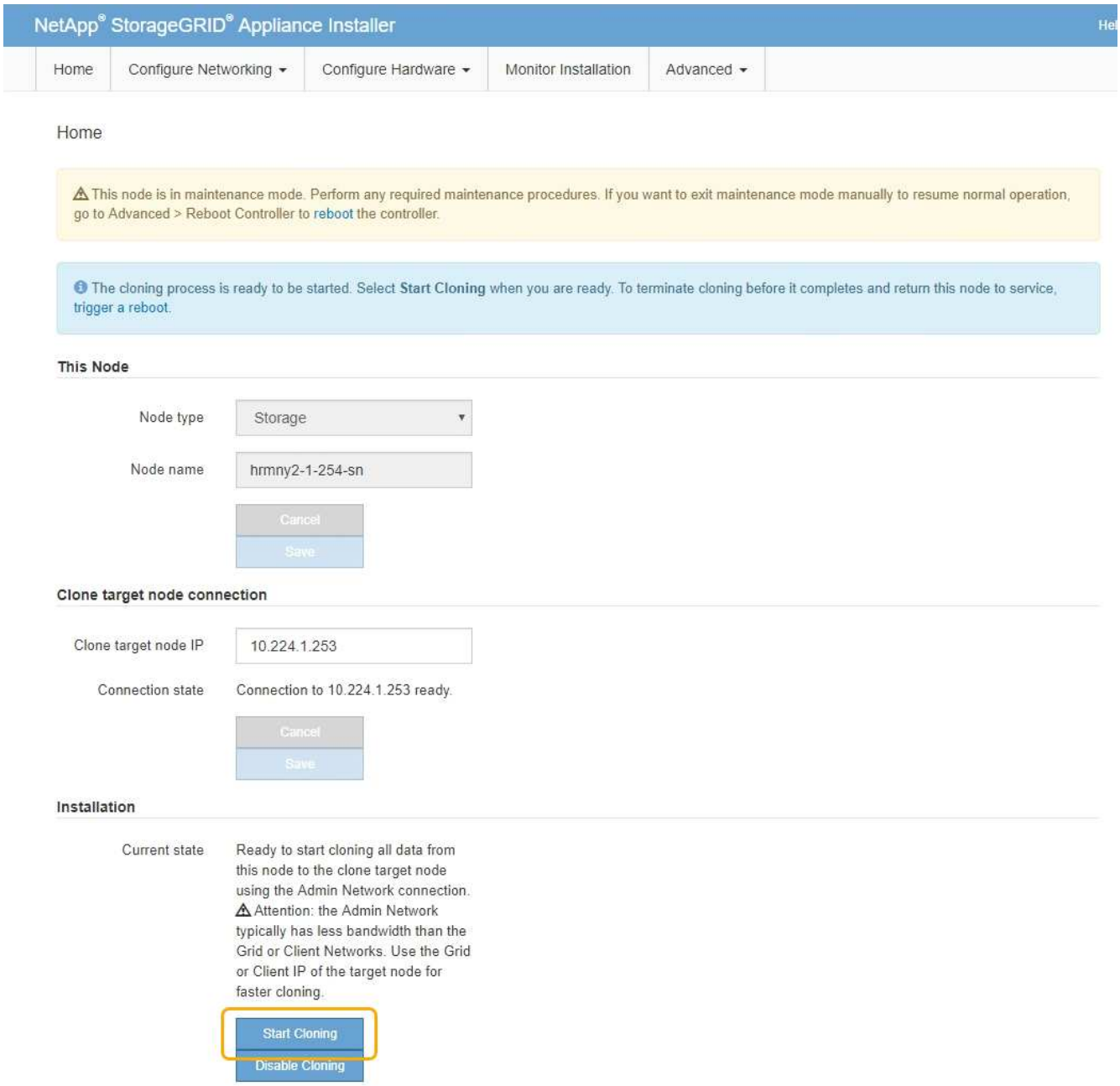


3. Para **Clone IP do nó de destino**, insira o endereço IP temporário atribuído ao nó de destino para que a rede use para clonar tráfego de transferência de dados e selecione **Salvar**.

   Normalmente, você insere o endereço IP da rede de Grade, mas se precisar usar uma rede diferente para clonar tráfego de transferência de dados, insira o endereço IP do nó de destino nessa rede.

   > O uso da rede de administração de 1 GbE para clonar a transferência de dados resulta em clonagem mais lenta.

   Depois que o utilitário de destino é configurado e validado, na seção Instalação, **Iniciar clonagem** é ativado no nó de origem.



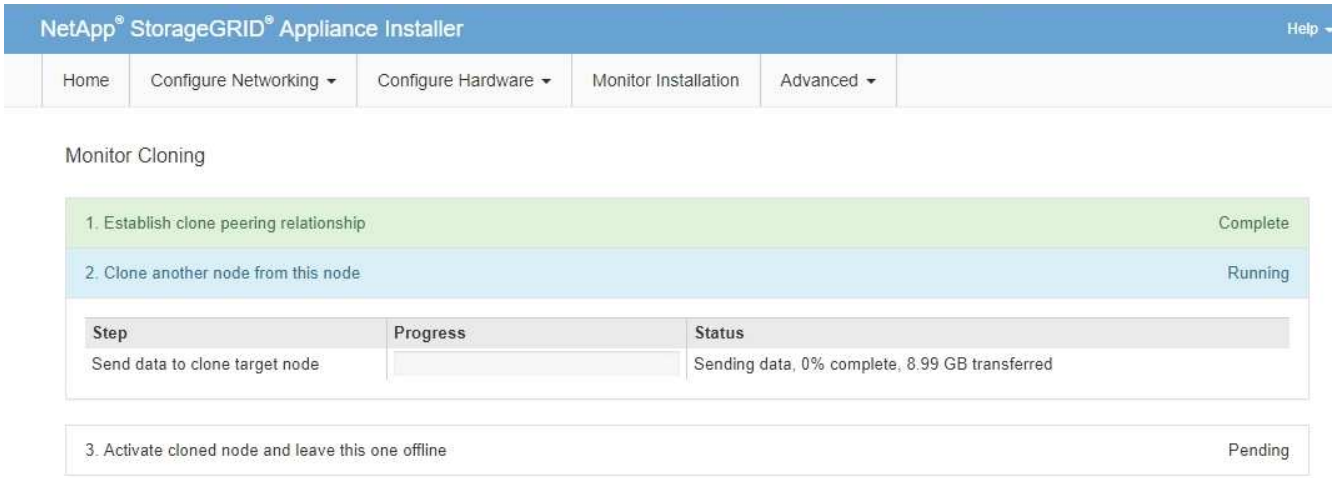
Se existirem problemas que impeçam a clonagem, **Iniciar clonagem** não está ativada e os problemas que você deve resolver são listados como **estado de conexão**. Esses problemas são listados na página inicial do instalador do dispositivo StorageGRID do nó de origem e do dispositivo de destino. Apenas um problema é exibido de cada vez e o estado é atualizado automaticamente à medida que as condições mudam. Resolva todos os problemas de clonagem para ativar **Iniciar clonagem**.

Quando **Iniciar clonagem** está ativada, o **estado atual** indica a rede StorageGRID selecionada para o tráfego de clonagem, juntamente com informações sobre como usar essa conexão de rede.

"Considerações e requisitos para clonagem de nós do dispositivo"

4. Selecione **Iniciar clonagem** no nó de origem.
5. Monitore o progresso da clonagem usando o instalador do StorageGRID Appliance no nó de origem ou de destino.

   O Instalador do StorageGRID Appliance nos nós de origem e destino indica o mesmo status.



A página monitorar clonagem fornece progresso detalhado para cada etapa do processo de clonagem:

- **Estabelecer relação de peering de clone** mostra o progresso da configuração e configuração da clonagem.
- **Clone outro nó deste nó** mostra o progresso da transferência de dados. (Esta parte do processo de clonagem pode levar vários dias para ser concluída.)
- **Ativar nó clonado e deixar este offline** mostra o progresso da transferência de controle para o nó de destino e colocar o nó de origem em um estado de pré-instalação, após a transferência de dados estar concluída.

6. Se você precisar encerrar o processo de clonagem e retornar o nó de origem ao serviço antes de a clonagem ser concluída, no nó de origem vá para a página inicial do Instalador do StorageGRID Appliance e selecione **Avançado** > **Reiniciar controlador** e, em seguida, selecione **Reiniciar no StorageGRID**.

   Se o processo de clonagem for terminado:

   - O nó de origem sai do modo de manutenção e regozija-se com o StorageGRID.
   - O nó de destino permanece no estado de pré-instalação. Para reiniciar a clonagem do nó de origem, inicie o processo de clonagem novamente a partir da etapa 1.

Quando a clonagem for concluída com sucesso:

- Os nós de origem e destino trocam endereços IP:
  - O nó de destino agora usa os endereços IP originalmente atribuídos ao nó de origem para redes de Grade, Admin e Cliente.
  - O nó de origem agora usa o endereço IP temporário inicialmente atribuído ao nó de destino.
- O nó de destino sai do modo de manutenção e une o StorageGRID, substituindo o nó de origem.
- O dispositivo de origem está em um estado pré-instalado, como se você o tivesse preparado para reinstalação.

  "Preparação de um aparelho para reinstalação (apenas substituição da plataforma)"

Se o dispositivo não se juntar novamente à grade, vá para a página inicial do Instalador de dispositivos StorageGRID para o nó de origem, selecione **Avançado** > **Reiniciar controlador** e, em seguida, selecione **Reiniciar no modo de manutenção**. Depois que o nó de origem for reinicializado no modo de manutenção, repita o procedimento de clonagem do nó.

Os dados do usuário permanecem no dispositivo de origem como uma opção de recuperação se ocorrer um problema inesperado com o nó de destino. Depois que o nó de destino se juntou ao StorageGRID com sucesso, os dados do usuário no dispositivo de origem ficam desatualizados e não são mais necessários. Se desejar, peça ao suporte StorageGRID para limpar o dispositivo de origem para destruir esses dados.

Você pode:

- Use o dispositivo de origem como destino para operações de clonagem adicionais: nenhuma configuração adicional é necessária. Este dispositivo já tem o endereço IP temporário atribuído que foi originalmente especificado para o primeiro destino clone.
- Instale e configure o dispositivo de origem como um novo nó de dispositivo.
- Deite fora o aparelho de origem se já não for utilizado com o StorageGRID.

Outras versões da documentação do NetApp StorageGRID

Você pode encontrar a documentação para outras versões do software NetApp StorageGRID aqui:

- "Documentação do StorageGRID 11,9"
- "Documentação do StorageGRID 11,8"
- "Documentação do StorageGRID 11,7"
- "Documentação do StorageGRID 11,6"
- "Centro de Documentação do StorageGRID 11,4"
- "Centro de Documentação do StorageGRID 11,3"
- "Centro de Documentação do StorageGRID 11,2"

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.

"Aviso para StorageGRID 11,5"

Informações sobre direitos autorais

Informações sobre marcas comerciais